



## William F. Friedman Collection Pre-Release

In late April, 2015, the National Security Agency (NSA) will release over 52,000 pages of historical material relating to the career of William F. Friedman. On this page you will find a small sampling of those documents.

Considered the dean of American Cryptology, William F. Friedman (1891-1969) was a pioneer in the field as one of the first to apply scientific principles to the making and breaking of codes. His most well-known accomplishment was leading a small team which broke Japan's "Purple" diplomatic cipher prior to the Pearl Harbor attack, but through his lectures, textbooks, and mentorship Friedman also trained several generations of American cryptologists, thus laying the foundation for the 20th century U.S. signals intelligence community.

NSA's William F. Friedman Collection consists of materials created or collected by Mr. Friedman over the course of his government career and comprising his official working files. The Collection was augmented by documents related to Friedman's work and contributions to cryptology subsequently compiled by NSA historians and archivists. Covering almost 60 years, the records shed light on both the career of this legendary cryptologist and the history of American signals intelligence.

This collection, composed of over 52,000 pages in more than 7,600 documents (along with some sound recordings and photographs), has been preserved in the NSA Archives for its historic significance and value. The bulk of the material dates from 1930-1955 and represents Mr. Friedman's work at the Signals Intelligence Service, the Signal Security Agency, the Armed Forces Security Agency, and NSA.

*Please Note: The following historical documents are scanned images of formerly classified carbon paper and letters that have been declassified and saved as PDFs. Due to the age and poor quality of some of the images, a screen reader may not be able to process the images into word documents. In accordance with Sections 504 and 508 of the Rehabilitation Act of 1973, as amended, individuals may request that the government provide auxiliary aids, alternate formats, or services to ensure effective communication of the substance of the documents. For such requests, please contact the Public Affairs Office at 301-688-6524.*

1. Certain Aspects of "Magic" In the Cryptological Background of the Various Official Investigations Into the Attack on Pearl Harbor
2. Conversation Between William Friedman and Col. Sadtler on Pearl Harbor
3. Examination - Thesis Submitted by W.F. Friedman; the Duties of the Officer-in-charge of the Signal Intelligence Service, GCHQ
4. Final Report and Papers of the U.K.-U.S. Conference on the Communications Security of the NATO Countries (USCIB 23/65); Agenda Item for USCIB's 88th Meeting, 10 July 1953
5. Final, Lecture No. 1, Introduction to Cryptology by William F. Friedman; Introductory Remarks and General Introduction of the Subject
6. Friedman TDY Trip to London, Apr-Jun 1943; Diary - Daily Activities
7. Friedman's Contributions In the Fields of Communications Security and Communications Intelligence, 1930-1945
8. Friedman's Diary - TDY Trip to Europe, Oct 1946; Itinerary, Daily Activities
9. Friedman's Original Worksheets of Hebern Solution, 11 Nov 1936
10. Handwritten Notes for Introduction to Cryptology by William F. Friedman, Lecture No. 5
11. Important Contributions to Communications Security, 1939-1945; Summary of Contributions Made by Mr. Friedman
12. Introduction to Cryptology - IV, Draft, Cryptology In the Civil War by William F. Friedman
13. Introduction to Cryptology-VI by William Friedman; Handwritten Draft of Lecture Deals with Cryptology from the End of WWI to End of WWII, No. 6, 1st Draft
14. Japanese Broadcast of Office Chief's Code; Circular #2353 Translation Revised 26 Sept 44
15. Japanese Broadcasts In Office Chief's Code; Circulars # 2353 and #2354
16. Japanese Office Chief's Coded Broadcasts
17. Job Descriptions - Special Assistant to the Director and Cryptologic Research Advisor; Plus Others; Duties and Responsibilities
18. Lecture 2, Final Version, Introduction to Cryptology by William F. Friedman; Historical Information About Cryptology
19. Lecture 3, Introduction to Cryptology, Draft, William F. Friedman; Deals with the Cryptosystems Employed by the British Regulars and the Colonials During the Period of American Revolution

20. Lecture on Code Work Given to the Naval Academy Graduating Class at Annapolis In 1922
  21. Mr. Friedman's Appointments, 1954 and 1955; Notebook Listing Daily Appointments
  22. Report on Temporary Duty, ETO, by Mr. Friedman; Copy of Orders; Account of Movements and Duty on Trip
  23. SCAG Conference, 31 May 1951
  24. The Influence of Cryptologic Power on History-Lecture No. 3 "Making the Most of A Cryptologic Opportunity" - the Zimmerman Telegram; William F. Friedman, UCMC Lecture Series: History of Cryptology-
-

Memo:

8 May 1957

A week ago I phoned General Sanford, Director NSA, to request he give consideration to my being permitted to publish this brochure, minus the classified portions. My reason: the "revisionists" literature, including the books by Adm. Theobald & Adm. Kimmel,

Gen. Sanford said then he was dubious about the advisability of raking over the dead embers, etc., that the Theobald charges were balderdash & not worthy of serious attention. But he said he'd consider my request & would let me know.

Today Gen Sanford

planned me to say that he had considered my request & did not think it would be advisable to publish the brochure at all - for the reasons he gave before.

I told him immediately I accepted his decision without question. He thanked me. I thanked him for calling me.

W. J. S.

~~SECRET~~

CERTAIN ASPECTS OF "MAGIC" IN THE CRYPTOLOGICAL BACKGROUND  
OF THE VARIOUS OFFICIAL INVESTIGATIONS  
INTO THE ATTACK ON PEARL HARBOR

by

William F. Friedman

~~SECRET~~

~~SECRET~~

Certain Aspects of "Magic" in the Cryptological Background  
of the Various Official Investigations  
into the Attack on Pearl Harbor

## INDEX

<u>Section</u>	<u>Page</u>
1. Introduction . . . . .	1
2. The Real Essence of the Problem . . . . .	11
3. A New Look at the Revisionists Allegations of Conspiracy to Keep Kimmel and Short in the Dark . . . . .	18
4. Was MAGIC Withheld from Kimmel and Short and, if so, why? . . . . .	35
5. The "Winds Code Messages" . . . . .	49
6. The Question of Sabotage . . . . .	53
7. Conclusions . . . . .	65
8. Epilogue . . . . .	68

APPENDIX 1: "Pearl Harbor in Perspective,"  
by Dr. Louis Morton. United States Naval  
Institute Proceedings, Vol. 81, No. 4,  
April 1955; pp. 461-468

APPENDIX 2: "Pearl Harbor and the Revisionists," by  
Prof. Robert H. Ferrell. The Historian, Vol. XVII,  
No. 2, Spring 1955, pp. 215-233

## 1. INTRODUCTION

More than 15 years have passed since the Japanese, with unparalleled good luck, good luck that now seems astounding, and with a degree of skill unanticipated by the United States, executed their surprise attack on Pearl Harbor during the morning hours of 7 December 1941. It was an attack that constituted a momentous disaster for the United States; it made our Navy's Pacific Fleet, for all practical purposes, hors de combat for many months. In the view of Mark S. Watson, in a volume written for the Army series on the history of the U. S. Army in World War II, Chief of Staff: Prewar Plans and Preparations (1950), the disaster was the result of a "fateful series of mischances" among which he listed those which he considered the most important. He did not list them all; to do so would make the disaster partake of the character of an enormous, and almost incredible Greek tragedy--so many big and little things went wrong to make the disaster possible and to prevent its being averted with little or no damage.

The Battle of Pearl Harbor is still being fought but the adversaries this time are all Americans; and though the battle is bloodless, because the weapons are now words, not bullets or bombs, it is quite acrimonious and intense, as internal or civil wars generally are. This time the battle is intended to capture, by a sort of literary "brainwashing," the minds of a large segment of the American people who more or less dimly feel that the truth, the whole truth, has not yet been told. Many Americans, I am sure, are still undecided in regard to who or what was

responsible for this most momentous and most humiliating naval disaster in our history.

Fifteen million words, more or less, have been written concerning, explaining, or attempting to assess and fix responsibilities for the Pearl Harbor disaster, and to show why the U. S. forces at Honolulu were caught napping in the early hours of what President Roosevelt referred to as that "day of infamy" when he appeared before Congress on 8 December 1941 to declare war on Japan. The Report and Hearings Before the Joint Committee on the Investigation of the Pearl Harbor Attack (79th Congress, 2d Session, Government Printing Office, Washington, 1946), hereinafter referred to as PHR, alone contain 15,000 transcript pages; the over-all final report of the Committee comprises some ten million words and fills 40 volumes of closely printed text. Thus far, in addition to this vast amount of material there must be at least five million words in the writings of private individuals. Some of them defend the Findings, Conclusions, and Recommendations of the Majority in the PHR; others defend the Findings and Conclusions of the Minority in the PHR; still others disagree and violently attack both what the Majority and the Minority said. Even representative Keefe, a Republican who signed the Majority Report found it necessary to add to that report some additional views of his own where he could not agree with those of the Majority. It is obvious that in this brochure it will be impossible to deal with all that has been written on the subject. Even to list by title the books, brochures, articles (not to mention the thousands of newspaper accounts, letters to editors, etc.) which have something to add to the



story would be a fairly large task. A bibliography covering the items on Pearl Harbor in my private collection will be found in the "Subject file" now in the NSA Library. But it is a strange, indeed, it is a remarkable fact that not a single new item of information having a direct bearing upon attempts to explain why the Pearl Harbor attack could have come or did come as a complete surprise to the U. S. has been turned up since 1946, when the Joint Congressional Committee completed its task. One may well assume, therefore, that since no new facts have come to light it must be something else that is keeping the Battle of Pearl Harbor going. The assumption is true: the facts developed in the various investigations of 1944, 1945, and 1946 are being scrutinized now through different sorts of spectacles and by different observers; this results in new "interpretations" of the old, well-known facts.

It is the purpose of this brochure to make a few observations and comments on the current Battle of Pearl Harbor. They are directed at the writings of certain historians who call themselves or are known as "revisionists," and who find much support in two recently published books, both by high-ranking officers of the U. S. Navy. These charges are very serious--indeed they are tantamount to imputing at least very questionable behavior by persons of such stature as the late President Franklin D. Roosevelt, the Army's Chief of Staff, General George C. Marshall, and the Navy's Chief of Naval Operations, Admiral Harold R. Stark. The charges are really not new; their antecedents, or nuclei of them or carefully veiled hints at them, can be found in some of the early writings of the more rabid Roosevelt-haters, and even in some parts of the

reports made by various official U. S. investigating bodies appointed to look into the matter during the last phases of World War II or soon after that war had been won.

In another section of this report will be found an attempt to explain the genesis of the suspicions which aroused the Roosevelt haters and which kept them "needling" the President and his Administration for an explanation of how it was possible that the U. S. was taken so completely by surprise when the Japanese attacked Pearl Harbor; to introduce the explanation at this point I think would be confusing. All that can logically be said right here is that the President, his Administration, and the Chiefs of the two military services simply could not afford to permit the true explanation to be broadcast while the war was still in progress.

A very impartial bibliographical survey of the principal items in the literature of the subject has been prepared by a historian of recognized standing, Dr. Louis Morton, Chief of the Pacific Section of the U. S. Army's Office of Military History. His survey, entitled "Pearl Harbor in Perspective," was published in the April 1955 issue of the United States Naval Institute Proceedings (Vol. 81, No. 4, Whole No. 626, pp. 461-468). A copy of Dr. Morton's survey forms Appendix 1 to this brochure.

A second recapitulation of the Pearl Harbor story and also a source of material which may interest the reader in what the present brochure aims to do is found in an article by Robert H. Ferrell, Assistant Professor of History at Indiana University, published also in 1955, in The Historian, under the title "Pearl Harbor and the Revisionists"

(Vol. XVII, No. 2, Spring 1955, pp. 215-233). Prof. Ferrell's article (given completely in Appendix 2 to this brochure) begins as follows:

It was perhaps inevitable that after the second World War, as after the war of 1914-18, there should appear in the United States a school of historians questioning the purposes of the war and the motives of the wartime statesman. The cost of both world wars, in human lives and in physical resources, was very high; and it was only natural that some individuals should question such expenditure. Yet the new school of "revisionism" appearing after the second World War has undertaken a line of investigation which, if successful, will force the rewriting of an entire era in American history. The revisionists hope to prove that in 1941 President Franklin D. Roosevelt purposely exposed the Pacific Fleet at Pearl Harbor, and goaded the Japanese into attacking it, thus bringing the United States into the war on the side of the Allies. As Professor Harry Elmer Barnes has put the case, in rather plain English, "The net result of revisionist scholarship applied to Pearl Harbor boils down essentially to this: In order to promote Roosevelt's political ambitions and his mendacious foreign policy some three thousand American boys were quite needlessly butchered.

...

Professor Ferrell follows this extract from Professor Barnes with the following words (in a footnote):

"Of course, they were only a drop in the bucket compared to those who were ultimately slain in the war that resulted, which was as needless, in terms of vital American interests, as the surprise attack on Pearl Harbor." H. E. Barnes, ed., Perpetual War for Perpetual Peace (Caldwell, Idaho, 1953), Ch. 10, "Summary and Conclusions," p. 651.

Strong language, isn't it? Very strong, I think, coming from a well-known historian such as Barnes. What substance is there to the strident claims of those professional historians, some of them very well-known and able men, who are the spokesmen for the revisionists? What is it that they wish to prove from their study of the facts concerning the Pearl Harbor disaster? First, they wish to prove that there was no need at all, "in terms of vital American interests," for the U. S. to enter into World

War II as one of the belligerents. Some of them no doubt believe that we fought on the wrong side, with the wrong allies! With this phase of the subject I shall not concern myself in this brochure, since I make no pretence whatsoever of being a historian competent to deal with such an important subject. Next, some of the revisionists claim or believe that they have proof that the disaster at Pearl Harbor was no "accident," that it was brought about deliberately by President Roosevelt. They believe that what they call our "back-door" entry into the conflict was based upon an erroneous view, held by him and his Administration, as to what the U. S. role should be in world affairs; also, they want us to believe that our entry into World War II was for the personal political advantage of President Roosevelt and his followers in the Administration. They contend, in fact, that he goaded the Japanese into making the attack, that he enticed them into doing so by using the U. S. Pacific Fleet as a "lure;" that he knew from the so-called "MAGIC", the Japanese secret communications which Army and Navy cryptanalysts had solved, the exact time the attack would be made and the exact place where they were going to make it; that the President sensed that such an attack was the only thing which would unify American opinion and bring the people of the United States to a pitch of excitement and resentment sufficiently high to lead them to accept with equanimity U. S. entry into World War II on the side of the British and the French, thereby, as Roosevelt felt and as turned out to be the case, assuring the complete defeat of the Axis powers; that President Roosevelt should and could have avoided the disaster at Pearl Harbor but deliberately chose not to do so, for the

reasons cited above; and that he purposely withheld MAGIC intelligence from Admiral Kimmel, Commander-in-Chief of the U. S. Pacific Fleet, and General Short, Commanding General of the Hawaiian Department, the two highest-ranking commanders in Hawaii who should have been but were not given this information and who, therefore, were permitted by him to be deliberately misled as to the real situation, misled to the point, in fact, that when the attack came they were entirely unprepared even to meet it, let alone repulse it. In withholding this information, one of the proponents of this theory, a retired admiral of the regular U. S. Navy, Rear Admiral Robert A. Theobald, implies in his book, The Final Secret of Pearl Harbor (New York: The Devin-Adair Co., 1954), that to make it quite certain that the Japanese attack would be a complete surprise, so far as General Short and Admiral Kimmel were concerned, the President had to have and did have as reluctant partners in his conspiracy, or what was tantamount thereto, General Marshall, the Chief of Staff of the Army, and Admiral Stark, the Chief of Naval Operations, both regular officers of highest integrity and repute. And although Admiral Kimmel in his own book Admiral Kimmel's Story (Chicago: Henry Regnery Co., 1955) does not go quite so far as does Admiral Theobald as to make charges tantamount to conspiracy, he does go quite a long distance along the same route. There is a degree of confusion in regard to this point, however. The following, for example, appears on the inside flap of the dust cover:

Admiral Kimmel sticks to his own end of the story. He tells us about the material he was denied, the warning messages he didn't get. He impugns no motives, he makes no deductions from unproved hypotheses. [ "Is this a slap at Theobald?" ] But the book is

sufficient to nail down the inescapable point: the blame for the loss of the Pacific Fleet battleships rests squarely on Washington not on the men at Pearl.

But on the back of the dust jacket, repeated from the last chapter of his book (p. 186), Admiral Kimmel says:

Again and again in my mind I have reviewed the events that preceded the Japanese attack, seeking to determine if I was unjustified in drawing from the orders, directives and information that were forwarded to me the conclusions that I did. The fact that I then thought and now think my conclusions were sound when based upon the information I received, has sustained me during the years that have passed since the first Japanese bomb fell on Pearl Harbor.

When the information available in Washington prior to the attack was finally disclosed to me long after, I was appalled. Nothing in my experience of nearly forty-two years service in the Navy had prepared me for the actions of the highest officials in our government which denied this vital information to the Pearl Harbor commanders.

If those in authority wished to engage in power policies, the least that they should have done was to advise their naval and military commanders what they were endeavoring to accomplish. To utilize the Pacific Fleet and the Army forces at Pearl Harbor as a lure for a Japanese attack without advising the commander-in-chief of the fleet and the commander of the Army base at Hawaii is something I am wholly unable to comprehend.

While I am still able to do so, I feel that I must tell the story so that those who follow may fully realize the imperative necessity of furnishing the naval and military commanders at the front with full and clear information. Only in this way can the future security of our country be preserved.

Dr. Morton in commenting upon Admiral Kimmel's Story says (p. 461):

Admiral Kimmel's case rests upon the allegation that he was deliberately denied information available in Washington. Had he had this information, he says, he would have known the Japanese intended to strike Pearl Harbor and could have adopted measures to meet the attack and minimize the losses. These measures, which he outlines, are of considerable interest, though one wonders to what extent they are guided by hindsight.

Dr. Morton continues as follows: (p. 462)

To support his case, Admiral Kimmel draws on the evidence presented during the investigations of the Pearl Harbor attack. This evidence, he claims was not only obscured at the time but was evaluated to produce a desired result. Inconsistencies in the testimony were ignored, and important questions raised during the hearings left unanswered. He charges bias on the part of investigating officers and a deliberate effort to white-wash the administration and block an impartial search for the truth. "The Congressional investigation," Kimmel declares, "was governed by the majority party, the Democrats. The huge volumes of testimony in that inquiry served to confuse the public mind as to the significance of the facts and to smother testimony damaging to the administration."

Responsibility for Pearl Harbor, Kimmel charges, rests squarely upon the shoulders of his superiors in Washington and ultimately on the Commander-in-Chief, President Roosevelt. "Until this day," he writes, "I have kept silence on the subject of Pearl Harbor . . . Now, however, I deem it my duty to speak out. What took place in Washington must be so clearly placed on the public record that no group of persons in administrative power will ever dare again to invite another Pearl Harbor and place the blame on the officers in the fleet and in the field."

The charges that Admiral Kimmel makes are not new and were being circulated even before the end of the war. The Japanese attack on December 7 had unified the country and ended temporarily the debate between the "Isolationists" and the "interventionists" which had marked the prewar years. All classes and parties closed ranks for the duration of the struggle. But even during the war, there had been a recognition of the political implications involved in the question of responsibility for Pearl Harbor, and the administration had taken steps to preserve the record. Six investigations had been conducted even while the conflict raged, all but one of them by the Army and Navy. As a result, a large volume of testimony and documents that might otherwise have been lost was assembled. But the requirements of wartime security and a unified national effort made public debate impossible.

The war over, partisan differences reappeared, and critics of President Roosevelt began to challenge openly the views so widely held during the war years. The cooling of passions and disillusion with the postwar world raised further questions about American participation in the war. Historians and publicists, as they have done after every war, sought to reassess the causes of the war and to place Roosevelt's policy in the larger perspective of American history. Thus, in the years following the end of the conflict, a new interpretation of the events that had preceded the war and of the conduct of the war itself emerged.

The foregoing final paragraph of the extract from Dr. Morton's article brings us directly to the principal revisionist contention which will be examined in the present brochure. The contention, as noted above, was first stated in 1945 by John T. Flynn, one of the early and most vitriolic revilers of President Roosevelt, in a pamphlet entitled The Final Secret of Pearl Harbor, in which he revealed the fact that U. S. cryptanalysts had solved the Japanese diplomatic codes and ciphers before the Pearl Harbor attack. His contention was that the intelligence derived or derivable from the solved and translated messages, the so-called MAGIC, told exactly where and when the Japanese were going to strike; that this priceless information Roosevelt deliberately kept from Admiral Kimmel and General Short, with the result that the Japanese were able to make their attack with complete surprise; and that the loss of men and ships that resulted therefrom, however unfortunate it was for the U. S. and a few American families, unified the country. That, claims Flynn, was Roosevelt's aim. At any rate, as Dr. Morton indicates, the Japanese attack on Pearl Harbor ended the debate between the "isolationists" and the "interventionists."



## 2. THE REAL ESSENCE OF THE PROBLEM

Distilled down to its essence, therefore, the first question is: Did MAGIC really contain clear and unequivocal indications as to exactly where and when we would be hit by the Japanese in the war which Roosevelt knew, or was expecting, or at least felt was in the offing?

Much has been written on this basic question; hundreds of thousands--indeed, millions of words, in fact--have been published on the question in an attempt to answer it either affirmatively or negatively. If some Americans now scoff at the whole business and say that all that could be said on the point was said years ago--why not stop flogging a dead horse?--let them note that in as staid and unsensational a newspaper as The Wall Street Journal there appeared a long review of Admiral Kimmel's Story in the issue for 14 January 1955, accompanied by a lengthy editorial entitled "Pearl Harbor" in the same issue; let them note, too, another lengthy editorial entitled "Myth of the broken code" in the issue of the same newspaper for 21 January 1955; let them read also the baker's dozen "Letters to the Editor" in the issues for 21 January, 31 January, 4 February, and 6 February 1955, all commenting upon the two editorials and the book review mentioned above. The question therefore can by no means be said to be "dead and buried;" in fact, even to this day references to the "MAGIC" that was available and was not used at the time of Pearl Harbor keep popping up in the daily newspapers, in periodicals, and in books. For instance, there are two "Letters to the Editor" in the Washington Post on Pearl Harbor as recently as 31 December 1956 and 4 January 1957. And

as I write this brochure word has just come that the Chicago Tribune is about to publish another (revisionist, no doubt) article on the subject.

Let me therefore repeat the question: Did MAGIC really contain clear and unequivocal indications as to exactly where and when we would be hit by the Japanese in the war which Washington knew, or was expecting, or at least felt was probably soon to come?

In this brochure I shall attempt to dispose of this basic question in a rather simple and, in my opinion, a definitive manner by attacking it in what may seem to be a round-about way. But just before getting right down to it I will place before the reader a short extract from a book published late in 1956 by a recently-deceased and a highly-respected (by certain Americans who knew him) Japanese whose words were such-- he died in prison--as to indicate that he had no particular reason for hiding the truth. I refer here to the book written by Shigenori Togo, the man who was Japanese Minister of Foreign Affairs at the time of the attack on Pearl Harbor and across whose desk there certainly must have passed the most important of the messages to and from the Foreign Office and Japanese ambassadors, ministers, and consuls abroad.<sup>1</sup>

It is to be noted, and indeed emphasized, before going into this phase of the subject, that at the time of the attack the only cryptographic systems which the U. S. cryptanalytic agencies had solved and were able to read were not the Japanese military or naval systems; they were only the systems used by the Foreign Office. Whatever intelligence the U. S. authorities were able to obtain from MAGIC therefore must have been and

---

<sup>1</sup> The Cause of Japan. New York: Simon and Schuster, 1956.

was clearly derived from Japanese diplomatic communications. With this fact in mind let us take a look at an item of much interest in Togo's book (pp. 118-119 and 197):

It is not difficult to conceive the extent of the tyranny of the military power from the fact that on the eve of the Pacific War such a fundamental datum as the total tonnage of Japanese naval vessels—not to speak of the displacement of the gigantic battleships Yamato and Musashi, or the plan to attack Pearl Harbor—was vigilantly withheld from the knowledge of the civilian cabinet ministers. General Togo even told me in Sugamo Prison that it was only at the IMTFE that he had first learned that the Japanese task force which carried out the attack on Pearl Harbor had assembled at Hitokappu Bay on 10 November, and weighed anchor for Hawaii on the morning of the 26th! The high command did not divulge its secrets even to the full general who was Premier and Minister of War; it is easy to conceive how other ministers were treated.

. . . . .

The war decision was thus made, and various problems which would arise with the opening of the war were submitted to meetings of the Liaison Conference. One thing which—needless to say—was not discussed in the Liaison Conference was operational aspects of the impending hostilities. It was disclosed at the IMTFE that the naval task force under Admiral Nagumo had sailed from Hitokappu Bay on 26 November under orders to strike Pearl Harbor, and in its judgment the tribunal made the absurd finding that the scheduled attack was freely discussed at the meeting of the Liaison Conference on 30 November. We had, of course, no knowledge of the plan; it was the invariable practice of the high command not to divulge to civilian officials, such as us, any scrap of information bearing on these highly secret operations, and anyone familiar with the system will readily understand our total lack of knowledge of them. (This condition is sufficiently well illustrated by the fact, which I have mentioned elsewhere, that Tojo told me that it was only at the IMTFE trial itself that he first learned any operational details of the Pearl Harbor attack; a mass of additional evidence was adduced at the trial showing that the civilian members of the Cabinet had no prior knowledge even of the existence of the plan to attack Hawaii.)

It is a fair and logical deduction to conclude that if Togo was telling the truth, i.e., that the civilian members of the Japanese Cabinet, including Prime Minister Tojo and the Foreign Minister himself, had no

prior knowledge of the plan, including of course the exact date on which the Pearl Harbor attack was to take place (as set by the Japanese high command) then the MAGIC messages themselves in the communications from and to the Foreign Office could not possibly have contained any definite information, let alone a clear-cut statement, on this very important point. And if the MAGIC messages did not contain this information or statement how could President Roosevelt or any members of his immediate official family, or the heads of U. S. Army and U. S. Navy intelligence staffs know from the MAGIC messages exactly where and when the attack was coming? But this question does arise: did Togo tell the truth in his book? If he did, how are we to explain certain of the MAGIC messages the records of PHR contain?

After re-reading the hundreds of MAGIC messages that were exchanged between the Foreign Ministry and its offices abroad in the year 1941 it seems fantastic, it strains our credulity, to believe that Togo did not know what was being planned. To mention only one set of messages, the "dead line" messages—after which "things are automatically going to happen"—how could Togo not know what was being planned? How are we to explain them, if he didn't know that the U. S. was going to be attacked? But let it be remembered that we are now re-reading the messages from the vantage point of hindsight. There is not a single message that can be said to contain categorical evidence proving that Minister Togo must have known that Pearl Harbor was to be the target. In 1946, and even now when we re-read those messages in Part 12 of the PHR, I realize that it is fantastic that somebody in U. S. Intelligence did not or could not see that the blow was being prepared against Pearl Harbor. But if we

believe Togo was an honorable man and was telling the truth, then we must conclude that he and his closest associates in the Foreign Office were no better at intelligence than our own intelligence authorities! They knew or only guessed that something was going to happen after 29 November 1941, but they didn't know exactly where or when! Or shall we assume that somebody in the Japanese Foreign Office, some subordinate of Togo, the Foreign Minister, was "in on the secret"—and it was he that took care of all the messages that pointed to Pearl Harbor? Could be! Could easily be! How many messages going out of any one of our own large executive departments and signed by the Secretary thereof are actually seen by the Secretary? But I do not wish to belabor the point. Let us merely say that it is quite possible that Togo saw none of the crucial messages or, what is more probable, that he saw them but, not being "in on the secrets" of the Japanese high command, did not draw the correct deductions—that the U. S. was to be attacked, without warning, at Pearl Harbor in the early hours of 7 December 1941, and that the object of the attack was to destroy the U. S. Pacific Fleet if possible. But let us also remember that reading the MAGIC messages in 1946 or in 1956 is analogous to reading the final chapter of a detective tale—before the preceding chapters, with their false and purposely misleading clues injected by the author to evoke the reader's interest. In reading such a detective story in the normal manner the final chapter often makes the reader feel inferior, even silly, that he could not see the truth, the real elements of the mystery right from the beginning. The Japanese were getting intelligence reports—call them if you will, "ordinary spy reports" from several U. S. military bases

besides Hawaii, such as the Philippines, Panama Canal, Seattle, and San Francisco. It is true that Japanese interest in Pearl Harbor seemed to be and actually was much greater than at any other base; but one could also say that this greater interest stemmed from a perhaps justifiable fear by the Japanese that the U. S. Pacific Fleet might sortie some dark night and strike the first blow at Japan. They, as well as the U. S., did not want to be taken by surprise! Perhaps an intelligence specialist with the proper kind of imagination might have hit upon the real reason for the greater Japanese interest in Pearl Harbor, but who can be certain of this? All that can safely be said in regard to the Togo statement is this: Both he and Prime Minister Tojo may have been told, or they may have guessed, that Japan was going to strike—but not exactly where and when. These two very important elements the Japanese high command kept to itself even after the task force left Japanese waters. And for those revisionists who think the U. S. note of 27 November 1941 was an ultimatum and that it was that note which triggered off the attack on Pearl, let them ruminate on the fact that the Japanese task force which attacked Pearl left Japanese waters the day before that note was sent off by Secretary of State Hull. His note may have constituted an ultimatum—but it did not bring on the attack. The attack was planned very carefully, months before that, and, to repeat, was already launched to the point of having departed from Japanese waters.

But there is another revisionist prop, and a very important one, I must emphasize, which I wish to undermine, for it should be greatly weakened when consideration is given to another argument which is so obvious

and simple that it has been a source of astonishment to me that the revisionists themselves have not thought of it. (Parenthetically I want to preface the argument by saying that any hesitancy I might have in stating it melts away when I find that several very able naval historians with whom I have discussed it expressed astonishment that it had not hitherto been mentioned. One of them said of it in a recent personal letter:

"In retrospect I realize that some of the ideas you mentioned about the events leading up to the attack on Pearl Harbor (like Columbus' egg trick!) are startling in their simplicity and obviousness--which is probably why no one has heretofore recognized their importance." My contention, I think, warrants taking a new look at a certain phase of the Pearl Harbor mystery--if indeed there is any mystery about the factors entering into our being taken by surprise.

3. A NEW LOOK AT THE REVISIONISTS ALLEGATIONS OF CONSPIRACY TO KEEP  
KIMMEL AND SHORT IN THE DARK

The revisionists' argument, which I hesitate to repeat (since it has already been stated in this brochure; but its repetition may make what I have to say crystal clear) runs as follows: President Roosevelt desperately needed a good reason for justifying America's entry into World War II. He needed it in order to save the British from utter defeat by Germany; France was already down and out! Britain was next on Hitler's list--and then the United States. (The revisionists deny this most vehemently, but everything that Hitler had done thus far was strictly in accordance with the plans he outlined in Mein Kampf. In this connection, and as I write this, there has just come out a book which must be regarded as authoritative and which is called The German Weapons and Secret Weapons of World War II, by Rudolf Lusar. Lusar was head of the Technical Arms Department of the Wehrmacht. He discloses that Germany was also building the Heinkel 343, a bomber capable of reaching the United States and returning without refuelling. Several of the planes were ready at the end of the war. The book also says that it was originally planned to stage the first air raid on the United States in May 1945. So much for the revisionist contention that the benign Herr Hitler had no designs whatsoever on the United States; for it is very clear that he planned to bomb this country just as soon as he had finished off England.) The President wanted to get the U. S. into the conflict not only to save Britain but, ultimately, also to save the U. S. Timely action was needed. He had goaded Hitler by several unneutral acts in the Atlantic, as well as in establishing certain U. S.



logistical relations with Britain ("lend-lease," the transfer of 50 U. S. destroyers, etc.); but Hitler was too clever to be pushed to the point where Germany would have to declare war on America prematurely or where German action would justify an American declaration of war on Germany before Germany was ready for such action. Hitler realized, as well as President Roosevelt, that what American did held the answer to Germany's problem. President Roosevelt knew that the American people were not at all anxious to be drawn into the European war; but he felt that it was absolutely necessary that something be "engineered," so to speak, in order that the U. S. would, willy-nilly, be drawn into the conflict. This, the revisionists contend, as I have reiterated, Roosevelt felt was necessary to save England; it was incidentally also intended, they contend, to divert attention from the failure of the New Deal to bolster the badly sagging economy as a result of defective monetary policies and other internal difficulties. U. S. participation was also a Democratic objective, they say, for Roosevelt's reelection; and, of course, it was desirable to preserve the Rooseveltian prestige. The long-drawn out arguments with the Japanese might, in view of the Tri-partite pact of the German, Italian, and Japanese Axis, and despite Hitler's canny strategy of not succumbing to American provocation in the Atlantic, serve his purpose. Americans did not like the Japanese anyhow and were distrustful of these Orientals. Japanese ambitions in the Far East and distrust of the Japanese kept popping up everywhere in the American press and public opinion. But Roosevelt felt that there was one sine qua non to getting into a shooting war with the Japanese. In the words of Mr. Stimson, his

Secretary of War, unfortunate words one must now admit, it was all a matter of how the Japanese "could be maneuvered into the position of firing the first shot," otherwise the American people would be lukewarm about a war with them. MAGIC, that is, the secret intelligence which the solution of the Japanese diplomatic communications made available to the Roosevelt Administration in great abundance, provided a golden opportunity--so the revisionists, including Admiral Theobald, fervently believe. I have already and more than once stated in this brochure that the revisionists are convinced that MAGIC told the President exactly when and where their attack was going to be launched: in the early hours of the morning of 7 December 1941, at Pearl Harbor. By withholding from the U. S. commanders at Pearl Harbor this private knowledge which President Roosevelt gained from MAGIC--the horse's mouth, so to speak--enabled the President to accomplish his heart's desire. With this highly secret information he could maneuver the Japanese so that they would fire the first shot; he realized, they concede, that there would be some losses of men and ships, of course, as so callously stated in the extract from Professor Barnes which was quoted above, but these losses, they contend, he would regard as justified in the long run by saving England, France, and, later on, America from the Axis Powers--and it would incidentally save his own prestige and insure his reelection.

The important element in the foregoing argument, let it be noted, is that, to quote from Secretary Stimson's diary a bit, Japan was to be "maneuvered into a position of firing the first shot." The maneuver, according to the revisionists, included using the ships of the U. S.

Pacific Fleet as a lure; that is why, they argue, Roosevelt insisted on having that fleet based on Pearl Harbor instead of on the west coast of the U. S., as Admiral Richardson, Kimmel's predecessor, wished. But let be noted that Admiral Richardson's objections stemmed from purely logistical considerations, such as easier maintenance and repair; and morale of the sailors entered into the picture--Hawaii was a long way from "home" for the men and officers of the fleet. (Admiral Richardson had not the slightest idea that keeping the fleet at Pearl would deter the Japanese from doing what they wished to do in the Far East. In fact, he thought keeping the fleet on the West Coast would be more effective. Well, the President, the Commander-in-Chief, didn't agree with Admiral Richardson--and that's all there was to it. It turned out, unfortunately, that Admiral Richardson's view was more nearly correct than the President's--but does that mean that the President had ulterior motives in keeping the fleet at Pearl? I don't think so at all.)

And now for my counter argument on this score.

If we assume for the moment that the revisionists' argument is valid, why don't they go just one step further? If all that President Roosevelt thought necessary for his purposes, if all that he was seeking, was "to maneuver the Japanese into firing the first shot," and if MAGIC contained all that the revisionists claim it contained, would it not have been possible, by means of that very MAGIC to accomplish his purpose without such a terrible loss of American lives and, without loss of any of the ships that constituted the apple of the President's eye, the Navy's big battleships? If Roosevelt was so clever a politician and so Machiavellian

in his strategy as to think up a way of maneuvering the Japanese into a position wherein they would be enticed or maneuvered into firing the first shot, should one doubt that he lacked the intelligence to have gone one step further in his thinking and saying something like the following to himself: "Eureka! I've got it. MAGIC will provide the golden opportunity I've sought for so many months. I've hit upon a perfectly marvelous idea and opportunity! An absolutely and amazingly wonderful opportunity! The Japanese have to come to Pearl Harbor to make their surprise attack, an attack clearly indicated by these MAGIC messages. They have to travel several thousand miles, in fact, to get to Hawaii from Japanese waters. If we caught them red-handed, so to speak, near Hawaii and preferably just before the attack, nobody could possibly claim they were on a simple, harmless reconnaissance mission--or on maneuvers. Why, with Japanese-American relations so tense, even if they were caught as many as 500 miles from Pearl Harbor every unbiased critic would say that they really fired first! So I'll bring Kimmel and Short fully into the picture--I'll tell them the story MAGIC is telling us. I'll secretly order them here right away (November 26th, for example) and I'll have Marshall and Stark come in. I'll show Kimmel and Short the crucial messages. Then I'll tell them something like this: Look, my boys, you see now, don't you, what your're in an excellent position to do to the Nips? You see, don't you that this inside and absolutely authentic information says that they are coming from Japan to attack Pearl Harbor by surprise at seven o'clock on the morning of 7 December; they're coming with a task force which will certainly be a pretty big one, you may be sure. It will comprise several

aircraft carriers; they'll have maybe as many as 350 aircraft, including dive bombers, etc., of course. Now as Commander-in-Chief, I direct you to do everything that will be necessary to meet them when or preferably just before they arrive to launch their attack. I direct you to destroy them; knock out the whole task force, carriers, planes, and all, just before they reach Oahu if you can. I direct you, Kimmel, to get all your battleships and, of course, your carriers out of their berthing positions at Pearl Harbor some time during the night, so that there won't be any ships there for them to bomb. And I want all your planes, including those on your carriers, the Lexington and the Enterprise, up in the air before seven o'clock; you'd better get off messages at once to Halsey, Newton, and Brown to alert their task forces; if they're not at Pearl get them back as soon as you can; maybe you'll want to get the Saratoga back from the West Coast to join your other carriers if there's still time, and that's OK with me. Short, I want all your anti-aircraft batteries on shore to be fully manned and with live ammunition at hand, ready for use; I know you don't have too much in the way of fighter and bomber planes but I want you to wipe out as many of their aircraft as possible with what you have. Forget that screwy message you sent about being prepared for sabotage—in view of these messages that's an absurd notion. You can see that the Japs are after our fleet and the protection of the fleet while at Pearl is your job, you know. Be sure your radar is working properly—24 hours a day. I want you, Kimmel, to get your carriers and battlewagons out where they can destroy the Japanese carriers and escort ships while their aircraft are being shot down just before they reach Pearl. This,

my lads, if done well will go down in history as the most thrilling and important battle of all time. Even much more important is the fact that if you knock off their task force and assuming we'll have minimal losses we'll come out far ahead in naval strength because right now our Pacific Fleet is no match for the Japanese Combined Fleet—they've got more ships, faster ships, and with longer-range guns than we have, I'm sorry to say. Now I don't want you to tell anybody I've alerted you because of what MAGIC is telling us. We're reading their most secret diplomatic codes and ciphers, which are all that count now anyhow right now, and it's very important that they don't get suspicious about the security of their Foreign Office communications. I want them to continue using those cryptographic systems because the information we're getting out of them now is priceless and will be even more so in the war which will without question ensue when you've destroyed their task force for Pearl. They won't get suspicious if you will act exactly as though your operations and maneuvers are a routine matter—training—but I want you to be on Alert No. 1. Don't forget that on 17 June 1940, when we thought the Japs and the Germans were about to gang up on us, we sent messages directing our commanders to put our forces at Pearl on a full alert, and you did so; that time, fortunately, nothing happened. We were probably jumping at conclusions then, but now it's different—now we've got this MAGIC. You'll have to go at this carefully, of course, so as not to alarm the Japs and lead them into calling the whole thing off, which they still can do, as we understand their plan. But the important thing is to keep from doing anything that will alarm them and make them call the whole thing off.

I want them to fire the first shot. I'm sure you can think up ways to work up to a condition of full alert so that they'll not get suspicious. That might precipitate an "incident" and give the Japs an excuse to say that we committed the first overt act. Besides we don't want to alarm the civil population, of course. Everybody knows that relations between Japan and ourselves are very tense right now, so that exercises and maneuvers of a defensive type will certainly be regarded as only logical and the natural thing to do. Now I suggest that you get back to your posts as fast as you can--you've got only a few days to prepare a real surprise for the surprise they think they're going to spring on us. Let's see how well you can knock 'em off. Give 'em hell! So long, and the best of luck to you. About 150 million Americans will probably never know how much they will owe you two for what I'm sure you'll be able to do, even with what little you have. I wish you had more--but you know what the trouble is. I don't have to tell you. It's enough merely to remind you that the Selective Service Act was extended in the House just a few months ago by a majority of just one vote."

On 3 December the President (in this imaginative account) sends a message to Kimmel and Short telling them that we've deciphered a long message from the Japanese Consul, Kita, in Honolulu to Tokyo. "Kita is the Jap whose been giving them the dope about ships in harbor; he's the one whose been sending Tokyo the detailed story of what ships are anchored where. But from this 3 December message it's clear that somehow Kita has figured out, or maybe somebody in Tokyo has figured out, that it would be a terrible denouement to come all the way from Japan to make their surprise

attack only to find that the 'birds had flown the coop.' So Kita has figured out a plan whereby he and his spies in and around Pearl can send last word to the Japanese Attack Force Commander that everything is OK, that the important elements of the U. S. Fleet are still in their berthing positions, and haven't suddenly departed just a few hours before the attack is scheduled to commence." (See Message from Kita to Tokyo, 3 December 1941, p. 267 of Part 12, PFR, a message which by the way was not processed until 11 December 1941 but which if there really was a conspiracy would certainly have been done before 7 December.) "Kita doesn't even have the slightest inkling, of course, that I'm telling you, Kimmel and Short, about the set-up he has prepared to make sure to get word to the Japanese task force that the birds haven't flown the coop. You arrange with Naval Intelligence, Army Intelligence and the FBI at Honolulu to grab Kita and Kita's spies on Saturday and hold them in cold storage until after the planned for attack has come off--and has, of course, failed, because it will fail, if you've done your part."

If any reader of this brochure thinks that the foregoing fanciful, imaginative, or conjectural account of what might have happened is too bizarre for serious consideration let me call his attention to what Admiral Kimmel says he could and would have done--if only he'd been "let in on" MAGIC, or at least had been told what was in those messages. Let me quote from his book (pp. 87-88):

No one had a more direct and immediate interest in the security of the fleet in Pearl Harbor than its commander-in-chief. No one had a greater right than I to know that Japan had carved up Pearl Harbor into sub-areas and was seeking and receiving reports as to the precise berthings in that harbor



of the ships of the fleet. I had been sent Mr. Grew's report earlier in the year with positive advice from the Navy Department that no credence was to be placed in the rumored Japanese plans for an attack on Pearl Harbor. I was told then, that no Japanese move against Pearl Harbor appeared "imminent or planned for in the foreseeable future." Certainly I was entitled to know when information in the Navy Department completely altered the information and advice previously given to me. Surely, I was entitled to know of the intercepted dispatches between Tokyo and Honolulu on and after September 24, 1941, which indicated that a Japanese move against Pearl Harbor was planned in Tokyo.

Knowledge of these intercepted Japanese dispatches would have radically changed the estimate of the situation made by me and my staff. It would have suggested a re-orientation of our planned operations at the outset of hostilities. The war plans of the Navy Department and of the Pacific Fleet, as well as our directives and information from Washington prior to the attack, indicated that the Pacific Fleet could be most effectively employed against Japan through diversionary raids on the Marshalls when the Japanese struck at the Malay Barrier. Knowledge of a probable Japanese attack on Pearl Harbor would have afforded an opportunity to ambush the Japanese striking force as it ventured to Hawaii. It would have suggested the wisdom of concentrating our resources to that end, rather than conserving them for the Marshall Islands expedition.

Admiral Kimmel cites instance after instance, message after message, which contained information which, he says, would have been of vital importance to him and would have prevented the disaster if only he had been given the information which he should have received as Commander-in-Chief of the U. S. Pacific Fleet. Maybe, maybe he's right in his contention. His proximity to the scene might have led him to make the imaginative jump that was necessary in order to reach the correct solution to the astounding story that MAGIC was unfolding.

Imagination bogs down when one considers what such a picture as I have conjured up might have been painted from what the Japanese messages were saying—or what the revisionists claim they clearly said.

It is true that in Hawaii there were fewer fighting aircraft, both Army and Navy, than were released from the Japanese carriers when the attack was launched. But the aircraft on the U. S. Navy carriers Lexington and Enterprise, had these carriers been positioned on the basis of the information the revisionists claim President Roosevelt had, would have made up for the lack of aircraft on Hawaii at the time of the attack.

In Admiral Kimmel's story the Admiral makes a few comments on the question of whether his account represents action that he might have taken. But let it be remembered that what he says is based on hindsight; and the Admiral freely admits this point. He contends that had he had the benefit of the intelligence which was in the MAGIC messages and which he never received the story would have been very different (pp. 109-111):

The question will arise in your minds, as it has in mine: Would the receipt of this information have made a difference in the events of December 7? No man can now state as a fact that he would have taken a certain course of action years ago had he known facts which were then unknown to him. All he can give is his present conviction, divorcing himself from hindsight as far as humanly possible, and re-creating the atmosphere of the past and the factors which then influenced him. I give you my views, formed in this manner.

Had I learned these vital facts and the "ships in harbor" messages on November 28th, it is my present conviction that I would have rejected the Navy Department's suggestion to send carriers to Wake and Midway. I would have ordered the third carrier, the "Saratoga," back from the West Coast. I would have gone to sea with the fleet and endeavored to keep it in an intercepting position at sea. This would have permitted the disposal of the striking power of the fleet to meet an attack in the Hawaiian area. The requirements of keeping the fleet fueled, however, would have made necessary the presence in Pearl Harbor from time to time of detachments of various units of the main body of the fleet.

On December 4, ample time remained for the Navy Department to forward to me the information which I have outlined,

and in addition the following significant facts, which the Navy Department learned between November 27 and that date:

- 1) Japan had informed Hitler that war with the Anglo-Saxon powers would break out sooner than anyone dreamt;
- 2) Japan had broadcast her winds code signal using the words "east wind rain," meaning war or a rupture of diplomatic relations with the United States.

Assuming that for the first time on December 5 I had all the important information then available in the Navy Department, it is my present conviction that I would have gone to sea with the fleet, including the carrier "Lexington" and arranged a rendezvous at sea with Halsey's carrier force, and been in a good position to intercept the Japanese attack.

At some time prior to December 6, 1941, the commanders of Hawaii could have been informed of the promise of armed support as detailed by the War Department in London to Air Marshal Brooke Popham in Singapore. This vital information was denied to them.

On December 6, fifteen hours before the attack, ample time still remained for the Navy Department to give me all the significant facts which I have outlined and which were not available to me in Hawaii. In addition, the Navy Department could then have advised me that thirteen parts of the Japanese reply to the American proposals had been received, that the tone and temper of this message indicated a break in diplomatic relations or war with the United States, and that the Japanese reply was to be formally presented to this government at a special hour soon to be fixed. Had I received this information on the afternoon of December 6, it is my present conviction that I would have ordered all fleet units in Pearl Harbor to sea, arranged a rendezvous with Halsey's task force returning from Wake, and been ready to intercept the Japanese force by the time fixed for the outbreak of war.

Even on the morning of December 7, four or five hours before the attack, had the Navy Department for the first time seen fit to send me all this significant information, and the additional fact that 1:00 P.M., Washington time, had been fixed for the delivery of the Japanese ultimatum to the United States, my light forces could have moved out of Pearl Harbor, all ships in the harbor would have been at general quarters, and all resources of the fleet in instant readiness to repel an attack.

For some years I, too, have wondered to what extent Kimmel's statements as to what we could or might have done, had he had or had he been given the information in MAGIC, are guided by hindsight. But having

read his book carefully I feel that it is quite possible that he is warranted in making his statements. The defense of Pearl Harbor was not his responsibility, of course--it was General Short's. But between Kimmel and Short, both capable officers, their closeness to the situation and the greater amount of time they had to think about their duties and responsibilities with respect to safeguarding the Pacific Fleet might have led them to a safe conclusion: that they had better take all precautions to avoid a sudden attack on Pearl Harbor.

One further comment: if, as a result of the inside information the revisionists say we got from MAGIC, all the submarines, destroyers, carriers and battleships in a large task force of the U. S. Pacific Fleet, or even the whole of the fleet had been lying in wait for the Japanese task force sent to make the attack on Pearl Harbor there would have been strength enough, I think, to wipe out the whole Japanese task force. It is true that the Japanese task force included only two battleships, but it had six carriers, two heavy cruisers, a light cruiser, eleven destroyers and a number of submarines, about five, some of which carried midget submarines. (Capt. Harley Cope, USN in "Climb Mount Nitaka," U. S. Naval Institute Proceedings, Vol. 72, No. 12, December 1946.) I say this on the assumption that Admiral Kimmel would have timed his counter-move so that the Japanese task force would not have had the protection of the aircraft of its carriers, because if Kimmel and Short had operated on the basis of information the revisionists claim was clearly in MAGIC the Japanese 361 planes would already have departed on their mission. This I regard as a point of considerable importance. There is reason to

believe that had only a task force of the U. S. Pacific Fleet gone out to engage the Japanese task force in battle on the high seas, the U. S. task force would probably have fared very badly because of the fact that the Japanese not only did have six carriers to our two but also their battleships were faster and had longer range guns. Also, if even the whole U. S. Pacific Fleet had gone out, on the basis of MAGIC--as MAGIC is conceived by the "revisionists"--to meet the Japanese task force which was to attack Pearl Harbor, and had the two navies met on the high seas, with the Japanese carriers still sailing with their entire complement of airplanes, the U. S. Pacific Fleet would probably have suffered a terrible, humiliating and ignominious defeat, because the Japanese task force because of what I have already said--~~they~~ had six carriers to our two, their first-line battleships were speedier and had longer-range guns than any of our own battleships had. Not only would there have been a great loss of American lives, but also none of our battleships or carriers could have been raised and repaired. As it was, and quite fortuitously, there were no carriers at Pearl on 7 December; and with one exception the battleships damaged or sunk at Pearl Harbor were soon back in commission, thanks to an obvious strategic error made by the Japanese high command--they could have but they failed to destroy the dry docks, machine shops, and the repair facilities at Pearl! Why the Japanese overlooked this rather obvious point is not too clear; it shows them to be not too good as naval strategists. Only one Japanese naval officer has thus far tried to explain this strategic error. They, or at least Admiral Yamamoto had the imagination to realize that with the U. S. Fleet in being in the Pacific

their plans for conquest could not be carried to completion very easily; therefore it was necessary to destroy the U. S. Fleet. Dr. Louis Morton in his article "The Japanese decision for war" (U. S. Naval Institute Proceedings, Vol. 80, No. 12, December 1954, p. 1329) says:

Against the almost unanimous opposition of the naval planners, Admiral Yamamoto remained adamant. Unless the American Fleet could be destroyed at one blow at the start of the war, he insisted, the Japanese would probably fail in their effort to seize the Netherland Indies and Malaya. And even if they were successful, he predicted that they would be unable to hold any of their gains for long. . . . A determined effort by the Pacific Fleet might well result in disaster. . . . The Japanese believed it necessary to destroy or neutralize the American Fleet at Pearl Harbor and to deprive the United States of its base in the Philippines.\* America's line of communications across the Pacific was to be cut by the seizure of Wake and Guam.

But that was as far as imagination of Japanese Navy strategists carried them: the only thing they thought necessary was to destroy the U. S. Pacific Fleet. On the other hand, although the U. S. war plans elaborated in the first half of 1941 (<sup>contemplated</sup> in May of that year) took into account the possibility that the Japanese might, (as they had three times before and successfully) begin a war on an enemy without a preceding declaration of war, that is, by a surprise attack, and although this possibility was placed first on the list of contingencies, with Pearl Harbor as the focal point of the attack, and although the war plans even envisioned that such an attack could come from aircraft flown from carriers, it is an almost inexplicable fact that all this was simply forgotten by the end of the same year. The U. S. high command in Washington certainly forgot this

\* Some American naval historians and strategists disagree with Dr. Morton on this point; they insist that the Japanese Navy needed a spectacular victory—the Army was getting too much publicity, and that is why Yamamoto insisted on the Pearl Harbor attack. It was not necessary for their plans to take all that could be taken in Southeast Asia.

contingency; and the two principal commanders in Hawaii, by December 1941, also apparently forgot it—or did they lack the imagination that the January to May 1941 war planners used in thinking up the things that the Japanese might do? In Washington they were thinking only of deterrents to Japanese expansion in the Far East. They imagined that as long as the U. S. Pacific Fleet remained intact in the Pacific it would serve as a deterrent to Japanese moves toward conquest in Southeast Asia. The Japanese attack Pearl Harbor, our greatest overseas bastion? How absurd! Washington, by December 1941, just simply could not imagine that the Japanese would be foolhardy enough to attack Pearl Harbor and try to destroy the ships of Pacific Fleet in their berthing positions in that harbor. Except here and there among the junior officers of the Navy the possibility of a surprise air attack on the Fleet was kept in mind. "A group of the younger officers (on the West Virginia) . . . anticipating an air attack on the Fleet, had discussed among themselves what to do in case it came, and knew exactly how to act." (Morison, S. E. The rising sun in the Pacific, Vol. III of History of United States Naval Operations in World War II, Little Brown and Co., Boston, 1953, p. 103). Their foresight, says Prof. Morison, saved the West Virginia. To repeat, it is true that this contingency about which I have already said a good deal, was explicitly stated in war plans—but apparently nobody seriously believed that it could be done, or that the Japanese would be so foolish as to try it. Indeed, Prof. Morison says of the attack on Pearl Harbor: (P. 132)

Thus, the surprise attack on Pearl Harbor, far from being a "strategic necessity," as the Japanese claimed even after the war, was a strategic imbecility. One can search military history in vain for an operation more fatal to the aggressor. On the tactical level, the Pearl Harbor attack was wrongly concentrated on ships rather than permanent installations and oil tanks. On the strategic level it was idiotic. On the high political level it was disastrous.



## 4. WAS MAGIC WITHHELD FROM KIMMEL AND SHORT AND, IF SO, WHY?

We come now to another very important question which has been raised in revisionist circles: Why did not the commanders at Pearl Harbor get MAGIC; why did they not have the machines and facilities for deciphering the Japanese highest level diplomatic communications, the so-called "Purple" crypto-system? Prof. Ferrell says: "The British and General MacArthur received the Purple decoding machines from Washington; why not the commanders at Pearl Harbor? (p. 225) This is a good question, and not as foolish as it might be made to appear by the usual answer that the authorities in Washington couldn't prevent the Pearl Harbor attack, even with the code, so what would Kimmel and his Army opposite at Hawaii, Lieutenant General Walter C. Short have done with it."

Let us agree that the question raised is not a foolish one but let us consider it in two parts. First, as to why the British got the Purple system. In the autumn of 1940 U. S. military and naval authorities on the highest level agreed that there should and could be some exchange of intelligence between the U. S. and the U. K. Included in the material to be exchanged was communication intelligence. It was ascertained that the U. K. communication intelligence experts had not succeeded in solving the highest-level Japanese diplomatic cryptosystem and the machine which was involved in enciphering and deciphering the messages in that system.

[Nor, parenthetically, had the German experts.] Cryptanalysts of the U. S. Army's Signal Intelligence Service, however, had accomplished this task and were reading the Japanese messages in that cryptosystem, which

they had named, for brevity as well as for disguise, the "Purple" system, its predecessor, also a machine system, having been named the "Red" system. On the other hand, it had been ascertained that the U. K. cryptanalysts, although they had been unsuccessful with the "Purple" system, had been quite successful with certain German and Italian diplomatic cryptosystems the study of which had only recently been undertaken by U. S. cryptanalysts. It therefore seemed that both the U. S. and U. K. could profit by some sort of exchange. A team of four cryptanalysts, two from the Army and two from the Navy, was sent to London in January of 1941 to discuss the technical aspects of an exchange of material. The U. S. team took with it a recently-completed "Purple" machine and the data necessary to use it in deciphering the Japanese messages. It is very important to understand that the British had not only extensive facilities for intercepting and forwarding Japanese diplomatic traffic to London but they also had a corps of very competent cryptanalysts and Japanese translators--without whom possession of the "Purple" machine would have been of little or no value. The British also were able to read and translate other systems carrying Japanese diplomatic traffic--and they did so not only in London but also at Singapore and Hong Kong, and possibly in one or two other strategic spots under the British Crown.

In the exchange of the "Purple" machine and informational details concerning the Purple system for specific technical data on certain German and Italian cryptosystems (principally diplomatic) both the U. S. and the U. K. gained advantages of inestimable value. On this point there never has been any doubt on either side. Moreover, this exchange paved the way

to a later complete U. S. - U. K. collaboration in cryptanalytic operations after the U. S. entry into World War II as one of the belligerents. The value of this collaboration can hardly be overestimated but this brochure will not deal with this aspect.

As long as we are dealing with the question about the U. S. delivery to the British of a "Purple" machine and the cryptosystem which used it, we may well go into a related question concerning which little has been said in the torrent of words about the Pearl Harbor disaster. The British acquired the "Purple" in January 1941, and were able from the very first to use it--no strings were attached to this usage, except that the secret would be treated with the care that it deserved in order to keep from enemy knowledge the fact that we had solved it. (There have always been very detailed and strict regulations governing the handling of communications intelligence and in time the U. S. and U. K. regulations became identical). The reason for mentioning that there were no strings attached to the U. S. gift to the British is to forestall a revisionist allegation that President Roosevelt must have permitted the gift to be made only on condition that no information coming from "Purple" would be used by the British in a manner that would interfere with his conspiracy to withhold from the two commanders at Pearl Harbor whatever intelligence they might obtain which would prevent the Japanese taking them by surprise. Such an allegation would, of course, be absurd on its face--but then the revisionists do not always argue in a logical manner. Exactly why the British would, even if they could have agreed, to keep "Purple" intelligence from Short and Kimmel is hard to understand. In the first place, although there

was no direct communication between these commanders and the British, certainly, there was communication between British and American intelligence authorities in the Far East. In the second place, let it be noted that the British had been able to read and were reading Japanese diplomatic systems other than Purple; in fact, many of the messages which the revisionists claim most definitely indicated that a surprise air attack was to be made at Pearl Harbor were in cryptosystems other than Purple. For example, the so-called "bombing plot" message was not in "Purple" at all but in a system held by consulates, a system designated by us as J-19; and several other messages related to the bombing plot message were in the same system.

What has all the foregoing to do with the British? Simply this: is it conceivable that the British, too, would have participated in a conspiracy of silence so as to let the Japanese destroy the U. S. Pacific Fleet, the fleet that was their principal protection against Japanese aggression in the Far East? Hardly. Is it not clear that the various messages in Purple and in the other Japanese systems conveyed to the British no definite statement as to an impending attack on the American bastion in the Hawaiian area? The British, let us remember, were then supposed to have the finest and most carefully trained intelligence experts in the world. Is it likely that the detailed story of an impending attack, if revealed by MAGIC, would have been completely overlooked by their experts? Is it conceivable that they would, if they saw the outlines of the story, have kept it to themselves? That they would have kept it from their U. S. friends? That they would have seen to it that no word of it

leaked to Short and Kimmel? The British were counting upon the U. S. to protect British interests in the Far East.

In the foregoing paragraphs it was stated that certain Japanese messages were long-delayed in their processing into plain English by the Army and Navy cryptanalytic units. These delays were caused by several things: (1) there were so many messages to be forwarded from U. S. intercept stations that U. S. radio facilities were then not equal to the task of carrying them all; many had to be sent by air mail pouch or even by ordinary U. S. Mail pouch; (2) there were so many messages and so few persons capable of processing them in Washington--let us not forget that a few dozens of persons in Washington were trying to keep up with what hundreds, perhaps thousands, of Japanese were doing in Japanese message centers in Japanese embassies, legations, and consulates all over the world; (3) there were many times when it was impossible to solve a new key until a sufficient amount of traffic had accumulated; (4) there were many cases when decrypting a message was stymied by errors in transmission or interception; (5) there were only a handful of persons in both the Army and the Navy cryptanalytic units who could translate Japanese--and no pool in the U. S. from which trained and trustworthy Japanese translators could be selected, as is the case in other foreign languages such as French, German, Spanish, etc.; and until the Japanese was converted into English, the messages containing useful intelligence about Japan might just as well be filed in the waste basket.

While we dwell upon the foregoing elements in the story it might be a good place to point out that a conspiracy to withhold information in

order that an attack might be carried out could hardly afford to risk certain contingencies. For instance, it would be essential, would it not, that a high degree of priority in processing be accorded all Japanese Government messages going to or coming from Honolulu, so that the alleged conspirators themselves might not be caught napping? But it is a fact that several very important messages having a direct bearing on the situation were not processed until several days after the attack. The very fact that the processing of all messages to and from Honolulu was not given the highest or even a high priority itself constitutes an argument against the alleged conspiracy being objective—and not completely subjective.

Let us now take up the question about the withholding of MAGIC from Admiral Kimmel and General Short—as viewed by the highest level authorities in Washington. First of all it is easy to admit the fact that the critical MAGIC messages of the early autumn of 1941 and up to the day of the attack were withheld from them; there can be no question whatever about this fact. But the important point is why? The revisionists say that it was necessitated by the Roosevelt-Marshall-Stark conspiracy to bring about the attack on the Fleet at Pearl Harbor. A dispassionate view, however, must take into consideration quite different and more logical factors. First, as the Purple messages continued to be read in Washington the strategic value of our solution of that cryptosystem became increasingly apparent. This is a good place to insert what General Marshall had to say on the subject of the value of MAGIC, which he described in detail in a highly secret letter he wrote to Governor Dewey, a

Republican, who had learned about MAGIC (nobody knows how or from whom).  
 Marshall had learned that Dewey was proposing to use this highly explosive  
 information in the 1944 Republican Presidential campaign against a fourth  
 term for Roosevelt. The war was not over! Here it is, in extenso:

Extracted from CONGRESSIONAL INVESTIGATION PEARL HARBOR ATTACK,  
 Part 3, pp. 1132-1133.

[2987D]

[Copy]  
~~TOP SECRET~~

For Mr. Dewey's eyes only.

27 September 1944.

My dear Governor: Colonel Clarke, my messenger to you of yesterday, September 26th, has reported the result of his delivery of my letter dated September 25th. As I understand him you (a) were unwilling to commit yourself to any agreement regarding "not communicating its contents to any other person" in view of the fact that you felt you already knew certain of the things probably referred to in the letter, as suggested to you by seeing the word "cryptograph," and (b) you could not feel that such a letter as this to a presidential candidate could have been addressed to you by an officer in my position without the knowledge of the President.

As to (a) above I am quite willing to have you read what comes hereafter with the understanding that you are bound not to communicate to any other person any portions on which you do not now have or later receive factual knowledge from some other source than myself. As to (b) above you have my word that neither the Secretary of War nor the President has any intimation whatsoever that such a letter has been addressed to you or that the preparation or sending of such a communication was being considered. I assure you that the only persons who saw or know of the existence of either this letter or my letter to you dated September 25th are Admiral King, seven key officers responsible for security of military communications, and my secretary who typed these letters. I am trying my best to make plain to you that this letter is being addressed to you solely on my initiative, Admiral King having been consulted only after the letter was drafted, and I am persisting in the matter because the military hazards involved are so serious that I feel some action is necessary to protect the interests of our armed forces.

I should have much preferred to talk to you in person but I could not devise a method that would not be subject to press and radio reactions as to why the Chief of Staff of the Army would be seeking an interview with you at this particular moment. Therefore I have turned to the method of this letter, with which Admiral King

concur, to be delivered by hand to you by Colonel Clarke, who, incidentally, has charge of the most secret documents of the War and Navy Departments.

In brief, the military dilemma is this:

The most vital evidence in the Pearl Harbor matter consists of our intercepts of the Japanese diplomatic communications. Over a period of years our cryptograph people analyzed the character of the machine the Japanese were using for encoding their diplomatic messages. Based on this a corresponding machine was built by us which deciphered their messages. Therefore, we possessed a wealth of information regarding their moves in the Pacific, which in turn was furnished the State Department—rather than as is popularly supposed, the State [2987E] Department providing us with the information—but which unfortunately made no reference whatever to intentions toward Hawaii until the last message before December 7th, which did not reach our hands until the following day, December 8th.

Now the point to the present dilemma is that we have gone ahead with this business of deciphering their codes until we possess other codes, German as well as Japanese, but our main basis of information regarding Hitler's intentions in Europe is obtained from Baron Oshima's messages from Berlin reporting his interviews with Hitler and other officials to the Japanese Government. These are still in the codes involved in the Pearl Harbor events.

To explain further the critical nature of this set-up which would be wiped out almost in an instant if the least suspicion were aroused regarding it, the battle of the Coral Sea was based on deciphered messages and therefore our few ships were in the right place at the right time. Further, we were able to concentrate our limited forces to meet their naval advance on Midway when otherwise we almost certainly would have been some 3,000 miles out of place. We had full information of the strength of their forces in that advance and also of the smaller force directed against the Aleutians which finally landed troops on Attu and Kiska.

Operations in the Pacific are largely guided by the information we obtain of Japanese deployments. We know their strength in various garrisons, the rations and other stores continuing available to them, and what is of vast importance we check their fleet movements and the movements of their convoys. The heavy losses reported from time to time which they sustain by reason of our submarine action, largely result from the fact that we know the sailing dates and routes of their convoys and can notify our submarines to lie in wait at the proper points.



The current raids by Admiral Halsey's carrier forces on Japanese shipping in Manila Bay and elsewhere were largely based in timing on the known movements of Japanese convoys, two of which were caught, as anticipated, in his destructive attacks.

You will understand from the foregoing the utterly tragic consequences if the present political debates regarding Pearl Harbor disclose to the enemy, German or Jap, any suspicion of the vital sources of information we possess.

The Roberts' report on Pearl Harbor had to have withdrawn from it all reference to this highly secret matter, therefore in portions it necessarily appeared incomplete. The same reason which dictated that course is even more important today because our sources have been greatly elaborated.

[2987F] As another example of the delicacy of the situation, some of Donovan's people (the OSS) without telling us, instituted a secret search of the Japanese Embassy offices in Portugal. As a result the entire military attache Japanese code all over the world was changed, and though this occurred over a year ago, we have not yet been able to break the new code and have thus lost this invaluable source of information, particularly regarding the European situation.

A further most serious embarrassment is the fact that the British government is involved concerning its most secret sources of information, regarding which only the Prime Minister, the Chiefs of Staff and a very limited number of other officials have knowledge.

A recent speech in Congress by Representative Harness would clearly suggest to the Japanese that we have been reading their codes, though Mr. Harness and the American public would probably not draw any such conclusion.

The conduct of General Eisenhower's campaign and of all operations in the Pacific are closely related in conception and timing to the information we secretly obtain through these intercepted codes. They contribute greatly to the victory and tremendously to the saving in American lives, both in the conduct of current operations and in looking towards the early termination of the war.

I am presenting this matter to you in the hope that you will see your way clear to avoid the tragic results with which we are now threatened in the present political campaign.

Please return this letter by bearer. I will hold it in my most secret file subject to your reference should you so desire.

Faithfully yours,

(Sgd) G. G. MARSHALL.

It seems to me that the foregoing letter goes a long way toward answering the question as to why MAGIC was withheld from Kimmel and Short. Stated briefly, the authorities in Washington were fearful that if MAGIC continued to be sent them the secret that we were able to read all their diplomatic cryptocommunications, including "Purple", their most secure system, would soon find its way to the Japanese. The whole of the island of Oahu had thousands of Japanese nationals, among whom it was natural to assume there were—there must have been—plenty of spies. The Army and Navy authorities in Washington felt that it was becoming too dangerous to the continued secrecy of the fact that we had solved and were reading messages in Purple to send any more of the messages to Kimmel and Short. Of course they could have been sent some gists—as had been done in the first half of 1941—but General Sherman Miles, the then Assistant Chief of Staff for Military Intelligence, stated before the Joint Congressional Committee that sending even gists would have been dangerous, by overloading the radio circuits; and he went on to say that while the Navy cryptosystems could have been used, because they were more secure than the Army's, even that would not remove the danger altogether. [I will interject at this point the statement that General Miles was not too well-informed on these practical matters, because <sup>use the Navy</sup> had adopted and was using an Army cryptosystem and a machine invented by Army personnel!] Both the Army and the Navy's cryptosystems could and would have stood up under the strain of sending all the important MAGIC messages to Kimmel and Short and in extenso.

But, insist the revisionists, the Navy furnished a MAGIC machine and information on how to use it to the Commander of the 16th Naval District—the Philippines. Why not to Kimmel and Short? There were very good reasons for this; but at this point we shall merely ask: did possession of MAGIC prevent General MacArthur from being taken by surprise and losing all his planes at one fell swoop more than 12 hours after the General knew of the Japanese attack on Pearl Harbor? General MacArthur blames his chief of the Army Air Corps forces in the Philippines, General Brereton, for being caught napping; and Brereton blames MacArthur. Possession of the Purple machine alone obviously was not sufficient—the interpretation, appreciation, and evaluation of MAGIC is just as important. It might be useful to quote what General Willoughby, MacArthur's G-2, said on this latter point in an affidavit dated 8 May 1945 (PHR, Part 35, p. 87) in protecting the Navy's monopoly of MAGIC:

In 1941 the Navy obtained and maintained a highly efficient crypto-analytical service, specializing in Japanese material; though the Army had notably participated in the development of this subject, the Navy appears to have obtained a lead; consequently, it can be said that the Navy enjoyed on almost monopolistic privilege. In an otherwise meritorious desire for security (though every modern nation knows that crypto-analysis is going on), the Navy has shrouded the whole enterprise in mystery, excluding other services, and rigidly centralizing the whole enterprise. At this date, for example, this same system is still in vogue: as far as SWPA is concerned, the crypto-analysis is made in Melbourne, forwarded via 7th Fleet D.N.I.; the Melbourne station is under direct orders of Washington, is not bound by any local responsibilities, forwards what they select, and when it suits them. The possibility of erroneous or incomplete selection is as evident now as it was in 1941. The only excuse the Navy has is that its field is primarily naval intercepts, but there is a lot of Army traffic or other incidental traffic. This collateral traffic is not always understood or correctly interpreted by the Navy, in my opinion.

The solution to this vexing and dangerous problem is a completely joint, inter-locking intercept and crypto-analytical service, on the highest level, with the freest interchange of messages and interpretation.

The sequence of messages referred to, had they been known to a competent intelligence officer, with Battle Order and tactical background, beginning with November 14th, would have led instantly to the inescapable conclusion that Pearl Harbor naval installations were a target for attack, with November 25th or November 29th as the deadlines, suggesting irresistibly that elapsed time was involved, for some sort of naval seaborne sortie.

C. A. Willoughby,  
C. A. Willoughby,  
Major General, G. S. C.,  
Asst. Chief of Staff, G-2,  
General Headquarters, SWPA.

The fact is that skilled cryptanalytic help and skilled Japanese translators were not in sufficient supply to permit either the Army or the Navy to maintain many such people anywhere outside the U. S.—they were badly needed in Washington. And besides, nobody thought or even imagined that they were so badly needed at Pearl Harbor as at Manila—the Japanese would never be so foolhardy as to attack Pearl! The U. S. Navy authorities believed that the Philippines might be cut off—but not Hawaii. Manila needed MAGIC much more than Pearl! That explains why there was a Purple machine in Manila, more than anything else. The Navy communications personnel at Pearl were assigned the mission of trying desperately to solve the important Japanese naval cryptosystems and to get what information could be gleaned from traffic analysis of Japanese communications; the Army had no signal intelligence or cryptanalytic personnel at all in Hawaii after 1939—the very small unit it did have in Honolulu was brought back to Washington after but one year's operations there—because the few trained persons of that unit were thought

to be much more useful in Washington. Hawaii seemed to be the last place the Japanese would try to attack! Why keep the few trained cryptanalytic personnel there when they could be so much more useful in Washington? What the Army had, therefore, was simply an intercept unit directed to listen in on certain assigned Japanese circuits and to forward the traffic to Washington for study.

In this decision to bring back to Washington that small Army cryptanalytic unit (two or three persons at most!) I am quite sure that the Chief Signal Officer consulted no higher authority—and, I am sure too, the Commanding General of the Hawaiian Department at that time, General Short's predecessor, was glad to get rid of the unit—its maintenance caused him difficult logistical problems. The secrecy of its operations certainly was a source of irritation to him and his staff—they never got to see the results. The trained Signal Corps officer the Signal Intelligence Service in Washington sent to Hawaii in 1940 performed no signal intelligence functions; by direction of the local commander he was soon given "more necessary" duties, such as devising and supervising the laying of communication cables in and around Honolulu. And with this decision I can take no exception—the Commanding General on the spot knew best what he needed. I know for a fact that when the Signal Corps sent a very small unit to Corregidor it was only with the greatest difficulty that the Commanding General there was finally persuaded to let the unit do what it was sent out to do—but only for a short time. The members of any Signal Intelligence unit (Signal Corps personnel) were badly needed for ordinary Signal Corps functions. Washington could do

very little about this--the local commander decided. In all that I have said above, however, the most important point by far was, so far as concerned both the Philippines and Hawaii, that an attack by the Japanese was too fantastic to warrant much thought, so preparations for a possible attack were somewhat neglected.

## 5. THE "WINDS CODE MESSAGES"

Many thousands of words have been expended in discussing and writing the story of the so-called "Winds Code Messages," and, in particular, whether there were any authentic "Winds Code Execute" messages.

There were two "Winds Code" set-ups, which were intended, for reasons peculiar to the Oriental mentality, to give a certain kind of warning but just exactly what kind of a warning is unclear because both of these "set-ups" were, to say the least, impractical, indeed quite foolish, because they were so susceptible of being confused with ordinary weather and news broadcasts. And, indeed, this is exactly what did happen with regard to the one of most interest to the U. S. A weather broadcast—now termed the false "Winds Code Execute" message was intercepted—and for a few hours at any rate was taken to be the real thing. But it wasn't "the real McCoy"—it resembled what the Execute message might have been but when carefully scrutinized it just didn't meet all the conditions specified in the code instructions. The alarm it set off subsided as soon as the discrepancies with what a real Execute should be were recognized.

I think that one thing was established conclusively after exhaustive investigation by several of the Pearl Harbor boards, including that of the Joint Congressional Committee: the Japanese never did send out an authentic "Winds Code Execute" message which clearly indicated that Japan was going to attack the U. S. If indeed the Foreign Ministry intended to transmit such a message it was forgotten at the last moment; and even if

it had not forgotten, the most the message could have conveyed was that there was going to be a break in relations between Japan and the country signified by the particular "Winds Code Execute" message. The other thing which seems to be certain is that having forgotten to send out the "Execute" meaning a break between Japan and the U. S., somebody seems to have remembered to send out after the attack on Pearl Harbor a "Winds Code Execute" signifying that Japan was breaking relations with Britain but not with the U.S.S.R. Even this one the Japanese who were interrogated after the surrender of Japan denied having transmitted but all the evidence I have examined indicates that they were not telling the truth. One might say, if they didn't tell the truth about that one we should not put any credence in their denial that a "Winds Code Execute" was sent out on 3 December, the one indicating a break in relations (or war) with the U. S. Certain of the Japanese interrogated on the point denied ever setting up the "Winds Code" in the first place. This point is examined in great detail in Appendix E to PIR, pp. 467-486 and there is consummate skill in this examination. The PIR arrived at the following conclusion, which I think represents the last word that can be said on this subject (p. 486):

**CONCLUSION:** From consideration of all evidence relating to the winds code, it is concluded that no genuine message, in execution of the code and applying to the United States, was received in the War or Navy Department prior to December 7, 1941. It appears, however, that messages were received which were initially thought possibly to be in execution of the code but were determined not to be execute messages. In view of the preponderate weight of evidence to the contrary, it is believed that Captain Safford is honestly mistaken when he insists that an execute message was received prior to December 7, 1941. Considering the period of time that has elapsed, this mistaken impression is understandable.



Granting for purposes of discussion that a genuine execute message applying to the winds code was intercepted before December 7, it is concluded that such fact would have added nothing to what was already known concerning the critical character of our relations with the Empire of Japan.

This conclusion reached in 1946 remains unshaken to this day--nothing has turned up to make a change in it desirable, so far as concerns any "Winds Code Execute" message that might have been transmitted on 3 December, as Captain Safford contended. One could only wish that the conclusion had stated categorically that there was such a message in regard to a break in relations between Japan and the British (and also the Dutch East Indies) because the evidence is clear that such a signal was sent--but then, by that time, 8 December, the attack on Pearl Harbor was finished.

The "revisionists," however, still believe in Captain Safford--the sole person who stuck to his statement that there was a 3 December warning, and that all copies of that message were deliberately destroyed. The interesting thing about this whole tempest-in-a-teapot is that even if there had been an authentic U. S.-Japan execute message it would have told us nothing whatever that was <sup>not</sup> already known on 3 December. Moreover, and this I think is very important, the attack on Pearl was prepared for with so much secrecy I would doubt very much that the Japanese would take any chance whatever in sending out a message which might "tip their hand". It just doesn't fit in the picture at all.

It is interesting to note that Admiral Kimmel, while he mentions the "Winds Code" affair and cites (p. 100) what the Naval Court of Inquiry said about it--later proved to be wrong--does not press the

matter to seriously. I think the Admiral is very dubious that a real Execute was ever sent out on 3 December as claimed by Captain Safford, although he does say (p. 101): "The findings of the Naval Court of Inquiry on this subject are confirmed by the evidence presented to the joint congressional investigating committee." The Admiral does not state specifically what the "findings" were but the reader is left to conclude that the committee found that there was an Execute transmitted on 3 December and that it was intercepted by us—but the information was not transmitted to him or to other commanders afloat.

Senators Ferguson and Brewster in their Minority Report say (p. 526): "Even if the wind execute message they saw was a false one they believed it true at the time and should have acted accordingly." A good point, and I think, one that should be emphasized; it is too bad it wasn't followed up regardless of any other considerations.

## 6. THE QUESTION OF SABOTAGE

What led General Short to prepare for sabotage rather than for military action by the Japanese?

In my opinion the reason for General Short's very brief answer to the war warning message sent him after the 26 November 1941 American rejoinder to Japanese proposals for arriving at a modus vivendi was not, as many people believe, utter nonsense. Short said merely that he was prepared for sabotage. The fact is that everybody in Washington and, apparently, also in Honolulu had but two things in mind as to possible or probable Japanese action. First, the Japanese march was certainly to be to the southward (to Malaya, Thailand, Indo-China, Borneo, or the Dutch East Indies; indeed all their actions seemed to point in those directions) and Short was not able to do anything at all about that. Then, secondly, there was incessant talk in America, including in the radio broadcasts and in the writings of columnists, sabotage was what we had to guard against. The generally-held view was that the Japanese were tricky, that attempts to thwart their march would be countered by the various mechanisms of sabotage. This I remember very vividly. And I feel sure that when General Gerow received General Short's message stating that all steps to prevent sabotage had been taken and that he was in liaison with the Navy, General Gerow probably thought "Fine business—Short's on the job." So must have the others in Washington who saw it—General Marshall included. By hindsight Short's message seems entirely unresponsive to the message sent him. But the matter of

sabotage was in the air. That's what we had to look out for. Confirmation of this attitude can be seen in various messages. Even the Navy's strong message beginning "This dispatch is to be considered a war warning" ends with "Continental Districts Guam Samoa directed to take appropriate measures against sabotage." Everybody had forgotten all about the war plan of May 1941 which envisaged as the first and most dangerous contingency a surprise air attack on the Fleet at Pearl Harbor. Parenthetically I may add that those whose memories of World War I included the two great acts of sabotage by German agents in this country (the Black Tom explosion and the Kingsland Fire) before the U. S. became a belligerent in that war will perhaps agree with me that Japanese sabotage was the thing Americans thought was most to be feared in regard to American territory. Let us not forget that this fear quickly expressed itself very clearly and heartlessly in what was done to thousands of Japanese-American citizens (including Nisei) in California the moment we declared war on Japan. Why did they move them out of the port cities? What were the authorities afraid of? Sabotage! For this reason I, for one, find it difficult to criticize General Gerow in his handling of General Short's message in response to the 26 November message from Washington.

But what about the views held by U. S. intelligence authorities on this question of sabotage? Were they the same as those of the average American citizen, "the man-in-the-street"? I think they were—and just as the views of "the man-in-the-street" of those days were wrong, so it seems were the views of our intelligence authorities. Why? Because we never have paid too much attention to intelligence. After several

thousands of years of experience, why do military and naval authorities seem to pay less attention to intelligence than to logistics, for instance? Why does intelligence have to play the role of step-child in the conduct of warfare? What is there about intelligence that makes it less desirable as a career than artillery, for example? The reasons are clear when one looks into the matter.

Admiral Theobald lays great emphasis on Tokyo to Honolulu message number 83 of 24 September 1941 (the so-called "Bombing Plot Message") and says (p. 46):

After studying Tokyo dispatch #83, no military intelligence organization could fail to reach that deduction /that it was to prepare the detailed plan for a surprise attack on the major units of the Fleet moored there/.

Here I think is the kernel of the nut--the secret of why the U. S. was taken by surprise. I have underlined the phrase "no military intelligence organization" in the foregoing extract because I think that our military and naval intelligence organizations had serious defects at that time--and I think they still have. (Theobald does not mean just military, U. S. Army Intelligence, but also U. S. Navy Intelligence.) I think that serious defects in our military and naval intelligence made it possible for the Japanese to take us by surprise at Pearl Harbor. A strong statement? Yes, but I think it is warranted. I will with some diffidence go into this question because I do not know too much about the situation as of 1957. I did know what it was like in 1940-41 and in 1950, four years after the PFR was released. It is clear that the intelligence situation in the U. S. was defective in 1940-41 and in 1950, when the Korean "police action" broke out without warning. Where

were our intelligence services then? What were they doing or thinking about? By 1950 we had CIA. What help was CIA?

Four years after the PHR was released, Major General Sherman Miles, Assistant Chief of Staff for Intelligence of the War Department General Staff, from April 1940 to February 1942, in what some people may regard as an apologia, has many things to say in an endeavor to explain what appear to have been derelictions of himself and his staff.<sup>1</sup> It was an attempt to absolve G-2 from its responsibility for the debacle on 7 December 1941. For the most part he does as good a job of this, perhaps, as could be done to exculpate G-2 from its failures, omissions, and lack of the kind of imagination which might have foreseen and forestalled the disaster caused by the Japanese surprise attack. A salient paragraph among many which could be quoted is the following (p. 71):

The plain fact is that the war warnings sent out by the highest military authorities nine days and more before Pearl Harbor were far more authoritative and more definitive of what the Hawaiian commands might expect, and what was expected of them, than any information or interpretations from "magic" that Military or Naval Intelligence could possibly have sent. Complete reliance was placed on the effect those warnings should have had—and did have everywhere except in Hawaii. But Tokyo apparently believed that the incredible might happen and Hawaii be surprised: Washington did not.

General Miles takes it for granted that the warnings sent out by Washington properly alerted all our overseas commands except the one in Hawaii. One wonders about the basis for the General's assumption in this regard. Indeed, in one case, already mentioned, even 12 hours after General MacArthur in the Philippines knew that the Japanese had made the

1 - "Pearl Harbor in retrospect" in the Atlantic Monthly for July 1943, pp. 65-72.

surprise attack at Pearl Harbor his command was nevertheless taken completely by surprise, when the Japanese destroyed all his planes on the ground, just as they did in Hawaii. General Miles, notwithstanding his statement that (p. 70):

"The Hawaiian commands later complained that this "magic" information was not transmitted to them--this in spite of their failure to react to the authoritative warning orders sent them when the situation was commonly known to be far more critical. By comparison, it may be noted that General MacArthur, who had access to "magic," could not later identify the more important "magic" messages; he apparently took no action on them, but alerted his command for war on Washington's warning orders.

Thus assumes that General MacArthur "alerted his command for war on Washington's warning orders." What does "alerting" mean, anyhow, if a commander loses all his planes by what I think was inattention?

General Miles admits (pp. 70-71) that "there were two "MAGIC" messages ... which have subsequently been held to have been sigposts, had we so read them, to Pearl Harbor." The General devotes many words to these two cases and concludes that the sigposts pointed to a half-hearted proposal, admittedly discussed in Washington, that the British and U. S. occupy the Netherland Indies before the Japanese did so--and he thus tried to explain away the famous clue contained in a Tokyo message to Berlin telling General Oshima, the Japanese Ambassador to Germany, to tell the Germans: "Say very secretly to them that there is extreme danger that war may suddenly break out between the Anglo-Saxon nations and Japan through some clash of arms, and add that the time of the breaking out of this war may come quicker than anyone dreams." The explanation of Miles (or, better perhaps, the lack of imagination) on the part

of U. S. intelligence agencies appears to me (even by hindsight, of course) to be pretty thin.

Here are two more paragraphs from General Miles' article, both of which I think are of considerable significance:

The last twenty-four hours in Washington before the bombs fell have come in for much scrutiny. Why did the President, with most of the Japanese final answer before him, conclude that it meant war and then, after a fitful attempt to reach Admiral Stark by telephone, quietly go to bed? Why was he in seclusion the following morning? Why was no action taken on the Japanese reply by the Secretaries of State, War, and Navy when they met on that Sunday morning? Why did they not consult the President, or he send for them? Where was everybody, including my humble self? Why, in short, didn't someone stage a last-minute rescue, in good Western style?

The picture undoubtedly is one of men still working under the psychology of peace. They were, to quote Secretary Stimson again, "under a terrific pressure in the face of a global war which they felt was probably imminent. Yet they were surrounded, outside of their offices and almost throughout the country, by a spirit of isolationism and disbelief in danger which now seems incredible." They were men who thought they had done their possible to prepare for impending war, and who had no idea that there was an innocent maiden in need of rescue.

I will add another extract that may be helpful in seeing things in what I regard as their proper light. This extract comes from Secretary Stimson's statement with respect to the report of the Army Pearl Harbor Board, repeated as a footnote (p. 239) to the PHR:

As expressed by Mr. Stimson: "A keener and more imaginative appreciation on the part of some of the officers in the War and Navy Departments of the significance of some of the information might have led to a suspicion of an attack specifically on Pearl Harbor. I do not think that certain officers in the War Department functioned in these respects with sufficient skill. At all times it must be borne in mind, however, that it is easy to criticize individuals in the light of hindsight, and very difficult to recreate fairly the entire situation and information with which the officers were required to deal at the time of the event." See statement of the Secretary of War with respect to the report of the Army Pearl Harbor Board, committee exhibit No. 157.



My own explanation of the failures and derelictions of U. S. intelligence can be stated in few words: I do not think there were no imaginative officers in G-2 or in Naval Intelligence; but more important there was nobody in either the Army or the Navy intelligence staffs in Washington whose most important, if not sole duty, was to study the whole story which the MAGIC messages were unfolding and which played so important a part in our failure to deduce that the Japanese were planning a surprise attack on the U. S. Fleet at Pearl; there was nobody whose responsibility it was to try to put the pieces of the jig-saw puzzle together. Certainly there was nobody in the Army's Signal Intelligence Service who was assigned to or available for this purpose—even if the responsibility for this sort of work had been fixed on that organization, which it wasn't. This was likewise true of the equivalent Navy organization. This important phase of intelligence was a responsibility which in both services was jealously held by the Intelligence staffs. And the distribution of the MAGIC messages was so rigidly controlled that there was nobody in either of these Intelligence staffs whose duty it was to study the messages from a long-range point of view. The persons, officers and civilians, in intelligence, as well as in the White House, had the messages only for so short a time that each message represented only a single frame, so to speak, in a long motion picture film—a film which should have been shown and should have been intently studied as a continuous series of pictures, because they were telling a story. But the film was simply not there to be studied and this was a very serious weakness, I think, in the intelligence organizations of the two Services. It may have been that they

simply did not have the people to devote to such work.

Of course, there are those critics who point to the message which Navy Captain McCollum testified that he thought should be sent to Admiral Kimmel, and to the one which the Army's Colonel Sadtler testified that he thought should be sent to General Short. They, it seemed, sensed that MAGIC was telling a story and was pointing toward a surprise attack, the most likely target being Pearl Harbor. But both efforts came up against stone walls—their superior officers claimed enough had been sent to put Kimmel and Short on full alert: To send more would only confuse them, or worse than that, irritate them. But the latter were obviously wrong—or so it seems to us now—again by the aid of hindsight. Admirals Theobald and Kimmel have made the most of this failure on the part of those above Captain McCollum and Colonel Sadtler to realize how inadequate the warnings that had been sent to Short and Kimmel really were.

The Joint Congressional Committee (Majority Report) clearly felt that what Kimmel and Short were sent by way of information left much to be desired. One thing seems certain, as I have already said: the intelligence arrangements in both Services were inadequate. The Committee reached certain conclusions and made but five major recommendations, the second of which is as follows:

That there be a complete integration of Army and Navy intelligence agencies in order to avoid the pitfalls of divided responsibility which experience has made so abundantly apparent; that upon effecting a unified intelligence, officers be selected for intelligence work who possess the background, penchant, and capacity for such work; and that they be maintained in the work for an extended period of time in order that they may become steeped in the ramifications and refinements of their field and employ this reservoir of knowledge in evaluating material received.

The assignment of an officer having an aptitude for such work should not impede his progress nor affect his promotions. Efficient intelligence services are just as essential in time of peace as in war, and this branch of our armed services must always be accorded the important role which it deserves.

What has been done about this recommendation by the Services? Very little; in fact, I think it can be said that nothing has been done. Of course, we have the Central Intelligence Agency; but is that establishment really responsive to the Joint Committee's recommendation? I hardly think so. The three services no doubt can cite good reasons why they have not made a professional career in intelligence possible or attractive to its officer personnel; no doubt they can cite at length factors and difficulties that would have to be overcome. All I can say is that judging by what the Army has done the attitude toward intelligence seems not to have changed very much, as is indicated by the following editorial which appeared in the Washington Post on 5 December 1955 and which states the case in succinct terms:

## *Snub to Intelligence* <sup>Post</sup> 5 Dec 55

The recent reorganization in the Army General Staff leaves the Military Intelligence Service in an ambiguous and rather humiliating position. Although directors of the other major staff divisions have been designated as Deputy Chiefs of Staff with the rank of lieutenant general, the Chief of Intelligence remains a major general with the subordinate title of Assistant Chief of Staff.

The extraordinary thing about all this is that not long ago the special task force which investigated the intelligence problem for the Hoover Commission strongly recommended that in the case of those units associated with the three armed services their chiefs "be evaluated in the organizational structure to level of Deputy Chiefs of Staff in the Army and Air Force, and Deputy Chief of Naval Operations in the Navy." This was a rather prolix way of saying that they ought to have a little more prestige and influence, along with a little more gold braid, than they now enjoy. Why, in the case of all three services, was this recommendation ignored by the Department of Defense?

The chief function of military intelligence is to collate and interpret the information provided by the attaches abroad and by other agencies, such as the CIA, the FBI and its own counterespionage service. Correct interpretation requires more than the accumulation of relevant facts; it also requires a considerable knowledge of the psychology of the potential enemy, and this in turn requires an extensive study of his language, history, culture, customs and philosophic tradition, since these afford the keys to such an understanding. But all this, together with the secrecy in which their activities are necessarily cloaked, seems to have made intelligence officers somewhat suspect to a certain sort of politician. Even professional military men are often inclined to discount the value of the critical function exercised by intelligence officers in the discussion of pet military projects or plans.

The question raised by the reorganization is whether we can realistically expect to increase the quality of military intelligence by deemphasizing its significance. It is hard to see how a career in intelligence can be made to appeal to capable officers when the importance of intelligence is so obviously downgraded in comparison with other staff functions.

High-level Army authorities obviously don't think that Intelligence is as important as Personnel, Supply, and similar services. How long will it take before it becomes quite clear to them that Intelligence can be of the greatest help in fighting a war? For too many years intelligence in the Army and in the Navy has been a "deadend" for officers who showed an interest in it, or an aptitude for it. Is this to continue indefinitely? Do the Armed Forces think that the Central Intelligence Agency will or can do the job? Of course, CIA representatives can be assigned to the headquarters of military commands—but will that fill the need? I doubt it, I doubt it very much.

The introductory statement of the "Supervisory, Administrative, and Organizational Deficiencies in our Military and Naval Establishments revealed by the Pearl Harbor Investigation" (p. 253) the PHR begins as follows:

The Committee has been intrigued throughout the Pearl Harbor proceedings by one enigmatical and paramount question: Why, with some of the finest intelligence available in our history, with the almost certain knowledge that war was at hand, with plans that contemplated the precise type of attack that was executed by Japan on the morning of December 7—Why was it possible for a Pearl Harbor to occur? The answer to this question and the causative considerations regarded as having any reasonably proximate bearing on the disaster have been set forth in the body of this report. Fundamentally, these considerations reflect supervisory, administrative, and organizational deficiencies which existed in our Military and Naval establishments in the days before Pearl Harbor. In the course of the Committee's investigation still other deficiencies, not regarded as having a direct bearing on the disaster, have presented themselves. Otherwise stated, all of these deficiencies reduce themselves to principles which are set forth, not for their novelty or profundity but for the reason that, by their very self-evident simplicity, it is difficult to believe they are ignored.

It is recognized that many of the deficiencies revealed by our investigation may very probably have already been corrected as a result of the experiences of the war. We desire, however, to submit these principles, which are grounded in the evidence adduced by the Committee, for the consideration of our Army and Navy establishments in the earnest hope that something constructive may be accomplished that will aid our national defense and preclude a repetition of the disaster of December 7, 1941. We do this after careful and long consideration of the evidence developed through one of the most important investigations in the history of the Congress.

What have the Services done to ameliorate the deficiencies mentioned?

In my opinion, very little. Maybe it would be correct to say "nothing."

As a colleague said to me recently "Nothing will be done--until war breaks out. Then, of course, intelligence is no longer treated a step-child."

Is that what we want? The chances are that there won't be time to use intelligence after a war breaks out: maybe the U. S. will be down and out by that time.

## 7. CONCLUSIONS

After reading some but not all the millions of words alluded to at the beginning of this brochure to what conclusions have I arrived? I will be brief.

First, I must confess, I think that Kimmel and Short were not as culpable as I first thought they were back in 1941-1942, despite all the "warnings" sent them. The Washington authorities were culpable, too—maybe a lot more culpable than were these two officers. Both the Majority and the Minority Reports make good sense. The Report of the Majority contained some very pertinent recommendations—but nobody seems to be doing very much about implementing the second and perhaps the most/<sup>important</sup> of these recommendations; nor has much, if anything, been done about following up on the Conclusions of the Minority, Senators Ferguson and Brewster. In 1946 I thought the latter two senators were "hitting below the belt" but today, in 1957, I think they hit closer to the truth than the Majority. I think Mr. Keefe's "additional views" on the Majority Report make good sense—Kimmel and Short, he said, were not the sole culprits. I think that the Intelligence Services came off rather easily—too easily in the fixing of responsibility and pointing out derelictions. I think the intelligence staffs might have used more imagination but this was not because they were staffed with obtuse officers or persons of low-grade intelligence. As a matter of cold fact, I think, they were badly understaffed, because in both the Army and the Navy "intelligence" didn't count—for much at any rate, then. This raises the question: does it

count for much more today in the Armed Services? I think that Kimmel and Short should have been sent more information—even if they were sent only "gists" of MAGIC—to let them evaluate for themselves the significance of what the Japanese were saying. General Miles says that the warning messages sent them were of far more importance than anything they could have got from "Magic". I don't agree. They might have had more time to ruminate; they might even have guessed—as Admiral Kimmel hints—what the Japanese were planning; our commands might therefore have been much more prepared than they were to meet the attack. This, one must admit, could have been done even without their having a Purple machine or a crypt-analytic staff to solve and translate messages in that or in the other Japanese diplomatic systems.

I think that Admiral Stark was wrong in waiting for General Marshall to be found before sending off a message to Kimmel and Short—and to the other overseas commanders—as soon as the last part of the 14-part Tokyo to Washington message became available—especially when he knew from "Magic" that Kurusu and Nomura were told exactly to the minute when to present the whole message to Secretary Hull. (That we knew the contents of the last part of that message [“deliver this whole message exactly at 1:00 p.m.”] before the Japanese Embassy code clerks had them is a credit to the efficiency of Army and Navy cryptanalytic staffs.)

I think that Colonel Edward French, Chief of the Signal Corps Message Center, used very poor judgment when he sent Marshall's message via commercial radio. He could have used Navy radio or FBI radio—but I am sure he thought it was infra dig to ask a "sister" government radio



service (especially the Navy) to do (at a critical moment) something that Army radio couldn't do. Or maybe Colonel French didn't realize the gravity of the situation, or was not told so in impressive enough language.

The Ferguson-Brewster Minority Report does not point the finger at all the high ranking officials who should share the responsibility but it does say (p. 573) "Both in Washington and in Hawaii there were numerous and serious failures of men in the lower civil and military echelons to perform their duties and discharge their responsibilities. These are too numerous to be treated in detail and individually named." I would have liked them to have named the Directors of Intelligence in the Army and in the Navy, specifically, because I think poor intelligence work played such a large part in the debacle.

And, of course, although it is clear that MAGIC was withheld from Kimmel and Short after the summer of 1941, I do not think (and of this I am quite sure) that it was deliberately withheld for the specific purpose of bringing on the attack at Pearl! Except for the most rabid of the revisionists this is too fantastic a thesis; but there is a stronger argument against such a thesis: it is not supported by the facts.

## 8. EPILOGUE

What was it that so aroused the anti-Rooseveltians, leading them to suspect that it was "skullduggery" and gross negligence in Washington that was responsible for the Pearl Harbor disaster?

Why did the President, his closest associates in the White House, and the officers in the top-level positions in the Army and in the Navy, generate so much suspicion in the minds of the Republicans? Why such reluctance to have an investigation to explain why the U. S. forces were caught by surprise at Pearl Harbor? This is a point which I do not think is explained in the literature and which ought to be. Why did the President and his administration allow so much suspicion to grow up in the minds of the Republicans by the questions which the latter raised after 7 December 1941 and which they continued to raise throughout the war? Could this have been avoided? It is my opinion that it was this refusal to explain, this subjection to continued "needling" of the President and the Democrats by the Republicans throughout the war that aroused the gravest suspicions that there was indeed gross negligence in the White House and at the highest executive levels, and maybe greater derelictions to be hidden. The adamant resistance the President and the Democratic Administration had to maintain against Republican pressure for Congressional hearings on this point and the reasons therefor were quite obvious: we now know that such hearings would have "let the cat out of the bag"—that the U. S. was reading all the Japanese crypto-communications between the Foreign Office and its embassies, legations, and consulates abroad. The Japanese would have changed their Purple system without delay. It

is inconceivable, the Administration believed, that the secret could have been kept even if all the hearings were in Executive Sessions. They felt and were warranted in feeling that Hearings on the subject would be disastrous during the war: too much vital information on the subject would have leaked out. It is true that the Japanese had been alerted during the war by the Germans; they were told, in fact—and nobody knows to this day just how the Germans found out—that we were reading Japanese diplomatic messages. All this appears in the PHR and makes interesting reading. But it is astonishing that even after they were told the Japanese just simply refused to believe the story and continued to use the Purple system. (Neither, for that matter, did the Germans put much credence in the suspicions, forwarded by Marshal Rommel from Africa, that the British must be reading his messages; Rommel felt that this and only this could account for his continuing defeats in North Africa after 1943! Have these two episodes any lessons for us? Yes, indeed! Cryptographers become enamored of their inventions and their minds become polarized in a sort of conviction ~~that~~ that the systems they have concocted are invincible. It happened to us, too! I can remember the mental shock I had when indubitable evidence was placed before me showing that the Germans were reading the enciphered code system we were using for communications between U. S. Army Observer with the British Expeditionary Forces in North Africa in 1942-3 and Washington! That is why I believe that some body—experts, of course—outside the one that thinks up and produces our own cryptosystems but within NSA should be called in frequently to take a good look at those systems to make sure that some crack in the strong cryptosecurity

edifice the NSA cryptographers think they have erected doesn't exist and that such a crack can not be widened.

*William F. Friedman*

WILLIAM F. FRIEDMAN

INVOICE

TO: Director  
National Security Agency  
Washington 25, D. C.  
Attention: Contracting Officer, NSA

In accordance with Article II (Delivery) on Contract No.  
DA49-170-sc-1739, File No. 694-NSA-56, 56-NSA/PR-270,  
this invoice is submitted for payment

..... \$4,000.00

\_\_\_\_\_  
WILLIAM F. FRIEDMAN

CERTIFICATE

I certify that the above bill is correct and just and that  
payment therefor has not been received.

\_\_\_\_\_  
WILLIAM F. FRIEDMAN

Director  
National Security Agency  
Washington 25, D. C.  
Attn: Chief, Central Office of Reference

Sir:

Reference is made to Contract No. DA49-170-sc-1739, File No. 594-NSA-96, 56-NSA/PR-270, which was entered into as of 1 August 1955 by and between the United States of America and the undersigned and which was modified only as to date of delivery of all the items called for under said contract. In accordance with the provisions of Article II (Delivery) of said contract, I am sending you herewith (a) approximately 150 catalog cards supplementary to those sent under Project 1, Article I, paragraph b(1) of said contract; and (b) the completed manuscript called for under Project 3 of the same Article, viz., a special report originally tentatively entitled The Cryptological Background of the Various Official Investigations into the Attack on Pearl Harbor. The said tentative title of the item called for under Project 3 is now not quite suitable and I have deemed it advisable to amend it by prefacing it with the words "Certain aspects of 'Magic'", making the complete title "Certain aspects of 'Magic' in the Cryptological Background of the Various Official Investigations into the Attack on Pearl Harbor."

I have adopted a rather informal style which may perhaps make the brochure more interesting. Several ideas therein cast a new light, I think, on certain aspects of the investigations and the questions raised by a category of historians who have much to say about the attack on Pearl Harbor and who are known as "revisionists." My brochure may therefore be useful in a study of the Pearl Harbor Disaster, especially for historians who take a more realistic view of what happened and why the U. S. forces in Hawaii were caught by surprise. It is perhaps unfortunate that I had to use a small amount of material which is still classified and therefore the brochure as a whole has had to be classified.

I realize only too well that the present brochure can certainly be improved by further work but the time limit—already twice extended—permits of no additional delay in the delivery of this item. Let it be considered, in the words of the previous Director of the National Security Agency, as "Model No. 1."

Sincerely,

WILLIAM F. FRIEDMAN

2 Incls:

W/F

Dec 5 - about 1000 Noyes called Sadtler & said  
 "word is in". "Fus has I'll go right over & tell  
 you." - It was one that means Jap + G.B. - not  
 Jap + U.S. - acc to Sadtler's recall.  
 Noyes called again by Sadtler but couldn't get the word.  
 Sadtler again went to Nubs - Bratton - Kruener. Said

~~Dec 4~~ <sup>1000 - War Com Bd</sup> Thurs a.m. "Gaston incident" - "War in 48 hrs."  
~~Sadtler~~ Sadtler then did not know of winds  
 execute msg.

Tony Muto - Rep of 20th Cent - Fox. Told Sadtler re  
 Chinese rept - Japs would continue neg until ready  
 to strike.

Sadtler never heard w/king of warnings from  
 Australian govt re movements Jap fleet

62-113  
 Notes in  
 conversation with  
 Col. Sadtler evening  
 of 17 Nov 44 at my  
 home. J.

ORGANIZED RESERVES  
 HEADQUARTERS WASHINGTON UNITS  
 Rooms 3602-18 Munitions Bldg.  
 Washington, D. C.

WVMcC-d-ak

November 20, 1934.

SUBJECT: Examination

TO: Major William F. Friedman, Sig-Res.,  
 Office of the Chief Signal Officer,  
 War Department, Washington, D. C.

1. Under date of October 16, 1934, you stated in a 1st Indorsement to this Headquarters that pressure of work had prevented completion of the thesis required in connection with your examination for promotion, and that the completed thesis may be expected about October 31st. The date same has not been received.

2. Information is requested as to the status of this matter.

W. W. McCAMMON,  
 Colonel, Infantry,  
 Senior Instructor.

OCSigO 201-Friedman, W.F.  
 Major, Sig-res.

1st Ind.

3

Friedman, W.F., Major, Sig-Res., OCSigO, Washington, D. C., November 24, 1934 - To: Senior Instructor, Organized Reserves, Washington Units, Rooms 3602-13 Munitions Building, Washington, D. C.

The required thesis in duplicate is being submitted herewith.

William F. Friedman,  
 Major, Signal Reserve.

Attached:  
 Thesis in duplicate.



THE DUTIES OF THE OFFICER-IN-CHARGE OF THE SIGNAL  
INTELLIGENCE SERVICE, GHQ.

Thesis submitted by William F. Friedman, Major, Sig-Rcs.,  
in connection with examination for Certificate of Capacity for  
promotion to the grade of Lieut. Colonel.

	Paragraph
Introductory note as to sources of data . . . . .	1
Basic authority for Signal Intelligence Service . . . . .	2
Position occupied by Signal Intelligence Service in the GHQ Signal Service . . . . .	3
Relations with Radio Intelligence Company, GHQ Signal Service . . . .	4
Organization of the GHQ Signal Intelligence Service . . . . .	5
Functions of administrative section . . . . .	6
Functions of enemy documents section . . . . .	7
Functions of goniometric identification section . . . . .	8
Functions of communications security section . . . . .	9
Functions of secret inks section . . . . .	10
Functions of code and cipher compilation section . . . . .	11
Functions of code and cipher solution section . . . . .	12
Relations with other branches of Signal Intelligence Service . . . .	13
Duties of the officer-in-charge of the GHQ Signal Intelligence Service . . . . .	14
Appendix I	

1. Introductory note as to sources of data. - a. In preparing this thesis the writer has had access to the files of the Chief Signal Officer, including those of current as well as historical information. Among many other documents, the following may be mentioned:

- (1) Tables of Organization, Signal Intelligence Service
- (2) Technical Papers of the Signal Intelligence Section, War Plans and Training Division, Office of the Chief Signal Officer.
- (3) Army regulations pertaining to codes and ciphers.
- (4) Letters pertaining to the work of the Signal Intelligence Service.

b. In addition, files pertaining to the World War, as contained in the World War Records Division of The Adjutant General, have also been studied. Among the latter were the following:

- (1) Final report of the Officer-in-Charge of the Radio Intelligence Section, General Staff, GHQ, A-F (G-2 - A6)
- (2) Final report of the Code Solving Subsection (G-2 - A6)
- (3) Final report of the Cipher Solving Subsection (G-2 - A6)
- (4) Final report of the Goniometric Subsection (G-2 - A6)
- (5) Final report of the Security Subsection (G-2 - A6)
- (6) Final report of the Administrative Subsection (G-2 - A6)
- (7) Final report of the Radio Intelligence Officer, First Army, A-F

2. Basic authority for the Signal Intelligence Service. - a. Basic authority for the establishment of the Signal Intelligence Service is given in AR 105-25; March 15, 1933, as amended by Changes No. 1, August 21, 1934.

Par. 2 e thereof now reads as follows:

"2. Duties of the Chief Signal Officer. - In addition to such other duties as may be prescribed, the Chief Signal Officer will have immediate charge, under the direction of the Secretary of War, of the following:

\* \* \* \*

e. The preparation, publication, revision, storage, accounting, and distribution of all codes and ciphers required by the Army, and in time of war the interception of enemy radio and wire traffic, the geometric location of enemy radio stations, the solution of intercepted enemy code and cipher messages, and laboratory arrangements for the employment and detection of secret inks.

\* \* \* \*

3. Unit signal officers. - a. A chief signal Officer will be detailed for every expeditionary force and a Signal Corps officer as unit signal officer will normally be detailed for each corps area and every tactical unit larger than a brigade containing Signal Corps troops. When no unit signal officer has been so detailed in orders, the senior Signal Corps Officer present for duty with the command will act as such. The unit signal officer will be a member of the staff of his commanding officer. He will be charged, under the direction of his commanding officer, with the command, in so far as relates to operations, of signal troops not assigned or attached to subordinate units. The unit signal officer is also charged with specific duties as follows:

\* \* \* \*

(3) Preparation, publication, storage, accounting, and distribution of codes and ciphers.

\* \* \* \*

(3) Supervision of the installation, maintenance, and operation of the signal communication system, including the message center, of the unit.

(9) Supervision of such activities pertaining to the meteorological, signal intelligence, pigeon, and photographic services as affect the unit."

\* \* \* \*

b. Based upon the foregoing authority, we may now study the following extracts from a directive given the Chief Signal Officer by the Secretary of War, in a letter dated April 24, 1939, dealing specifically with the Signal Intelligence Service:

"5. Upon mobilization the various activities of this service will operate at the following headquarters:

a. Under the War Department:

(1) The preparation of all means of secret communication employed by the Army in peace and war including secret inks, except that, upon its organization, GHQ will begin the preparation of field codes and ciphers required for current replacement for subordinate units.

(2) The interception of enemy communications by electrical means, including the necessary goniometric work incident thereto.

(3) The detection and solution of secret or disguised enemy communications including those written in code, cipher, secret ink or those employing other means for disguise.

b. At General Headquarters:

(1) The preparation of field codes and ciphers for employment by subordinate units to replace those previously prepared under the War Department during peacetime.

(2) The interception of enemy communications by electrical means.

(3) The location of enemy radio transmitting stations by goniometric means.

(4) The detection and solution of secret or disguised enemy communications including those written in code, cipher, secret ink or those employing other means for disguise.

c. At Headquarters of Field Armies:

(1) The interception of enemy communications by electrical means.

(2) The location of enemy radio transmitting stations by goniometric means.

(3) The solution of intercepted enemy code or cipher messages by the assistance of cipher keys and solved codes as furnished by the service at General Headquarters."

3. Position occupied by the Signal Intelligence Service in the GHQ Signal Service. - a. Coming now directly to the manner in which the Signal Intelligence Service fits into the organization of the GHQ Signal Service, we find a graphic picture of the latter organization in T/O 507-# shown in Appendix I.

b. GHQ Signal Service consists of

- 1 Headquarters, GHQ Signal Service
- 2 Operation Companies
- 3 Meteorological Companies
- 1 Radio Intelligence Company
- 1 Construction Battalion

c. In T/O 507-W we are interested only in:

- (1) Headquarters, GHQ Signal Service
- (2) Radio Intelligence Company

4. Relations with Radio Intelligence Company, GHQ Signal Service. - a.

The Radio Intelligence Company, GHQ Signal Service, is the technical agency which intercepts enemy electrically-transmitted traffic and locates enemy transmitting stations by goniometry or radio direction finding. Copies of all intercepted enemy messages and the goniometric data are furnished directly to the GHQ Signal Intelligence Service. Copies of the plain-language messages, if any, are immediately forwarded to the G-2 section of the General Staff.

b. The USA Radio Intelligence Company also intercepts our own radio traffic, for purposes of furnishing information to the Communications Security Section of the GHQ Signal Intelligence Service. This will be discussed in detail under Par. 7 below.

c. The functions performed by the Radio Intelligence Company, GHQ Signal Service, as given under a and b above are performed by a similarly organized Radio Intelligence Company, Army Signal Service; the data obtained are furnished to the Signal Intelligence Service, Headquarters Army Signal Service. This must be mentioned for reasons which will become apparent subsequently.

5. Organization of the GHQ Signal Intelligence Service. - a. Coming now directly to the GHQ Signal Intelligence Service, we find a graphic picture of its organization in T/O 503-W, shown in Appendix I. As shown in the table, this service consists of the following sections:

- (1) Administrative
- (2) Army documents
- (3) Goniometric identification
- (4) Communications security
- (5) Secret links
- (6) Code and cipher compilation
- (7) Code and cipher solution

b. Since T/O 508-W was approved the Signal Corps has been assigned the additional responsibilities of publishing, storing, distributing, and accounting of cryptographic publications. Although these added duties can be allocated to one of the sections of the code and cipher compilation section, it will be noted, nevertheless, that the additional work thus imposed upon the GHQ Signal Intelligence Service is of very great importance and will necessitate some expansion of the present authorized organization.

c. Each of the foregoing sections will be taken up in turn, the duties set forth, the relations with other sections, and all details connected with its efficient operation discussed.

6. Functions of administrative section. - a. The administrative section comprises the following subsections, the duties of which will be described presently:

- (1) Headquarters subsection
- (2) Correspondence subsection
- (3) Reproduction and tabulating machinery subsection
- (4) Files subsection
- (5) Communications subsection
- (6) Guard subsection
- (7) Liaison subsection
- (8) Library and current information subsection

b. The headquarters subsection handles all matters relating to the general policies of the service, the obtaining and administration of personnel, quarters, office equipment and supplies for the service. The officer-in-charge of the GHQ Signal Intelligence Service maintains his office in this subsection.

c. The correspondence subsection comprises the necessary stenographic and typing personnel for conducting the large volume of correspondence of the whole GHQ Signal Intelligence Service. It is deemed best to have a fairly large stenographic and typing pool so that the work may be centralized.

d. The reproduction and tabulating machinery subsection makes copies of texts, tables, etc., required for the various sections. This will include mimeographing, multigraphing, and other methods of reproducing copies. In addition, there will be needed certain machines usually employed for accounting purposes, but easily adaptable to cryptographic and cryptanalytic work. The use of such machines very greatly reduces the amount of time and labor involved in code compilation and in making statistical studies in cryptanalytic work.

e. The files subsection is a central agency for maintaining the files and records of the entire GCHQ Signal Intelligence Service.

f. The communications subsection may have direct telegraph wires to Army Signal Intelligence Service headquarters, to outlying intercept stations, and to other places (for example, Navy Signal Intelligence Service headquarters), for the purpose of avoiding all delays in the transmission and receipt of messages relating strictly to the technical work of this service, especially that of the solution section, where time is of the utmost importance.

g. The guard subsection has supervision of the special sentries assigned to patrol the quarters occupied by the Signal Intelligence Service at all hours of the day and night. It is felt that these special guards are necessary in order to prevent the surreptitious operation of enemy agents in the vicinity of the quarters where most of the vitally secret work is carried on.

h. The liaison subsection maintains the necessary contacts with the Signal Intelligence Services of Field Armies, with other arms, with branches of the General Staff, with the Navy Signal Intelligence Service in case of joint action, and with the Signal Intelligence Services of Allied Governments, if any. In other words, the section serves as a central agency for coordination of work with other Signal Intelligence organizations, or with other agencies concerned in the results obtained.

i. The library and current information subsection maintains a small but fairly comprehensive library of books having a bearing on signal intelligence activities and of books likely to be necessary as sources of information for particular use of the solution section. Files of certain newspapers may be necessary if they are not readily accessible at GCHQ. Reference books of special types are also required for cryptanalytic work that may not be available at the library of GCHQ.

7. Functions of enemy documents section. - a. This section is the depository for documents relating to the signal service of the enemy in all its phases, but primarily as regards his signal intelligence organization, its agencies, operations, systems, and devices.

b. A small unit of translators is essential if the language of the enemy is different from our own. These persons must have some technical knowledge in signal intelligence in order to translate properly such documents in form suitable for our ready use.

c. The translators may also be called upon to assist personnel of the code and cipher solution section and for this reason also they must have a certain amount of training in cryptanalysis.

d. The importance of rapid forwarding of captured documents such as codes, cipher keys, files of cryptographed messages with their translations, to the Signal Intelligence Service is apparent. For this reason a special subsection is deemed advisable, the duties of which are to see that no time will be lost in bringing back captured documents and placing them in proper form for study by various interested personnel of the Signal Intelligence Service.

6. Functions of geometric identification section. - a. The work of this section is primarily of interest to the Battle Order Section of G-2, and to the code and cipher solution section of the Signal Intelligence Service. It assists in enabling the latter to sort intercepted messages properly according to the enemy units from which they emanate and for which they are intended, since tactical messages rarely carry addresses and signatures in plain text, and externally carry few indications from which it may be determined whether two messages are in the same code, in the same cryptographic system, or in the same key.

b. This section works in close liaison with the Radio Intelligence Company assigned to G-2. The latter intercepts the messages and records on them the location of the transmitting stations, as found by intersection from the radio-compass bearings taken on the emitted waves. The geometric identification section records the locations and call signs of these stations on a suitable map, and from a study of intercommunicating stations, establishes the probable enemy radio nets. These nets are then analyzed with the point of view of identifying the units which the transmitting and receiving radio stations serve and this in turn, by noting the groupings which intercommunicating stations form, furnish valuable information concerning enemy order of battle.

c. Having identified the units in this manner, it is then possible to indicate on the intercepted messages the unit from which and to which they are coming and going, their location, the larger units to which they belong, etc. Thus, the messages can be sorted so as to isolate messages in the same cryptographic system, key, or in the same code. This is, of course, of primary importance to, and constitutes an essential preliminary step in solving the messages.

d. From the point of view of furnishing information concerning enemy order of battle, the work of this section is also of great value, since this information may be obtained at comparatively little expense, without entailing the loss of lives, and, moreover, in contrast to similar information obtainable from prisoners or spies, is not subject to psychological, or purposive distortion of the facts.

9. Functions of communications security section. - a. The work of this section is exclusively that of furnishing data for the supervision of our own signal communications from the point of view of their protection and the maintenance of security and secrecy in signal communication.

b. Its duties include the following:

(1) Study of our own messages to insure that the regulations governing cryptographic security are being observed. This involves analyzing radio messages transmitted by our own forces. The messages for this purpose are obtained by the Radio Intelligence Company assigned to CMC and are forwarded to the Communications Security Section of the Signal Intelligence Service. The latter, of course, has the codes or ciphers and decrypts the messages, devoting special attention to violations of the regulations essential to cryptographic security.

(2) Switchboard facilities are provided so that personnel of this section may cut in on important telephone lines and listen in on conversations for the purpose of noting indiscretions which might impair secrecy. Particular attention is devoted to listening for the mention of unit designations, plans of operation, troop movements and the like. It must be assumed that the enemy will attempt to intercept



and record such conversations by placing agents at strategic points suitable for this purpose. Direct tapping of the telephone wires is, of course, not necessary because by suitable apparatus the electrical currents may be detected by induction, amplified, and led away to a place where the conversations may be recorded with ease.

c. The personnel of this section should include a stenographer of considerable ability, so as to be able to record the conversations as rapidly as they are spoken, otherwise the evidence obtained might not be considered valid. All the listening-in personnel must be carefully selected for their discretion and integrity.

d. When serious violations are observed, one of two procedures may be followed. Under the first procedure a letter may be drafted, calling attention to the irregularities, and forwarded through the Adjutant General to the commanding officer of the organization concerned. If the violations continue and are of a serious nature, an inquiry may be held by the Inspector General's Department. Under the other procedure, it has been contemplated that an officer to be known as the Communications Security Officer would be designated in each large unit, whose duties would include the supervision of communications from the point of view of security. If this is the case, the liaison between the G-2 Communications Security Section and the unit security officer would be more direct. This would expedite the correction of irregularities leading to insecurity in communication by radio or other means.

10. Functions of secret inks section. - a. This section maintains and operates a laboratory for the preparation and detection of invisible writing fluids, and for the detection of other means of transmitting information to elude censorship, as for example, microscopic writing.

b. The subsection for preparation of secret inks functions only intermittently, when the G-2 section of G-2 desires to send out secret agents into enemy territory and must provide these agents with means for sending back information in a form that will escape detection by enemy censorship.

c. The subsection for detection functions continuously and is furnished its material by the censorship bureau. Documents suspected of containing invisible writing are passed through the various chemical tests, and if secret

writing is discovered the results of the examination are forwarded to G-2 for action.

d. This section works in closest liaison with the censorship agency, and also with the larger laboratory at the War Department, where better facilities and more personnel are available for research.

11. Functions of code and cipher compilation section. - a. This section comprises the following subsections, the duties of which will be briefly discussed in turn:

- (1) Headquarters subsection
- (2) Code compilation subsection
- (3) Cipher compilation subsection
- (4) Publication subsection
- (5) Storage subsection
- (6) Distribution subsection
- (7) Accounting subsection

b. The headquarters subsection has charge of the administrative details relative to assignment of work to personnel, the use of the equipment, and the issue of supplies to the individual members of the section. All correspondence pertaining to the production, distribution, and accounting of codes and ciphers is initiated in the subsections and then passed through this office before going to the Administrative Section of the Signal Intelligence Service for signature and transmittal.

c. The code compilation subsection compiles new editions of authorized codes, as are required by field forces, principally for the Division Field Code, Air-Ground Liaison Code, Radio Service Code, and Esp Coordinate Code. Special codes adapted for special usage or entirely new codes the need for which is determined by the Commanding General, GHS, may be compiled.

d. The cipher compilation subsection prepares cipher tables, cipher keys, or cipher alphabets as may be required for use in connection with the various authorized codes, cipher systems and devices. It also has as one of its responsibilities the technical supervision and coordination of such automatic cryptographic machinery as may be employed for secret intercommunication among the highest headquarters of field forces.

e. The publication subsection has charge of the details pertaining to the printing and physical reproduction of copies of codes, ciphers, cipher tables, and cipher keys. If practicable, it should have facilities for printing or lithographic reproduction entirely under its own control, in order that proper safeguards may be established over this phase of secret communication facilities. However, if this is not practicable the printing and reproduction facilities of the Adjutant General, GAG, or of the Engineer Reproduction Plant, GRC, will have to be employed. The subsection is also responsible for all proofreading of galley and page proofs.

f. The storage subsection is the receiving office for printed cryptographic publications and is responsible for their safeguarding while in storage. It is necessary to provide it with suitable storage facilities, safes being preferable, and also with armed sentries to patrol the quarters at all hours during the day and night.

g. The code and cipher compilation section will make the most use of the automatic machinery referred to under par. 6 g. Without such machinery the section would either have to have much more personnel or else codes would have to be replaced less frequently.

12. Functions of code and cipher solution section. - a. This section comprises the following subsections:

- (1) Headquarters subsection
- (2) Distribution and records subsection
- (3) Codes subsection
- (4) Ciphers subsection
- (5) Research and training subsection

b. The headquarters subsection has charge of the administrative details relative to the assignment of work to the personnel of the section, the use of the equipment, and the issue of supplies to the individual members of the section. All correspondence pertaining to the work of the section, material furnished it for solution, the results accomplished, and liaison with other branches and agencies pass through this office before going to the Administrative Section for signature and transmittal. It also prepares daily, weekly, or monthly reports on cryptanalytic activities, which reports are intended for the G-2 section of the GAG staff and must be forwarded to that section for evaluation, coordination and distribution to all concerned. 7-

c. The distribution and records subsection distributes manuscript sheets, copies of messages, documents, etc., as received from the reproduction subsection of the Administrative Section direct to the personnel working upon the particular code or cipher concerned. Its personnel also are employed in indexing, tabulating, making frequency studies, etc., for the cryptanalytic staff.

d. The codes subsection studies and solves enemy code systems, attempts to reconstruct the codes as completely as possible, and decodes enemy messages so far as the reconstruction of the codes up to that moment will permit.

e. The ciphers subsection does the same type of work except on cipher systems.

f. The research and training subsection has the following duties:

(1) To investigate such new code and cipher systems, apparatus, and devices as are submitted to the Signal Officer, GHC, for consideration for use by field forces.

(2) To conduct a school for the training of enlisted and officer personnel assigned to duty in the Signal Intelligence Service of GHQ or Army. Such training will be essential for personnel obtained from sources other than the Chief Signal Officer because no other agency exists in the military service for training in signal intelligence activities.

13. Relations with other branches of Signal Intelligence Service. - a. The GHQ Signal Intelligence Service must maintain close liaison with the following other branches of the Signal Intelligence Service of the military establishments:

(1) Army Signal Intelligence Service. The signal intelligence service at the headquarters of each field army serves as a sort of forward echelon of the GHQ Signal Intelligence Service. Its personnel are trained only so far as will enable them to decipher and decode enemy messages for which the keys have been worked out by GHQ Signal Intelligence Service. The purpose here is to permit of speed in utilizing the results that may be obtained from solutions of enemy messages intercepted within the radius of action of the field army.

At the same time, the Army Signal Intelligence serves as a source of material for work by GHQ Signal Intelligence Service, since the messages which are intercepted by the Radio Intelligence Company assigned to Army and which cannot be solved by Army Signal Intelligence Service are forwarded for solution to GHQ Signal Intelligence Service. The officer-in-charge of Army Signal Intelligence Service should have had adequate training and experience in the GHQ Signal Intelligence Service. His assistants do not require such thorough training, but obviously the more they have the better will be their work.

(2) War Department Signal Intelligence Service. The largest unit of the Signal Intelligence Service and the one best equipped to work with the more complicated enemy codes and ciphers should be located at the War Department in Washington. Here the non-military codes and ciphers of the enemy government are studied, as well as the codes and ciphers of enemy commercial houses, agents, etc. It may be that the GHQ Signal Intelligence Service is in a better position to intercept such material than is the War Department Signal Intelligence Service, in which case the former should spend no time trying to solve this non-military traffic but should merely forward it to Washington. On the other hand, the enemy's field codes and ciphers may be so complicated as to be beyond the ability of personnel at GHQ Signal Intelligence Service, in which case the War Department Signal Intelligence Service may be called upon for cooperation and assistance.

(3) Corps Area and Department Signal Intelligence Services. If branches of the Signal Intelligence Service are established at the headquarters of corps areas and departments, liaison may be necessary between them and GHQ Signal Intelligence Service, for purposes of coordination, cooperation, and avoidance of duplication of effort.

b. It must also act in close liaison with the following:

(1) Censorship representative, GHQ. The censorship bureau will undoubtedly have offices in the Theater of Operations. Matters requiring cooperation between the Signal Intelligence Service and Censorship authorities in this region will require close liaison.

(2) Navy Signal Intelligence Service. The Theater of Operations may be located in such an area that direct liaison with Navy Signal Intelligence Service Afloat or Ashore is more conducive to good cooperation with GHQ Signal Intelligence Service than indirect liaison through the War Department Signal Intelligence Service, such direct contact should be established.

(3) Signal Intelligence Services of allied governments. - During the World War, the liaison that existed between the Radio Intelligence Section, G-2, GHQ, AEF, and the same service of French GHQ and British GHQ was most conducive to cooperation and elimination of duplication of effort. In case our government is engaged in a war conducted with Allies against a common enemy, such liaison may again be essential.

c. It will be seen from the foregoing that the activities of the Liaison Subsection of the Administrative Section, GHQ Signal Intelligence Service (par. 6a (7) above) are quite important and necessary for achieving the best results possible from coordinated efforts to solve all kinds of enemy communications.

#### 14. Duties of the officer-in-charge of the GHQ Signal Intelligence Service. -

a. It is the responsibility of the officer-in-charge of the GHQ Signal Service to administer the service under his charge in such a way that the functions of each section of his office, as outlined above, are efficiently conducted and that the service as a whole fulfills the mission assigned to it. He cannot be expected to be and, in fact, he may not be an expert cryptographer or an accomplished cryptanalyst, but he should know enough about these subjects to recognize the limitations that abound in practical work in these fields. He must realize first of all that the personnel assigned to him or selected by him are assumed to possess basic technical qualifications for the work and that if success does not crown their efforts or if it seems to him to come only too

slowly, this is inherent in the work itself: "supermind performances" are not the forte of cryptanalytic personnel, popular concepts to the contrary notwithstanding. It cannot be too strongly emphasized that cryptanalytic studies require a great deal of patience on the part of its working personnel; on the part of its directing and administrative personnel a similar degree of patience must be forthcoming. It is only rarely that spectacular situations and successes arise in the course of the work.

b. The last statement leads quite directly to a point which is touched upon with a certain amount of hesitancy but which nevertheless must be mentioned. As said before, signal intelligence is a specialty and its successes are rarely of a spectacular nature. They are, in this respect, quite different from the notable achievements which are much more frequently brought to light on the battlefield by brilliant tactics, resolute action, courage and fortitude. To those who have the good fortune to succeed on the battlefield, recognition and advancement come quickly, and this is of material importance toward the establishment and maintenance of a high stage of morale. But the successes of signal intelligence personnel, even when they do come (and they come only infrequently, very slowly, and most often as the result of long, hard labor), must usually be kept secret or, at the least, confidential. Consequently, these successes never can meet with popular acclaim and never can be awarded open recognition until long afterward. If, under these circumstances, promotion and advancement come more slowly than they do in other fields of action, the result is apt to be detrimental to the morale of the plodders in the signal intelligence field. It therefore is incumbent upon the officer-in-charge of the signal intelligence service to see that his personnel is accorded recognition for efficient, conscientious work in the same degree and with the same benefits as is accorded deserving personnel in the combat zone.

c. Finally, it is extremely important that the officer-in-charge realize that a vital factor in attaining success in signal intelligence work is the fostering of a competitive spirit among all personnel concerned but at the same time repressing to the utmost any spirit of professional jealousy, and try

attempts to deprive others of credit due for good work, merely for the sake of personal advancement of the offender. The officer-in-charge of each branch of the Signal Intelligence Service, wherever located, must be constantly on guard to prevent such destructive forces from gaining a foothold among his subordinates for the good and sufficient reason, aside from the one of fair play, that whereas the spirit of competition on a purely scientific basis is conducive to the production of results, will spur on his subordinates to do their very best, and will bring about a good state of morale, the corroding spirit of professional jealousy based merely upon avidity for personal distinction and advancement will not only disrupt a good organization but will prevent the establishment and maintenance of real cooperation. It may be stated that in signal intelligence work, especially in that of cryptanalysis, cooperation and coordinated effort are absolutely essential. The efforts of even a good many individuals, if each works alone, will avail very little; only good teamwork will produce results and will bring success in the assigned mission.



TENTATIVE

SUBJECT NUMBER

USCIB: 23/70      Item 2 of the Agenda for the Eighty-eighth Meeting of USCIB, held on 10 July 1953.

Subject:            Final Report and Papers of the U.K.-U.S. Conference on the Communications Security of the NATO Countries (USCIB 23/65).

The CHAIRMAN opened discussion on this item by inviting comments by the Chairman of the U.S. Delegation, Mr. Friedman.

MR. FRIEDMAN expressed his opinion that the conference report spoke pretty well for itself, and added that he thought the report should be approved as rendered. At a meeting on 6 July he said the Executive Committee approved the conclusions and recommendations of the report with exception of the CIA member who reserved his position on one or two points.

CAPTAIN TAYLOR replied that the CIA position had been circulated to the Members of the Board as USCIB 23/69.

MR. FRIEDMAN went on to say that there are some loose ends remaining to be tied up by a sub-committee or an ad hoc committee. He suggested that an ad hoc committee composed of some members of the U.S. delegation constitute such a group. He added that specific points to be worked out are the preparation of certain appendices and schedules of the communications security technical details, for which a small group should be set up in Washington. Also he said there were certain other matters to be considered, such as what might be done with regard to improvements in commercial machines which might interfere with our future work. He further stated that he was prepared to try to answer questions that might be raised by Members of the Board.

The CHAIRMAN suggested that USCIB 23/69 be taken up since some question had been raised by the CIA representative, and asked Mr.

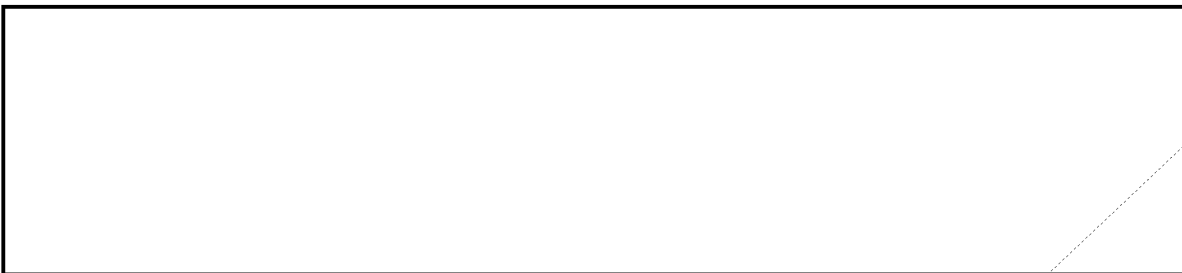
if he would like to speak on that.

OGA



USCIB: 23/70

USCIB: 23/70



The CHAIRMAN said he thought there was some strength in the CIA position and that until negotiations have been concluded with the French it will be difficult to tell just what the best procedure would be. He inquired if it would be agreeable to approve the report and to have another look at the question of the best method of proceeding with the other NATO powers, after we conclude with the French. He asked Mr. Friedman if he had any comment on that point.

MR. FRIEDMAN said he thought the important thing to do is to start and see how the French react, and if the French react favorably we could then consider the other countries one by one.

The CHAIRMAN said that CIA would not be estopped by this action from raising the question of other possible means of procedure.

MR.  agreed. OGA

MR. KEAY said he thought that was inherent in the report and he believed that the approach to the French was on the basis of further NATO approaches.

MR. FRIEDMAN said the French had already approached  with the statement that they were very much concerned about the insecurity of the communications of certain NATO countries.

EO 3.3(h) (2)  
PL 86-36/50 USC 3605

The CHAIRMAN said he thought the report is approved unless there was any other comment.

CAPTAIN ROEDER said that the Navy approved the report. He added that they felt that since five years have elapsed since the problem was first presented that it might be desirable to agree at this time to vote a deadline on when the problem would be re-examined rather than let it go on for another few years. He suggested the time limit of one year if that was agreeable and added that the problem could then be re-examined to see what progress has been made.

The CHAIRMAN inquired of Captain Taylor if there was any objection to Captain Roeder's proposal.

USCIB: 23/70

~~TOP SECRET CANOE~~~~SECURITY INFORMATION~~

USCIB: 23/70

CAPTAIN TAYLOR replied in the negative.

The CHAIRMAN then stated the proposal was approved.

The CHAIRMAN stated that the first matter for implementation was the appointment of the cognizant U.S. authority. He asked for suggestions.

MR. FRIEDMAN stated that in the deliberations of the conference, the conferees had originally definitely suggested that the Department of State and the Foreign Office be made cognizant authorities for making an approach to the French. He added that the specific reference was taken out at the suggestion of the CIA delegate who thought it was presumptuous of the conference to try to tell LSIB and USCIB whom to appoint.

MR.  <sup>OGA</sup> suggested the Department of State.

MR. ARMSTRONG said that the State Department was perfectly willing to undertake it on the part of USCIB. He added that he assumed that LSIB would appoint the Foreign Office. He added that he understood this to be the case and that the actual person to approach in the Foreign Office had been agreed in the early stages.

MR. FRIEDMAN agreed and added that it was Mr. Parodi.

The CHAIRMAN inquired if there were any other nominations and added that the job requires a high degree of diplomacy and skill. He said he would look to the State Department for that diplomacy. He added that he hoped Mr. Armstrong would take a personal interest in the matter.

MR. ARMSTRONG said he would indeed. He said he would see that the Ambassador, upon whom we would have to rely very heavily, would be fully briefed on the matter as to how and when, etc.

The CHAIRMAN inquired if the matter would be handled in Paris or London.

MR. ARMSTRONG replied that Paris would be best because it would prevent the French from having to communicate and it could be done with less attention drawn to it in Paris than London.

The CHAIRMAN stated that that would mean getting into higher diplomatic circles.

MR. ARMSTRONG said he thought we should start at the top. The first approach, he said, presumably would be to the Minister who would raise it in the inner-Cabinet level forthwith for approval per se.

USCIB: 23/70

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~~~SECURITY INFORMATION~~

USCIB: 23/70

The CHAIRMAN stated that if there were no other nominations, the designation of the State Department as the Cognizant U.S. Authority is approved. He pointed out to Mr. Friedman that he thought the U.S. element of the Combined Working Group would be the State Department and technicians from NSA.

MR. ARMSTRONG stated that with respect to paragraph 32b, the State Department would have to rely very heavily upon NSA and the others.

The CHAIRMAN noted that paragraph 32e stated that "Agreement on the terms and composition of the Combined Working Group to be set up in Washington to facilitate coordination of this action" is required.

MR. FRIEDMAN said that was referred to in the last sentence of paragraph 24. He then proceeded to read this sentence, and added that he assumed that the Group would assist the State Department and the U.S. members of this Combined Working Group.

The CHAIRMAN said it could be left up to the Cognizant U.S. Authorities to see that the Combined Working Group is set up.

MR. FRIEDMAN said he thought that many of these details could be worked out by the Executive Committee.

CAPTAIN TAYLOR asked if it was the sense of the Board that the initial action on the Combined Working Group will be referred to the Executive Committee by the Cognizant U.S. Authorities.

MR. ARMSTRONG replied that it was his understanding that it would be.

The CHAIRMAN stated that the above action was approved.

The CHAIRMAN suggested that the Executive Secretary advise the British of the action taken at this meeting.

CAPTAIN TAYLOR said he would prepare a suitable document.

DECISION: (10 July 1953) USCIB approved the final report and papers of the US/UK conference on Allied (NATO) communications security as a basis for negotiations with the U.K. and agreed that U.K. authorities would be so notified.

It was agreed, further, that:

- (1) The Department of State would be the "Cognizant U.S. Authority".

USCIB: 23/70

- 7 -

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~~~SECURITY INFORMATION~~

USCIB: 23/70

- (2) As "Cognizant U.S. Authority" the Department of State would take action as necessary and appropriate to refer to the Executive Committee the problem of initial action in the establishment of the Combined Working Group in Washington.
- (3) No member would be estopped from raising the question of desirability of using other than NATO channels after negotiations with the French have been undertaken.
- (4) That this problem will be reviewed by the Board at approximately one year from date.

USCIB: 23/70

- 8 -

~~TOP SECRET CANOE~~

IN THESE RECORDS WILL BE  
FOR OFFICIAL PURPOSES.  
DO NOT REMOVE PAPERS  
OR CONTENTS TO UN-  
AUTHORIZED PERSON(S)

RECORDS CHARGE-OUT  
REF ID: A62861

5223

DATE OF REQUEST

SUSPENSE DATE

25 Mar '60

FILE OR  
SERIAL  
NUMBER  
AND  
SUBJECT

From the Files of the Special Consultant - Friedman)  
Final Version of Lecture No. 1 - 24 pages (carbon copy), No. 2 - 24 pages,  
No. 3 - 19 pages and 1 page of notes. ~~CONFIDENTIAL~~

(All carbon copies)

NAME AND EXTENSION OF PERSON REQUESTING FILE

ORGANIZATION, BUILDING, AND ROOM NUMBER

Mr. William F. Friedman ( Home )

Special Consultant

RETURN  
TO

NSA Records Management Br, AG-24 - Christian

DATE RET'D

INITIAL HERE

INSTRUCTIONS

WHEN TRANSFERRING FILE TO ANOTHER PERSON COMPLETE SELF-ADDRESSED TRANSFER COUPON BELOW, DETACH,  
STITCH TO BLANK LETTER-SIZE PAPER AND PLACE IN OUT-GOING MAIL SERVICE

2ND TRANSFER COUPON

TO:

FILE (serial number and subject)

TRANSFERRED TO (name and extension)

ORGANIZATION, BUILDING, AND ROOM NUMBER

DATE

(sig)

(ext)

5223

*Final  
Lecture 1*

~~CONFIDENTIAL~~LECTURE I

The objective of this series of lectures is to create an awareness of the background, development, and manner of employment of a science that is the basis of a vital military offensive and defensive weapon known as CRYPTOLOGY, a word that comes from the Greek kryptos, meaning secret or hidden, plus logos, meaning knowledge or learning. Cryptology will be specifically defined a little later; at the moment however, I'm sure you know that it has to do with secret communications.

Let me say at the outset of these lectures that I may from time to time touch upon matters which are perhaps essentially peripheral or even irrelevant to the main issues of cryptology, and if a defense is needed for such occasional browsing along the by-ways of the subject while travelling along the main highways of the science, I'll say that long preoccupation with any field of knowledge begets a curiosity the satisfaction of which is what distinguishes the dedicated professional from the person who merely works just to gain a livelihood in whatever field he happens to find himself a job. That's not much fun, I'm afraid. By the way, a British writer, James Agate, defines a professional as the man who can do his job even when he doesn't feel like doing it; an amateur, as a man who can't do his job even when he does feel like doing it. This is pretty tough on the gifted amateur and I for one won't go all the way with Agate's definition. There are plenty of instances where gifted amateurs have done and discovered things to the chagrin and red-facedness of the professionals.

~~CONFIDENTIAL~~

Coming back now to the main thoroughfare after the foregoing brief jaunt along a by-way, I may well begin by telling you that the science of cryptology has not always been regarded as a vital military offensive and defensive weapon, or even as a weapon in the first place. Here I am reminded of a story in a very old book on cryptography. The story is probably apocryphal, but it's a bit amusing, and I give it for what it's worth.

It seems that about two thousand years ago there lived a Persian queen named Semiramis, who took an active interest in cryptology. Whether it was because of that interest or for other unnatural reasons, such as curiosity about what people call "secrets", the record doesn't say, but anyhow it is reported that she met with an untimely death. Presumably she went to Heaven, or perhaps to the other place, but she left instructions that her earthly remains were to be placed in a golden sarcophagus within an imposing mausoleum on the outside of which, on its front stone wall, there was to be graven a message, saying:

Stay, weary traveller!  
 If thou art footsore, hungry, or in need of money--  
 Unlock the riddle of the cipher graven below,  
 And you will be led to riches beyond all dreams of avarice!

Below this curious inscription was a cryptogram, a jumble of letters without meaning or even pronounceability. For several hundred years the possibility of sudden wealth served as a lure to many experts who tried very hard to decipher the cryptogram. They were all without success, until



one day there appeared on the scene a long-haired, be-whiskered, and bespectacled savant who, after working at the project for a considerable length of time, solved the cipher, which gave him detailed instructions for finding a secret entry into the tomb. When he got inside, he found an instruction to open the sarcophagus, but he had to solve several more cryptograms the last one of which may have involved finding the correct combination to a 5-tumbler combination lock--who knows? Well, he solved that one too, after a lot of work, and this enabled him to open the sarcophagus, inside which he found a box. In the box was a message, this time in plain language, and this is what it said:

O, thou vile and insatiable monster! To disturb these poor bones!  
 If thou had'st learned something more useful than the art of  
 deciphering,  
 Thou would'st not be footsore, hungry, or in need of money!

I'm frank to confess that many times during my 48-year preoccupation with cryptology, and generally near the middle and the end of each month, I felt that good old Queen Semiramis knew what she was talking about. However, earning money is only a part of the recompense for working in the cryptologic field, and I hope that most of you will find out sooner or later what some of these other recompenses are and what they can mean to you.

If Queen Semiramis thought there are other things to learn that are more useful than the art of deciphering, I suppose we'd have to agree, but we are warranted in saying, at least, that there isn't any question about the importance of the role that cryptology plays in modern times: all of

us are influenced and affected by it as I hope to show you in a few minutes.

I will begin by reading from a source which you'll all recognize--

TIME magazine, the issue of 17 December 1945. I will preface the reading by reminding you that by that date World War II was all over--or at least V-E and V-J days had been celebrated some months before. Some of you may be old enough to remember very clearly the loud clamor on the part of certain vociferous members of Congress who had for years been insisting upon learning the reasons why we had been caught by surprise in such a disastrous defeat as the Japanese had inflicted upon us at Pearl. This clamor had to be met, for these Congressmen contended that the truth could no longer be hushed up or held back because of an alleged continuing need for military secrecy, as claimed by the Administration and by many Democratic senators and representatives. The war was over--wasn't it?--Republican senators and representatives insisted. There had been investigations--a half dozen of them, but all except one were TOP SECRET. The Republicans wanted, and at last they got what they desired--a grand finale Joint Congressional Investigation which would all be completely open to the public. No more secrets! It was spectacular! Not only did the Congressional Inquiry bring into the open every detail and exhibit uncovered by its own lengthy hearings, but it also disclosed to America and to the whole world everything that had been said and shown at all the previous Army and Navy investigations. Most of the

information that was thus disclosed had been and much of it was then still TOP SECRET; yet all of these precious secrets became matters of public information as a result of the Congressional Investigation.

There came a day in the Congressional Hearings when the Chief of Staff of the United States Army at the time of the Pearl Harbor Attack, 5-star General George C. Marshall, was called to the witness stand. He testified for several long, long days, eight of them in all. Toward the end of the second day of his ordeal he was questioned about a letter it had been rumored he'd written to Governor Dewey in the Autumn of 1944, during the Presidential Campaign. The letter was about codes. With frozen face, General Marshall balked at disclosing the whole letter. He pleaded most earnestly with the Committee not to force him to disclose certain of its contents, but to no avail. He had to bow to the will of the majority of the Committee. Here's a picture of General Marshall and Governor Dewey. I will now read from TIME a bit of information which may be new to many of my listeners, especially to those who were too young in December 1945 to be coming into periodical literature or to be reading any pages of the daily newspaper other than those on which the comics appear.

Said TIME, and I quote:

"U.S. citizens discovered last week that perhaps their most potent secret weapon of World War II was not radar, not the VT fuse, not the atom bomb, but a harmless little machine which

cryptographers had painstakingly constructed in a hidden room in Washington. With this machine, built after years of trial and error, of inference and deduction, cryptographers had duplicated the decoding devices used in Tokyo. Testimony before the Pearl Harbor Committee had already shown that the machine known as 'Magic' was in use long before December 7, 1941, and had given ample warning of the Japs' sneak attack if only U.S. brass hats had been smart enough to realize it. Now, General Marshall continued the story of 'Magic's' magic.

1. "It had enabled a relatively small U.S. Force to intercept a Jap invasion fleet, win a decisive victory in the Battle of the Coral Sea, thus saving Australia and New Zealand.

2. "It had given the U.S. full advance information on the size of the Jap forces advancing on Midway, enabled our Navy to concentrate ships which otherwise might have been 3,000 miles away, thus set up an ambush which proved to be the turning-point victory of the Pacific war.

3. "It had directed U.S. submarines unerringly to the sea lanes where Japanese convoys would be passing.

4. "By decoding messages from Japan's Ambassador Oshima in Berlin, often reporting interviews with Hitler, it had given our forces invaluable information on German war plans." End quote.

TIME goes on to give more details of that story, to which I may later return but I can't leave this citation of what cryptology did toward our winning of World War II without telling you that the account given by TIME of the achievements of MAGIC makes it appear that all the secret intelligence gained from our reading Japanese messages was obtained by using that "harmless little machine" which TIME said was used in Tokyo by the Japanese Foreign Office. I must correct that error by telling you that the secret information we obtained that way had little to do with those portions of the MAGIC material which enabled our Navy to win such spectacular battles as those of the Coral Sea and Midway, and to waylay Japanese convoys. The naval parts of MAGIC were nearly all obtained from Japanese naval messages by our own very ingenious U.S. Navy cryptanalysts. At that time, I may tell those of you who are new, that the Army and Navy had separate but cooperating cryptologic agencies and activities; the United States Air Force was not yet in existence as an autonomous and separate component of the Armed Forces, and work on Japanese, German, and Italian air force communications was done by Army cryptanalysts admirably assisted by personnel of what was then known as the Army Air Corps.

It is hardly necessary to tell you how carefully the MAGIC of World War II was guarded before, during, and after the war until the Congressional Inquiry brought most of it out in the open. Some remaining parts of it are still very carefully guarded. Even the fact of the existence of MAGIC was

known to only a very few persons at the time of Pearl Harbor--and that is an important element in any attempt to explain why we were caught by surprise by the Japanese at Pearl Harbor in a devastating attack that crippled our Navy for many months. Let me read a bit from page 261 of the Report of the Majority of the Joint Congressional Investigation of the attack:

"The Magic intelligence was pre-eminently important and the necessity for keeping it confidential cannot be overestimated. However, so closely held and top secret was this intelligence that it appears that the fact that the Japanese codes had been broken was regarded as of more importance than the information obtained from decoded traffic."

TIME says, in connection with this phase of the story of Magic during World War II:

"So priceless a possession was MAGIC that the U.S. high command lived in constant fear that the Japs would discover the secret, change their code machinery, force U.S. cryptographers to start all over again."

Now I don't want to over-emphasize the importance of communications intelligence in World War II, but I think it warranted to read a bit more of what is said about its importance in the Report of the Majority. The following is from p. 232:

"... all witnesses familiar with MAGIC material throughout the war have testified that it contributed enormously to the defeat of the enemy, greatly shortened the war, and saved many thousands of lives."

General Chamberlin, who was General MacArthur's operations officer, or G-3, throughout the war in the Pacific, has written: "The information G-2 that is, the intelligence staff, gave me in the Pacific Theater alone saved us many thousands of lives and shortened the war by no less than two years." We can't put a dollar-and-cents value on what our possession of COMINT meant in the way of saving lives; but we can make a dollar-and-cents estimate of what communications intelligence meant by shortening the war by two years, and the result of that estimate is that it appears that \$1.00 spent for that sort of intelligence was worth \$1,000 spent for other military activities and materials.

In short, when our commanders had that kind of intelligence in World War II they were able to put what small forces they had at the right place, at the right time. But when they didn't have it--and this happened, too--their forces often took a beating. Later on we'll note instances of each type.

I hope I've not tried your patience by such a lengthy preface to the real substance of this series of lectures, so let's get down to brass tacks. For those of you who come to the subject of cryptology for the first time, a few definitions will be useful, in order that what I shall be talking about

will be understood without question. Agreement on basic terminology is always desirable in tackling any new subject. In giving you the definitions there may be a bit of repetition because we will be looking at the same terms from somewhat different angles.

First, then, what is cryptology? Briefly, we may define it as the doctrine, theory, or branch of knowledge which treats of hidden, disguised, or secret communications. You won't find the word cryptology in a small dictionary. Even Webster's Unabridged defines it merely as "secret or enigmatical language"; and in its "Addenda Section", which presumably contains new or recently-coined words, it is defined merely as "the study of cryptography". Neither of these definitions is broad nor specific enough for those who are going to delve somewhat deeply into this science.

Cryptology has two main branches; the first is cryptography, or, very briefly, the science of preparing secret communications; and the second is cryptanalysis, or the science of solving secret communications. Let's take up cryptography first, because as a procedure it logically precedes cryptanalysis: before solving anything there must be something to solve.

Cryptography is that branch of cryptology which deals with the various means, methods, devices, and machines for converting messages in ordinary, or what we call plain language, into secret language, or what we call cryptograms. Here's a picture of one of the most famous cryptograms in history. It was the solution of this cryptogram which resulted in bringing America



into World War I on the side of the Allies on 6 April 1917, just about six weeks after it was solved. I'll tell you about it later in this series.

Cryptography also includes the business of reconverting the cryptograms into their original plain-language form, by a direct reversal of the steps followed in the original transformation. This implies that the persons involved in both of these bits of business, those at the enciphering and sending end, and those at the receiving and deciphering end, have some sort of understanding as to what procedures, devices, and so on, will be used and exactly how--down to the very last detail. The what and the how of the business constitutes what is generally referred to as the key. The key may consist of a set of rules, alphabets, procedures, and so on; it may also consist of an ordinary book which is used as a source of keys; or it may be a specialized book, called a code book. That cryptogram I just showed you was made by using a book--a German codebook.

To encrypt, is to convert or transform a plain-text message into a cryptogram by following certain rules, steps, or processes constituting the key or keys and agreed upon in advance by the correspondents, or furnished them by higher authority.

To decrypt is to reconvert or to transform a cryptogram into the original equivalent plain-text message by a direct reversal of the encrypting process, that is, by applying to the cryptogram the key or keys, usually in a reverse order, employed in producing the cryptogram.

A person who encrypts and decrypts messages by having in his possession the necessary keys, is called a cryptographer, or a cryptographic clerk.

Encrypting and decrypting are accomplished by means collectively designated as codes and ciphers. Such means are used for either or both of two purposes: (1) secrecy, and (2) economy. Secrecy usually is far more important in diplomatic and military cryptography than economy but it is possible to combine secrecy and economy in a single system. Persons technically unacquainted with cryptology often talk about "cipher codes", a term which I suppose came into use to differentiate the term "code" as used in cryptology from the same term as used in other connotations, as, for example, the Napoleonic Code, a traffic code, a building code, a code of ethics, and so on. Now, in cryptology, there is no such thing as a "cipher code". There are codes and there are ciphers, and we might as well learn right off the differences between them so that we get them straightened out in our minds before proceeding further.

In ciphers, or in cipher systems, cryptograms are produced by applying the cryptographic treatment to individual letters of the plain-text messages, whereas, in codes, or in code systems, cryptograms are produced by applying the cryptographic treatment generally to entire words, phrases, and sentences of the plain-text messages. More specialized meanings of the terms will be explained in detail later but in a moment I'll show you an example of a cryptogram in cipher and one in code.

A cryptogram produced by means of a cipher system is said to be in cipher and is called a cipher message, or sometimes, simply, a cipher. The act or operation of encrypting a cipher message is called enciphering, and the enciphered version of the plain text, as well as the act or process itself, is often referred to as the encipherment. A cryptographic clerk who performs the process serves as an encipherer. The corresponding terms applicable to decrypting cipher messages are deciphering, decipherment, and decipherer.

A cryptogram produced by means of a code system is said to be in code, and is called a code message. The text of the cryptogram is referred to as code text. This act or operation of encrypting is called encoding, and the encoded version of the plain text, as well as the act or process itself, is referred to as the encodement. The clerk who performs the process serves as an encoder. The corresponding terms applicable to the decrypting of code messages are decoding, decodement, and decoder. A clerk who encodes and decodes messages by having in his possession the pertinent code books is called a code clerk.

Technically, there are only two distinctly different types of treatment which may be applied to written plain text to convert it into a cipher, yielding two different classes of ciphers. In the first, called transposition, the letters of the plain text retain their original identities and merely undergo some change in their relative positions, with the result that the original text becomes unintelligible. Here's an authentic example of a

transposition cipher; I call it authentic because it was sent to President Roosevelt and the Secret Service asked me to decipher it. Imagine my chagrin when I had to report that it says "Did you ever bite a lemon?" In the second, called substitution, the letters of the plain text retain their original relative positions but are replaced by other letters with different sound values, by symbols of some sort so that the original text becomes unintelligible.

Nobody will quarrel with you very hard if you wish to say that a code system is nothing but a specialized form of substitution; but it's best to use the word code when a code book is involved, and to use substitution cipher when a literal system of substitution is used.

It is possible to encrypt a message by a substitution method and then to apply a transposition method to the substitution text, or vice versa. Combined transposition-substitution ciphers do not form a third class of ciphers; they are only occasionally encountered in military cryptography. Applying a cipher to code groups is a very frequently-used procedure and we'll see cases of that too.

Here's an example of a substitution cipher, and a very simple one.

It was found on a German spy in World War II. Here's the cipher alphabet; here's the plain text which happened to be in German; and here's the cipher text or encipherment.

Now for an example of a cryptogram in code. Here's a plain-text message in the handwriting of President Wilson, to his special emissary in London, Colonel House. Here's the cryptogram after the plain text was encoded, by Mrs. Wilson. The President then himself typed out the final message on his own typewriter, for transmission by the Department of State. It would appear that President Wilson lacked confidence in the security of the Department of State's methods--and maybe with good reason, as may be seen in the following extract from a letter dated 14 September 1914 from the President to Ambassador Page in London: "We have for some time been trying to trace the leaks, for they have occurred frequently, and we are now convinced that our code is in possession of persons at intermediary points. We are going to take thorough-going measures." Perhaps one of the measures was that the President got himself a code of his own. I must follow this up some day.

A cipher device is a relatively simple mechanical contrivance for encipherment and decipherment, usually "hand-operated", or manipulated by the fingers, as for example, a device with concentric rings of alphabets, manually powered. Here's an example--a cipher device with such rings. I'll tell you about it later. A cipher machine is a relatively complex apparatus or mechanism for encipherment and decipherment, usually equipped with a typewriter keyboard and generally requiring an external power source. Modern cryptology, following the trend in mechanization and automation in other fields, now deals largely with cipher machines, some highly complicated. Here's a picture of a modern cipher machine with keyboard and printing mechanism.

One of the expressions which uninformed laymen use but which you must never use is "the German code", or "the Japanese code", or "the Navy cipher", and the like. When you hear this sort of expression you may put the speaker down at once as a novice. There are literally hundreds of different codes and ciphers in simultaneous use by every large and important government or service, each suited to a special purpose; or where there is a multiplicity of systems of the same general nature, the object is to prevent a great deal of traffic being encrypted in the same key, thus overloading the system and making it vulnerable to attack by methods and procedures to be mentioned in broad terms in a few moments.

The need for secrecy in the conduct of important affairs has been recognized from time immemorial. In the case of diplomacy and organized warfare this need is especially important in regard to communications. However, when such communications are transmitted by electrical means, they can be heard or, as we say, intercepted, and copied by unauthorized persons, usually referred to collectively as the enemy. The protection resulting from all measures designed to deny to the enemy information of value which may be derived from the interception and study of such communications is called communication security, or, for short, COMSEC.

In theory, any cryptosystem except one, to be discussed in due time, can be attacked and "broken", i.e., solved, if enough time, labor, and skill are devoted to it, and if the volume of traffic in that system is large

enough. This can be done even if the general system and the specific key are unknown at the start. You will remember that I prefaced my statement that any cryptosystem can be solved by saying "in theory", because in military operations theoretical rules usually give way to practical considerations.

That branch of cryptology which deals with the principles, methods, and means employed in the solution or analysis of cryptosystems is called cryptanalytics. The steps and operations performed in applying the principles of cryptanalytics constitute cryptanalysis. To cryptanalyze a cryptogram is to solve it by cryptanalysis. A person skilled in the art of cryptanalysis is called a cryptanalyst, and a clerk who assists in such work is called a cryptanalytic clerk.

Information derived from the organized interception, study, and analysis of the enemy's communications is called communication intelligence, or, for short, COMINT. Let us take careful note that COMINT and COMSEC deal with communications. Although no phenomenon is more familiar to us than that of communication, the fact of the matter is that this magic word means many things to many people. A definition of communication that is broad enough for our purposes would be that communication deals with intelligent messages exchanged between intelligent beings. This implies that human beings, and human operators are involved in the preparation, encryption, transmission, reception, decryption, and recording of messages which at some stage or stages are in written form and in some stage or stages are in

electrical form as signals of one sort or another. But in recent years there have come into prominence and importance electrical signals which are not of the sort I've just indicated. They do not carry "messages" in the usual sense of the word; they do not convey from one human being to another an intelligible sequence of words and an intelligible sense. I refer here to electrical or electronic signals such as are employed in homing or directional beacons, in radar, in telemetering or recording data of an electrical or electronic nature at a distance, and so on. Information obtained from a study of enemy electronic emissions of these sorts is called electronic intelligence, or, for short, ELINT. The particular or specialized study of enemy radar signals is called RADINT. All these, COMINT, ELINT, RADINT comprise SIGINT, that is, signal intelligence. Cryptology is the science which is concerned with all these branches of secret signalling.

In this series of lectures we shall be concerned only with COMSEC and COMINT, leaving for others and for other times the subjects of ELINT, RADINT, and so on. This means that we shall deal with communications or messages.

Communication may be conducted by any means susceptible of ultimate interpretation by one of the five senses, but those most commonly used are seeing and hearing. Aside from the use of simple visual and auditory signals for communication over relatively short distances, the usual method of communication between or among individuals separated from one another by relatively long distances involves, at one stage or another, the act of writing or of speaking over a telephone.



Privacy or secrecy in communication by telephone can be obtained by using equipment which affects the electrical currents involved in telephony, so that the conversations can be understood only by persons provided with suitable equipment properly arranged for the purpose. The same thing is true in the case of facsimile transmission (i.e., the electrical transmission of ordinary writing, pictures, drawings, maps). Even today there are already simple forms of enciphered television transmissions. Enciphered facsimile is called CIPAX; enciphered telephony, CIPHONY; and enciphered television, CIVISION. However, these lectures will not deal with these electrically and cryptanalytically more complex forms of cryptology. We shall stick to enciphered or encrypted writing--which will be hard enough for most of us.

Writing may be either visible or invisible. In the former, the characters are inscribed with ordinary writing materials and can be seen with the naked eye; in the latter, the characters are inscribed by means or methods which make the writing invisible to the naked eye. Invisible writing can be prepared with certain chemicals called sympathetic or secret inks, and in order to "develop" such writing, that is, make it visible, special processes must usually be applied. Here's an interesting example--the developed secret-ink message that figured in an \$88,000,000 suit won by two American firms against the German Government after World War I sabotage was proved. There are also methods of producing writing which is invisible to the naked eye because the characters are of microscopic size, thus

requiring special microscopic and photographic apparatus to enlarge such writing as to make it visible to the naked eye. Here's an example--a code message in a space not much larger than the head of a pin. A simple definition of secret writing would be to say that it comprises invisible writing and unintelligible visible writing.

There is one additional piece of basic information which it is wise to call to your attention before we proceed much further, and I'll begin by stating that the greatest and the most powerful instrument or weapon ever forged and improved by man in his long struggle for emancipation from utter dependence upon his own environment is the weapon of literacy--a mastery of reading and writing; and the most important invention, the one that made the weapon of literacy practical, was the invention of the alphabet. It is therefore a rather striking anomaly that we should now come to the study of another weapon--a counter-weapon to the weapon of literacy--the weapon of secrecy, the basic intent of which is to thwart the weapon that man struggled so long to forge. Secrecy is applied to make writing more difficult and the reading of the writing very difficult, if not impossible.

Perhaps this is a good place to do a bit of theorizing about this matter of secrecy and what it implies.

Every person who enciphers a piece of writing, a message, or a text of any kind, for the purpose of hiding something or of keeping something secret, does so with the idea that some other person, removed from him in distance,

or time, or both, is intended to decipher the writing or message and thus uncover the secret which was so hidden. A person may possess a certain piece of knowledge which he does not wish to forget but which he is nevertheless unwilling to commit to open writing, and therefore he may jot it down in cryptic form for himself to decipher later, when or if the information is needed. The most widely known example of such a cryptogram is found in Edgar Allan Poe's romantic tale The Gold Bug. That sort of usage of cryptography, however, is unusual. There are also examples of the use of cipher writing to establish priority of discovery, as did the astronomers Galileo and Huygens. Here's a slide which shows both examples. I suppose I should at least mention another sort of cryptic writing famous in literary history, the diaries of persons such as Samuel Pepys and William Byrd. These are commonly regarded as being "in cipher", but they were actually written in a more or less private shorthand and can easily be read without the help of cryptanalysis. Here's a picture of a page of Pepys diary.

Now there can be no logical reason, point, or purpose in taking the time and trouble to encipher anything unless it is expected that some other person is to decipher the cipher some time in the future. This means that there must exist some very direct, clear-cut and unambiguous relationship between the enciphering and deciphering operations. Just what such a relationship involves will be dealt with later but at this moment all that it is necessary to say is that in enciphering there must be rules that govern or

control the operations, that these rules must admit of no uncertainty or ambiguity and that they must be susceptible of being applied with undeviating precision, otherwise it will be difficult or perhaps impossible for the decipherer to obtain the correct answer when he reverses the processes or steps followed in the encipherment. This may be a good place to point out that a valid or authentic cryptanalytic solution cannot be considered as being merely what the cryptanalyst thinks or says he thinks the cryptogram means, nor does the solution represent an opinion of the cryptanalyst. Solutions are valid only insofar as they are objective and susceptible of demonstration or proof employing scientifically acceptable methods or procedures. It should hardly be necessary to indicate that the validity of the results achieved by cryptanalytic studies of authentic cryptograms rests upon the same sure and well-established scientific foundations, and are reached by the same sort of logic as are the discoveries, results, or "answers" achieved by any other scientific studies, namely, observation, hypothesis, deduction, induction, and confirmatory experiment. Implied in what I have just said is the tacitly understood and now rarely explicitly stated assumption that two, or more, equally competent and, if necessary, specially qualified investigators, each working independently upon the same material, will achieve identical or practically identical results.

Cryptology is usually and properly considered to be a branch of mathematics, although Francis Bacon considered it also a branch of grammar and

what we now call linguistics. Mathematical and statistical considerations play an ever-increasing and prominent role in practical cryptology, but don't let my statement of this point frighten those of you who have not had much formal instruction in these subjects. We have excellent cryptologists who have never studied more than arithmetic, and some of our best ones would hide if you were to go searching for mathematicians around here. What is needed is the ability to reason logically as the mathematician sometimes does and this ability is found in the most curious sorts of persons and places. So those of you who are frightened by the words mathematics and statistics take heart--you're not nearly so bad off as you may fear.

But now to return to the main theme as to the place mathematics occupies in cryptology, let me say that just as the solution of mathematical problems leaves no room for the exercise of divination or other mysterious mental or psychic powers, so a valid solution to a cryptogram must leave no room for the exercise of such powers. In cryptologic science there is one and only one valid solution to a cryptogram, just as there is but one correct solution or "solution set" to any problem in mathematics. But perhaps I've already dwelt on this point too long; in any case, we'll come back to it later, when we come to look at certain types of what we may call pseudo-ciphers.

In the next lecture I'm going to give you a brief glimpse into the background or history of cryptology, which makes a long and interesting story that has never been told accurately and in detail. The history of communications

security, that is, of cryptography, and the history of communications intelligence, that is, of cryptanalysis, which are but opposite faces of the same coin, deserve detailed treatment but I am dubious that this sort of history will ever be written because of the curtain of secrecy and silence which officially surrounds the whole field of cryptology.

Authentic information on the background and development of these vital matters having to do with the security of a nation is understandably quite sparse.

But in the succeeding lectures I'll try my best to give you authentic information, and where there's conjecture or doubt I'll so indicate. I must add, however, that in this series I'm going to have to omit many highly-interesting episodes and bits of information not only because these lectures are of low classification but also because we won't and can't go beyond a certain period in cryptologic history for security considerations. Nevertheless, I hope you won't be disappointed and that you'll learn certain things of great interest and importance, things to remember if you wish to make cryptology your vocation in life.

WILLIAM F. FRIEDMAN  
% US MILITARY ATTACHE  
AMERICAN EMBASSY,  
LONDON, ENGLAND

3932 MILITARY ROAD,  
WASHINGTON, DC

"ENTIA NON SUNT MULTIPICANDA  
— PRAETER NECESSITATEM"  
— William of Occam

Approved for Release by NSA on  
01-23-2015 pursuant to E.O. 13526

Friday, April 23, 1943

Left National Airport on a C54 at 118 p.m. (instead of 7:30 a.m.) 26 passengers, crew of 8 nice passage to Gander, Nfld. Anxiety re no hydr pressure, no flaps, when due to land. Circled field 3 times, made good landing 8 45 p.m. 1350 miles Good supper played ping pong & rested Left Gander 12 45 p.m. (Wash time) in single hop to Prestwick (2211 mi) landed 10 40 a.m. Very cold at 16 000 ft + had use oxygen Then down to 2500 ft + quite rough Was nauseated several times Customs etc at Prestwick + after about 15 minutes boarded shuttle plane to London, arr. Hendon Airt 2 30 p.m. (Wash time) Bus from Airport to #8 Audley St, signed in + was assigned room at Park Lane Hotel. Time elapsed from dep to arr. Hendon 25 hrs. Flight 21 hrs.

Nice dinner at hotel + good room with Taylor at 18/ plus 3/6 for breakfast

To bed at 11 30 p.m. (London) + slept hard through air alarm at 12 30 a.m. Route tired but awoke much refreshed Bed very comfortable.

Sunday April 25 - Reported in at AG Office Phoned George Bisher, Bisher met him at ETOUSA HQ. With Eric Svensson Grand reception + lunch with them at Officers' mess, where we were introduced + given membership (we thru courtesy of Col. Lyman). Session with George in p.m. Dinner with George, Eric, + Lyman at mess. Spent evening at Eric's room, talking. Back to bed at 11 30

Monday April 26. - Arose 9 30 a.m. Breakfast hotel Reported to M A + met Gen. Peabody. Lunch at Club. Spent p.m. again with George, tour through his works. Talked with Johnson met Col. Black (Jr. ETOUSA) Dinner with George as our guest. Walked in



Hyde Park - Evening at George's hotel  
 must frank discussion George to take  
 off for US 7:30 a.m. wade continuous  
 session advisable Home at 1.15 a.m.  
 in blackout. Evr our guide Fred  
Tuesday April 27 - Breakfast in room  
 at 10.30. To HQ to present letter to  
 Gen Rumbough made date for us  
 to call in p.m. in C to Chase hall  
 to open account Tea at Gunter's.  
 This place <sup>4.30</sup> p.m. called on Gen  
 R + had nice visit Telegram this  
 a.m. with info for Travis made good  
 opening for us. Called him <sup>ETOUSEA</sup> ~~from~~  
 on special line from George's office <sup>(He left at 7.30 p.m.)</sup>  
 Cordial welcome <sup>from Travis</sup> Date for 12. 15  
<sup>next day</sup> p.m. for drink\* (Commandered bottle  
 Bourbon from Evr for occasion  
 + was good thing! Met Travis at  
 door as we were coming in. Very  
 cordial greeting up to my room  
 \*See insert p 5

where had fairly frank preliminary  
 talk I suggested his arranging for  
 meeting this p.m. with M + we  
 agreed good thing to do despite it  
 being departure from our instr re  
 going thru Gen Davidson first I said  
 had phone of OK Lunch at Off mess.  
 Back to hotel + rested 30 min I called  
 + took us to call on M Spent 1/2 hrs  
 with him Very dapper + pleasant. Cordial  
 welcome We will proceed w/dsp of  
 present control mention of Dutch mun  
 + info re our bldg of <sup>30</sup> machines I venture  
 expl that Verkeyl must have confused it  
 with Gen. Whizzer M offers us welcome to  
 go thru the works I took me back to  
 hotel mentioned our holding out on  
 our gadgets + says control will not be  
 settled until we come thru as they  
 have. Dinner ~~at~~ as guests of Gen  
 Rumbough Raining so back to hotel  
 and to bed

\* Next to page 3

Dinner at Club with Swenson as our guest. Walked Hyde Park & biked to Soap Box racers. Very interesting.

Bed at 10:30 but too tired for good

sleeping

Wednesday April 28 - Up at 9

Breakfast hotel & out by 11 a.m. to Emb. & then to Clinic to have 3d tetanus shot.

Back to hotel at 12:10 to meet Jravis

Thursday April 29 - Up at 8:30

breakfast. Wandered around looking for

PX & got lost. Bought caps, hangers

Washed on wages to Wash 1st report etc. Lunch at Red Cross. Walked

& saw Liberty's. Tried buy pipe but no

luck. Looked at sticks. Dinner with

Gen. Ingle's cockbirds his quarters &

dinner at Connaught. Back to his

quarters. here chat. Bed at 11:30

Poor sleeping again & suspect tetanus

shot did it.

Friday April 30 - Up at 7:30

Breakfast & out by 8:30 to meet lady

Damey who took us Waterloo Stn

& entrance for Tidworth to see RI

Co. Lunch there & interesting visit

Back on train at 3:40. Stood up

most way back. Car met us at Stn

& back to Embassy pick up wage

for me from Cord. Taylor & I

dinner at Club. Home very early

& to bed by 9:30. Bed, fixed up

clothes in drawers, unpacked, washed

socks. Asleep 11:30 - 8, good

Saturday May 1 - Up at 8

Breakfast was going out to the Audley

met Eric said too late & then

back to hotel where met Denniston

at door. I had phoned him 10:15

p.m. night before & was to phone him

today but he made country call

at hotel. Very cordial. Breakfast

them to Embassy. I wrote reply to  
 C's message & sent it off. Then to  
 Gen Peabody who took up in his  
 car to War Office to call on  
 Gen Dandon Doonan D'Arcy both  
 silk hat & colorful costume. Gen  
 D very pleasant. Very formal call.  
 no discussion of business. Back  
 with Gen Peabody who stopped at  
 shop where I bought stick. Back  
 to Emb. Lunch at Club. Returned  
 hotel. Fixed up this diary to part  
 just above, rested 15 min up at  
 4 to call on Jamiston at his office  
 with Taylor & McC. Good visit. Reference  
 to Turkish by T whereupon D tells  
 us M had indicated we could  
 have anything we wanted on it.  
 Indicates careful pre-discussions  
 between M & D. Invited D to  
 Club for drink & he accepted at

once. Call to club where we talked  
 semi-shop for about hour. We are  
 to give D a schedule on Tuesday  
 of what we want to see in his shop  
 I'm to spend week-end with him at  
 golf as soon as can be arranged.  
 Dinner at Club with Eric as our  
 guest. Met Wes Jervey & renewed  
 Wash acquaintance. Dinner &  
 then to our hotel, where played 4-  
 handed rummy. Up to bed at 10.15.  
 Note D told us that M was prob not  
 going to Wash but that T prob would,  
 and soon!

Sunday May 2. - Up at 9. Poor  
 sleeping for some reason or other, maybe  
 tetanus shot still working. Breakfast  
 hotel then to Fin Office to get per  
 diem which came to \$52.50 or £13/0/3  
 which latter I got back to hotel to  
 read & had conference with Taylor.

& M<sup>c</sup>C on next steps M<sup>c</sup>C drew up  
 list questions to present to Damien  
 tomorrow, in writing. Question as to  
 whether we shouldn't press forward  
 on F at BP. Decision to come back  
 to see spend Tues-Wed-Thurs going  
 thru D's shop & then to BP on  
 Friday where I confer on SAC.  
 No lunch today, I walked around  
 trying find place to eat - all closed  
 up until 4PM on Sundays <sup>10-15P</sup> ~~closed~~  
 this pm until 4, then T & I went to Gutter's  
 for tea. I have walked to Westminster  
 Abbey, looked around. Special service at  
 6.30 for ATS. We came out just in time  
 to hear Irish Guards band & to see  
 the ATS march up to Abbey. Interesting  
 to see their stride, with arms swing-  
 ing high forward & heads up. Many  
 & all sorts of faces, young &  
 old, pretty & pretty awful. Then

walked back to Club to dinner. The  
 parks & trees are lovely. Rather cool  
 today & damp but it cleared up by  
 6 & was lovely thereafter. Dinner  
 with T, M<sup>c</sup>C, & a Col Seltz. Ad frank  
 of Eric's & M<sup>c</sup>C's. I wasn't very  
 hungry. Anne had tea at 4.30. After  
 dinner we all went for long walks  
 around the Serpentine. Saw Albert  
 Hall, Albert Memorial (two terrible  
 monuments on the whole but some  
 of the figures on the memorial are  
 nice. Saw <sup>"Peter"</sup> ~~Stately~~ <sup>"Pam"</sup> ~~Station~~ again.  
 Walked then to Hyde Park & listened  
 to various orators. Then to hotel,  
 hot bath & now in bed. Must get  
 good night's sleep - tomorrow to BP.  
 Monday May 3. - up at 8 after good  
 night's sleep. Breakfast then to Embassy to  
 see if any mail or messages. Dropped  
 schedule of proposed visit to Dame

stop on way to train to BP. <sup>815P</sup> ~~en route there~~ - We arrived Bletchley  
 at 11:55a + were met at sta. by Col  
 Tiltman with car + after few minutes  
 we arrived at gate where we registered  
 in Shaver directly to Train's office where  
 met De Grey, Train's deputy (a <sup>sharp</sup>  
 looking, small man) and Cooper, in charge of Air  
 We had a few  
 minutes preliminary discussion of gen  
 relative to their set-up into 4 services  
 evaluated, during course of which he  
 informed us he was going to Wash  
 1st plane after coming Saturday He  
 is to go alone In then produced a  
 rather large chart depicting sources  
 of their raw material, method of  
 getting it to BP, + routing there-  
 after. Dated chart a bit out of  
 date but promised to amend it  
 + give us copy. The no + varieties  
 of their sources are striking + very  
 much better than our own. <sup>JP</sup> Then  
 \* Ref to 2 A, AF, N, ABW

12  
 (private dining room)  
 to lunch, as prelim to which there were  
 gun + letters, scotch, etc. There we met  
 Birch (head Naval Section - incidentally Tr  
 had informed us we were to see all except  
 N material) + an oldish retired Engineer office  
 who (Tr told me) works for nothing + takes  
 care of all their construction. A very full  
 lunch (which put Mr C to sleep, for shame!)  
 and then we went to Tiltman's office for a  
 few minutes, where we met Col Cooper, asst.  
 to Tr who'd just recently returned from Hq  
 Brief disc re SS frame + work now in prog  
 in Tr's research section on security. Quib  
 was raised by Admlty when it would stand  
 up under 500 wgs per day but several  
 of Tr's assts. Result of test indicates poss  
 sol if stereo lag are not avoided. Tr doubts  
 whether more than 300 wgs p/day are to  
 be expected but if not more thinks not  
 poss to get more than depth 2 - which  
 could hardly be solved. Tr showed us the

small Brig SS frame which looks very good but does not provide for vertical displacement of base card. Ti then called for McO + Taylor + I were taken by Ti for quick survey of BP they would have 4000 workers there exclusive of maintenance + guard personnel. The main bldg a veritable looking structure over a rich man's country home. Huts of various sizes some still in use, others abandoned + about 8 or 9 new 1-storey brick structure. We did not go inside them as Ti said no time to get involved yet. Dr. Gray then came for us + we made a rather hasty tour through their traffic reception + communications center. The teleprinter room has 64 print + has a complement of 3 shifts of 48 WAAFS about 20 on duty in a shift, each girl taking care of 3 machines. Jfc bears a

symbol (words beg with A for Air, N for Naval etc) so that at sorting desk the girl in charge can rapidly forward message to proper section which is done now by belt conveyor but will soon be done by pneumatic tube. Waafs have preliminary before getting to BP but get more intensive training there. Some of the arrivals on "Nippon" recorder + girls take slips, trans late message direct + operate keyboard of Type X, thus saving one operation. Most of the arrivals at central teleprinter room but we were told in several cases service is direct to section involved, messages being read in the section itself. Teleprinters are maintained at BP, as also Type X machines. We were then taken to room where outgoing operational solved Jfc is passed thru Type X by oldest + most trusted Waafs who operate machines, setting up keys (they

now have about 16 sets of keys). There are 60 Type X's in use now. Then saw the radio room where direct keying of transmitters by remote control is used to get the cipher t/c to ops hq. Also receiving radio signals rec'd here in cipher room from the special com system is a most essential element in their operations. Auxiliary power equip available in case of emergency. Saw switching central for teletype service. Promised to permit us to go more fully into com system later. Then rejoined Tr + W.C. & after few minutes departed for 4.52 p.m. train. Failed to take up our passes! which we turned in to driver of str. wagon that took us to Str. Arrived Str. 6:15 p.m. Then to Embassy - no usages.

Then to Club, dinner, short walk to hotel 10 PM

PS Add. White stated that on all outgoing of usages on Type X they depend to insure no errors. I suggested random encipher depth up, which received new idea. De Grey queried me on practicality & when I assured them it worked for us I think they are going to try it, as possible time saver.

White said they had 260 persons in com center, exclusive of the teletype personnel.

Saw also high-speed Creed reception, tape Morse, tape than passed thru translator & record slip than posted up on sheets. De Grey said its high speed enabled them to receive large volume t/c that were direct from radio receiving stations.

We also saw Vanox terminal - BP to NY & sent a greeting from Taylor & self to Wardman & Bayly. Later W.C. filed a greeting to our wives, to go via same channel.

Tuesday, May 4 - Today spent mostly at D's shop. Lunch at Red Cross place I took us to his Club "East India, Sport, + Caledonia" an amalgamation due to bombing out of two of the three. Nice place. Dinner at our Club Spent evening with Kip in our room discussing SIS in West. M<sup>r</sup> C has copious notes of what we saw today. I was much impressed with amount of work done by so few people. Met several of D's people, Mr. Reek, Mr. White, Col. Warden. Spent 2 hours in Distrib. + Record Section, in charge of Earnshaw-Smith (who was out today) but actually run today by a Greek prof of Cambridge named Jenkins. A Miss Hill assists in record maintenance. Two old P.O. women do the reception + sorting + forwarding (to sections) of the

incoming file. After lunch I spent an hour with Mr. Oswald White (ex Consul-General Inverness) in charge of I section. Met Col. Warden there. To return for more talk with him tomorrow.

Wednesday, May 5. -- Up at 8, breakfast, then to PX for cigarette. Answered message from (probably) Kellback telling of progress on JAC, + requested them to use System I-P-U instead of Special Hayes. Also reported our progress + told of forthcoming trip to BP then to D's shop where we went into details of G. Floadora but Mrs. Patricia Bartley, in charge of G section, a most charming young woman, sent P.W. Filby, Mr. Tomlinson, + others lunch as D's guests, with Mr. Earnshaw-Smith (D's deputy + in charge of Dr R Section), Mr. Hope, head of Commercial Sec. Went to Bagatelle Restaurant, delightful conversation with Earnshaw-Smith and Hope on my right + left. Both are Shakespeare



devotees. Cocktails ("Jim + French") then  
 a very nice lunch, after which we returned  
 to D's place for further discussion on I. We  
 drafted paper on revision of Kubov on back  
 log + are to see revised draft tomorrow met  
 Mr Väterlein, dean of crypt, who is over  
 75 + has been in work for 50 years. Told  
 me R's adopted 1-time syst in 1916-17 RFD  
 had staff of 5 beginning back in '96 Austrians  
 most clever + had R's pointer systems all  
 very simple 1-part cdes which remained in  
 effect for long time however, for exple, used same  
 one from '93 to 1940 V is still quite active  
 mentally + gets quite keek out of reconstruct  
 2-pts. He doesn't care for "machines". We  
 left at 5:45, walked to Haus Opera House  
 where we saw Ligier's The League Fleet  
 Very good performance + we had good  
 seats which I purchased at Selfridges  
 at premium of 1 shilling, making cost of  
 seat 10/ Opera began on dot of 6:30 +

finished on dot of 9 Crowds scurrying to  
 get to buses etc before darkness so we walked  
 to hotel + had dinner w/ (I bought us a  
 bottle of wine (£9<sup>00</sup>) + we had a very  
 nice dinner up to room, wrote I a letter  
 read paper a bit + to bed Friday the news  
 re Jan Andrews death. In flow account  
 Iceland. Jan Kay assumes end temp  
 of FTOUSA

Thursday May 6 11p at 8 Times had  
 cold. I went to pick up stick purchased  
 last Saturday. Cost £30<sup>00</sup> - new cks + got  
 back £7/7 (note 4 03 5 plus 2/1000 res-  
 plus stamps) to Embassy, guided by a nice  
 P.O. employee who pointed out places of inter-  
 est. Then to D's shop where we talked  
 with I trans staff. Were much impressed  
 with high calibre of man - practically all  
 ex-Consuls or Consul-Generals who had  
 had years of experience + ting in Far East  
 F.O. apparently glad to make them avail

able, realizing value of their services in this field. To lunch we took Miss Bartley to Bagatelle. It was a 2hr affair by time we got back but the y.l. was much pleased & good company. She was born in India where her father (now retired) was judge in high court. Back to work where we went thru J-19 & Purple section. Two men recover J-19 keys & about 7-8 women fell in values much impressed by efficiency of key-recoverers (both cpts loaned to FO) who prefer hand-op sol to Tee-whiggers (& besides they have no IBM base). One key recover this a.m. by 1 man in 1hr as result lucky guess on width. Saw one pump machine & one built here, which is much bigger & doesn't work as well. Servicing of machine by service man from Broadway. Talked to woman who works on pump keys. College grad (does she know any J?2). Saw 1 girl who operates Pump = Group

here trans practically all Pump, get all J-19 keys out & trans % of it, do very no LA (which is looked at in group - Com Section & is nearly completely processed). Then returned J & got revised draft of proposal for discussion work on Flora Han to Embassy to draw up tele to Wash on proposal. Packed belongings, prepared to take everything to Rajp. In bed late.

Friday  
~~Thursday~~, May 6 - Up at 8, left at  
 hotel, settled up there & found necessary  
 cash more than checks (\$40<sup>00</sup>) so as to settle  
 up & have some £ to take along to B/P. I  
 found ill & not well enough to travel. Decided  
 to take all my belongings to B/P & what a load!  
 Went out to Embassy, pick up some papers &  
 also M.C., with whom went to Euston Sta in good  
 time. Porter found us good carriage & we had  
 nice ride to Blatchley. Car awaited us & we were  
 whisked to B/P. Other members of Conf were already  
 there & anxious to start. Lt Col Pat Marr-  
 Johnson, from Delhi, India, Lt Col  
 Sandford, from Brisbane, <sup>Sulphur</sup> Australia, Major  
 Thompson, head of J-mail ops at B/P, Capt  
 Nank, also of J-mail ops B/P who serving as  
 secretary Met. Harris & De Gray M.C. was  
 it once whisked away. Harris opened  
 Conf in his office with well chosen words  
 of welcome to me as guest of honor, to which  
 I replied in suitable form. Harris outlined

the scope of Conf & main projects. Travis wanted me to act as chairman but I declined in favor of Iltman as leader in host government. We adjourned for the usual 2 1/2 hour lunch. Reconvened at 3<sup>15</sup> at the restaurant & took up personally the matters before us. At 4:15 h<sup>15</sup> C called & said he was very tired & how about knocking off for the day. I thought this rather strange but explanation later from h<sup>15</sup> C was that he felt De Stoy had purposely reached him through the F. show & whenever he stopped to examine anything closely he was dragged off & the papers were whisked away so that he was pretty sore. At any rate I acquiesced & a car was sent to take us to hotel at Newport-Pagnell, a small town about 8 miles from B.P. "The Anchor" which is a pub but very clean & quiet, no facilities for laundry or bath & one young woman takes care of all. We are apparently the only guests. We unpacked a bit & then

went for a short walk to see the village. Dinner at 7 & the food was excellent. Trunk spotless but no napkins. We talked at length until about 9:30, & explaining F machine & bombs etc in general to Al. I felt pretty punk with head cold coming on so got into bed with pyjamas, my quilt sheet of wool, & my woolen bathrobe, woolen footwarmers. I got warm in a hurry & fell into very sound sleep until 8:45 when "hot water" pitcher arrived at the door dressed, had breakfast of bacon & egg, good tea. Car came to fetch us to B.P., arriving at 10:15 there. Started in work but was soon interrupted by call from Travis who wanted to tell us that we were to be shown their "nat. h. machine" (modification of what he had told us the day before & etc, we were not to be shown anything on that side (at request of our navy)). He asked we not say anything

back home re Navy having requested this but we could say merely that we were not shown their part. Trans said he frankly did not see why he should bear the obloquy for this sort of action & wanted it straight so far as I was concerned. Then I rejoined Conf where W.C. de Szlo RAF gave data re communications facilities for passing the. Then had further discussions of JAC. Lunch again for 2 hrs Trans was there, just prior to taking off for US via Bomber. Gave him personal message for F & wished him good luck & safe flight. Doubt whether he'd get off from Prestwick because weather has been so bad. [It has been unseasonably cold, damp, & windy now for several days.] After lunch we got down again to more serious detailed discuss re JAC & reached conclusions, some of which were embodied in telegram to AH. Conf going very smoothly in a

most friendly spirit of cooperation. We had no representative from Canada but nevertheless took cog of their interests. We adjourned at 5:30 p.m. & Mrs Johnson took me to Tiltman's home which is close by gate to Park. Had a couple weeks Scotch talk, then Mrs T & daughters joined us. Dinner (prep by Mrs T) very pleasant, substantial food (chicken soup, hot sausage roll, vegetables, choc pudding). Set around fire after dinner (coffee, tea) listened to radio at 9 p.m. re taking of Tunis & Bizerta. At 10 T had car call for me & take me to Newport-Pagnell, reaching hotel just as it was getting really dark. Talked with M.C. a while - he absolutely amazed by what B have here - beyond all his imagination etc. Taylor was already in bed & did not join in conversation therefore but I'm sure he is just as impressed. I wonder whether everything in B Army is, even

as well. It is certainly good! "M<sup>c</sup>C  
 It's superb! But it's certainly not  
 military." That is also one of things  
 that has impressed me - rank or status  
 cuts no ice - whoever is best at a job  
 has charge. I said Strong should come  
 over, M<sup>c</sup>C said no chance I said Clarke  
 He doubted whether C is smart enough  
 to grasp any of the conception here & the  
 sheer wonder of organizing achievement the  
 B have to their credit To bed in the cell  
 but well-wrapped & I had a very fine  
 sleep again

Sunday, May 9 - up at 8 Breakfast  
 ham & egg! again and nice tea Car  
 was late in coming - to 10 a & we  
 got to B/P at 10.30 Had a session  
 with Tiltman & May Morgan on their  
 research section It is a very loose-  
 knit affair - composed of a very few -  
 but the most able - cryptanalysts whose

primary job is diagrams" after which they  
 pass the matter over to exploiters Tiltman  
 is leader, then May Morgan, Capt Morgan  
 Mrs Bradshaw, Mr Sansbury No need say  
 how engaged in IIRH studies on JAC as specialty  
 but have other JAC problems also Lunch with  
 De Grey, M<sup>c</sup>C, Taylor & met Cmdr Bradshaw  
 who is Deputy Dir for administration & has a big  
 job - feeding, billeting, transportation, supplies,  
 finances, etc Bradshaw retired few years ago  
 but knows sound crypt He sees all the to keep in  
 picture! After lunch at my request De Grey  
 got my chart & we went through it carefully  
 thereafter spent rest afternoon with Cooper,  
 Air Section & had most interesting tour through  
 his works met his Vette & his m in hall  
 & had chat she seemed thanking me for his  
 courtesy in sending present. Saw Eads  
 after tour had tea with De Grey & learned  
 what details re their general operations  
 Told us about their Special Com Unit

for handling their stuff; the A type crypta units for Army, B type for Corps; projected R type for feeding from front by radio intercept. He obtained by A or B units the amount of care + thought exercised by GOCs to protect the MSS stuff is amazing. They have their own rep in the field assigned specifically for purpose, with own crypto staff + 1-time pads. Stuff handed over to only 1 or 2 people + great care taken not to disclose by operations fact that ops are based upon MSS stuff. The GOCs rep is not attached to the staff but is a sort of MSS-Gestapo watchdog with full authority of Min Def (WC). Behind him car came for us at 6:15 - we returned to hotel. Had drinks + excellent dinner. Now writing up this + discussing things. Note re M<sup>c</sup>V "bon mot": "We don't do crypto but

cribby" He did one in the last 2 days which gives a 5-way crib! He says he should have finished it 2 years ago - when he got down to it it was struck by lightning he got it in 2 days. Another thing M<sup>c</sup>V impressed on me was first that metric work is of course useful in itself but also that it affords 1st class cribs into E or other stuff.

Monday, May 10<sup>th</sup> - up at 8 after good sleep although M<sup>c</sup>C + T + I sat up until 12<sup>30</sup> talking + drinking up my whole qt of Scotch! Terrible weather - cold + rain all day. I had put on my long underwear + my sweater, so was quite comfortable except for cold feet. Col Mann Johnson from India is suffering lots from the cold since he usually works at 110-120° at home + these rooms at B/P are ghastly cold these days. The Englishmen keep their windows open all the same! They seem to be immune to the cold + damp. Their working quarters, compared to ours at home, are veritable rabbit warrens,

and with primitive conditions as to chairs, furniture, etc - Car came for us late as usual (10<sup>10</sup>) & we had plenty time for breakfast - which was some canned tangerines! (excellent) and scrambled eggs. At B/P we resumed our JAC Conference and practically finished up what we could. Final conf to be held on Monday, May 17 of Brig Haines, chairman of Y Com here. Lunch at B/P, then session with Mr Welshman on E from 2.15 to 4pm. Had this session with Col Pritchard & associates there until 6pm. Talked with Tilt until 6.30 on J pol. Dinner with Mr & Mrs Duch at their hotel at Bedford Arms. Lt Cdr Dudley-Smith & young, attractive wife were also guests. We had Irish whiskey - 3 rounds - and a pretty nice dinner. Mrs B works at BP & so does Mrs D-S. Pleasant evening chatting. Bush showed me street down from hotel - oldest type Elizabethan structures most attractive. B had a car with very pretty ATS driver take us to Newport Pagnell at 10<sup>15</sup> just about dark. I am suffering from lack of bath! Facilities at hotel very plain &

I should be there early evening for it - which I haven't been able to manage. In a.m. there is no hot water except for shaving, which is brought in pitcher. It has been terrible weather & even the British complain! Rained all day, and cold. How they can work in their offices at B/P astonishes me but I suppose they must be accustomed to it. When got to hotel M-C & I were up and wasted on some scotch, which we purchased at the pub downstairs. Mrs Fenn (prop) gave Al several 3-penny bits & we had good chat there, then continued up in A's room until 11.30. I had to do my packing as we are to go back to Fdn tomorrow. To bed at 12.30 & a good sleep but not enough probably.

Tuesday, May 11 - up at 7<sup>30</sup> finished packing, decided to leave large bag at B/P. Packed again for egg! Car came early (as per my request) at 9.20. Loaded up (me itching from lack of bath, longies, & sweater - but it



wasn't any too warm at that so B/P at 9:45 + then immediately to my <sup>second</sup> press on E with ~~Wolshuman~~ <sup>Club</sup> ~~Wolshuman~~ <sup>Wolshuman</sup> on the W/T side of picture, which is very interesting. Saw Mrs Wolshuman who is a Capt in the ATS. They had arranged a schedule for us (Col Mann Johnson + self) which called for 1/2 hr with <sup>seems</sup> ~~seems~~ but we stayed at least 1 1/2! He asked had to be modified! And will be again, as I propose to go slowly + get all I can (no rushing thru for me) then had session on theoretical crypt side with Maj Babbage - 12<sup>15</sup> to 1<sup>15</sup> p lunch, where I met Eches + Clifford (his relief) At 2<sup>15</sup> back to Babbage until 3<sup>15</sup> then rushed to get to HQ where A + Tal were just entering car to go to Str. We waited at Str for 3/4 hr got to Str at 5:10, taxi (country of Rumanian who got his eng degree at Carnegie Inst then was attache R Leg at Wash for 20 years, now with "Free Run

in Gen Ito Embassy. Several messages for us but no letters then to Park Lane - where I had a bath at last! Dinner at Club + traugler back to hotel. Read over all my notes, sorted things out + now in bed wash-socks + longies. Gave 4 shots to Edy + had suit pressed. Just + nevertheless wrote letter to F + folks in NY (1st time) now 11:50 p + must to bed (PS note re p/l message from G Cuda to Allied Cuda about May 7<sup>th</sup> re ship with Brit pres locked in hold. Quite com-<sup>DN to</sup> munitions! From NA intercept Cheadle → B/P → NA all in time to save ship. Only 1 man killed + 1 wounded.)

Wednesday, May 12 - Turned out lights at 10:30 pm last night but soon decided no go - too many things on mind that I wanted to write notes on. Regret realized it was 1:30 am. Jay's first sleep long ago. Glad not to have to get up early - no engagement for this a m. no

Slept until 9 a.m. (not too soundly) and had breakfast in room with T whose cold is worse and decided to stay in all day. Dressed and hurried over to Embassy - letter for me! First one from E, dated April 27, postmarked 28<sup>th</sup>, via 30¢ air mail, which arrived in my hands only today - 15 days! It must have gone by boat, but glad to hear from home. The other two partners have nothing so far. Worked on notes and composing telegram with Al, then to lunch at Club with Seltman as guest of ours. Pleasant chat + good lunch after which I returned to Emb to continue working. I sent a long one to Cord, Al sent several, one long + 2 short ones. They take time to prepare though + it was 6 p.m. when I finished

Al had dinner date but I wasn't hungry + decided return hotel + get good night's rest. Stopped in little pub in back of our hotel + had beer + sandwich. Ted is better + went out to get a bite. I've rested, read paper + now this I smoked my new (2<sup>d</sup>) pipe (\$1<sup>25</sup>) now + it is terrible! Varnish inside!! Read Ted E's letter. To bed soon after I do a bit washing. Wish I had lot more Ivory Snow - can't buy soap here without ration + ldy facilities in the country are nil + at the Park Lane quite expensive. Celso is pressing - 80¢ for pressing a suit! X - I am coming down with a cold. Rather poor sleeping.

Thursday, May 13 - Restless night again. Taylor probably transf'd his cold to me. Up at 9 + feeling rather low but went about my

business. Spent all day at D's -- show going over the material in a detailed manner, under Cathy, head of section. He has been with D since 1925 met several fairly interesting people but on the whole I regard them as practicing "amateurs" If they didn't have all the wealth of background material they'd not do so well and their working quarters are a rabbit warren - but somehow they do 1st class work nevertheless. Lunch at Red Cross where I was eyed askance again - they are snooty about the place being only for people in uniform I put in my application a couple of weeks ago but the matter of admitting civilians is being taken up on the "high level" !! Which amuses

me a lot next year's contrib to RC won't be what it was this, so far as I'm concerned. Worked all p.m. again in I section. Dinner at Officers mess with Svensson & later to his flat where worked on lighters - his & Taylor's Jimmy re lighters - I bought my simple one in Wash several years ago for 15¢ It is the only one around here that really works all the time, much to the disgust of those who have the expensive \$5 dollar ones I fixed D's (maybe) but Eric's - no, because we couldn't figure out how to insert the wick - even if we had one, which we didn't I was going to go to bed at 9 & here it was 10:30 already so we scurried home It wasn't pitch dark yet or maybe the moonlight was sufficient to light the way Went to bed at 12 & slept poorly again Woke up many times in the a.m. almost decided to skip the

Friday, 11 May 1945  
 day in bed but got up (grumpily) & went about my business, feeling pretty dragged out, though. Then the cold is working on me. Over to Denmark again arriving there at 10:30. Looked over the Port & Braz stuff. Met Excell, head of sec who was Botanist at British Museum & his wife who was also Botanist & is working with him now. Excell & his crew are also self-trained amateurs but doing good job. They go in for more detailed study & work & records than we do. Also they get considerable help from direct contact with F.O. which sends them docs. regularly. Met also young Cooper, brother of head of Air Sec at B/P. Young C. has just recently returned from Australia, having been among those chased by the Japs from Hongkong - Singapore - Java. Deniston took us to lunch at Taylor,

Excell, Cooper, & self) to a swanky place again where 1 round of cocktails cost him 1£. The food must have been correspondingly expensive. I said must be one of 3 alternatives (1) D is rich, (2) he gets a large salary or (3) he is going to bankrupt himself entertaining us. When I stated this to Alfred Catter (who went along) said "Probably has an entertain-ment fund" which I think is probably true. I think Trans or Tiltman once hinted that very thick. During course of lunch I told D about the GCS examination paper of 1925 & D was greatly astonished I should have gotten such a thing & said it must have been skullduggery of some sort. He could hardly credit my statement that I'd got it regularly through our MA here. He said somebody in FO should have his head chopped off. After

lunch there was bit' more discussion at D's office but movement to go into another section so we decided to suspend for the day. Returned to Embassy where there was a message for me. At home still writing cables to Clarke but we dropped him out & went to see region about St. Pauls. Great destruction there but all the debris has been greatly cleared up. Walked about quite a deal & went into Guildhall which was well demolished except for the hall itself. Stopped in for some beer at a nice pub when 5:30 came (opening hour) Dax to Embassy - more messages for me. Dinner (after bath & rest at the Park Lane) at #8 Audley St where I ate well but not too wisely, judging by the "back-

fire" since then. Went back to Embassy, listened to Churchill broadcast from the White House, wrote letters to E, walked back to Park Lane. Lovely evening now 11pm & time for bed. Hope for good nights sleep.

Saturday May 15 - Wrote this on train to B.P. Sunday pm I up at 9 after pretty good sleep. To Embassy to see if any messages or mail none of latter but message from Cordre business over to D's shop & saw into H. East, French, & Com material. Had engagement with Turing at 10:30 but he didn't appear until 11:30 not inpt but told him about mod on X61753. Tried get some info out of him re what we might be able to do with E at AH. Gather that he thought we could do something OK. He was interested in our electronic devel but I fed him nothing.

except what we might expect in way of  
 speed. He is off on a weeks leave I  
 was astonished to learn that people of  
 GC&CS get 4 weeks leave with pay -  
 at rate of 1 week 4 times year. Talked  
 with D re this & he told us it was  
 wangled out of Civil Service but I think  
 the way they work it it is more or less of  
 a subrosa thing. Those running GC  
 & CS recognize the high pressure work  
 & the value of these distributed leave  
 weeks & apparently everybody takes  
 them. I think it would help us  
 too. We left RE there to sleep in a  
 chair, he having been up until 2:30  
 finishing long tel to Clarke which  
 he brought to us at midnight in  
 dicty & we suggested changes that  
 kept him working late - he has  
 sent reams of tel home on the E  
 matter I & Taylor & I had lunch

at RC where I straightened out matter  
 of my acceptability - somewhat in to be  
 admitted, I guess, as special concession.  
 Returned to D's place after good lunch. The  
 RC place is OK in that respect. I worked  
 about 1 hour more in FF section where met  
 very attractive young woman - Miss Hanson. All  
 personnel of F section women. Head has been  
 with D since last war. The number of old-timer  
 persons is very striking & is probably the  
 most important factor in the success of the  
 GC&CS. Taylor had date with D for week  
 end & they took off at 4:30. I was also  
 invited several days before but since I am  
 to be there next weekend & had work to do  
 decided to leave the field to T this time &  
 not overdo the hospitality on D's part. Al  
 & I had dinner at Club. Had an alert in  
 Idm this pm about 5:30 - lasted only 10  
 min. No action. I was told today that  
 each time there is an alert in Idm the

men on Merchant Marine vessels in port in Sdn get bonus of \$125. They get no such bonus if in submarine action in crossing. This info from a Navy warrant officer at our table at RC. Today I met Karl Compton at bar at Officers Club. He with Tom Pines & Gen W<sup>c</sup> Lellan had short talk with Compton. Nice dinner with Al after couple martinis (gin & sherry type). Al wanted to smoke heavily & I didn't, so I left him after dinner & took long walk down Piccadilly. Back to hotel at 10 & packed up a bit. Occupied room alone & it cost a good deal more. Slept rather poorly again - up at 9.

Sunday May 16 - Breakfast followed by walk to Embassy where there was message for me necessitating going over to George's office to phone Liltman on

private line to B/P. It seems that Capt Nank sent message to lieutenant for trans to get data which I had already asked for direct. Long walk to ETOUSA HQ & back for this purpose. Collected 15 days per diem & am in funds again. Lunch with Al at restaurant next door to Embassy - rather swanky & expensive as my very simple lunch cost 9 shillings, five of which were for one drink. After lunch sent reply to message of morning, then returned to Hotel to check out. We were to take 5.10 train from Euston Stn & there wasn't a great deal of time. I hurried but nevertheless nearly missed the train as I couldn't get a taxi at Hotel & had to walk to Embassy to pick up Al. Taylor was to be at Hotel but didn't show up & that delayed me too. Just made the train with 1 minute to spare. Lucky to get a seat. Auto met us at Bletchley & we

were taken to "The Swan" at Wolburn-Sands not as small as "The Anchor" at Newport Pagnell and I don't think it will be as comfortable & quiet. Beautiful lawn in the rear where there is bowling "Sat" in the late afternoon sunshine & had a glass of beer before dinner, latter being very good. At our table is a Mr. Low who works at BHP. He is professionally a writer (Life of Gibbon & some novels) and a fine gentleman. He took us for a long walk of the surrounding country after which we had some beer & sat around talking until midnight. I did not sleep well again.

Monday, May 17th - I don't understand this further to sleep unless it be that I must not drink any tea, coffee, or alcohol whatever. The pleasure of my visit is being much impaired by my inability to get good sleep. Perhaps

I'm held out from being so much on the go and shifting base so much, together with minor excitements due to rushing Mother & you. I've used up about  $\frac{1}{2}$  of my little  $\frac{1}{2}$ gms amylals & must go easy with them to make them last. Maybe I should take off a couple of days and stay in bed - but the bed is very hard! Breakfast this a.m. of porridge, poached egg on toast, tea now waiting for car to take us to BHP - Evening, 10<sup>PM</sup> A full day. Bus took us to BHP & soon after arrival met Brig Harris, who remembered me (or said he did) from Wash 1924 Conf. There were also Maj Grant, on WH side, Sq Ldr Laurie of RAF on the side. Eric Swenson, in addition to the regular members of our SAC Conf. We got down to work quickly, De Gray presiding. Subcom apptd on communication matter, to which I was appointed for U.S., to meet at 2.30 Main Session



finished at 12 45. Lunch with the whole crowd Subcom met & finished its work at 3 30. Rest of afternoon on various discussions, approval of draft of minutes of a m & p session draft of tel by me to AH Cocktail party at the Tiltmans at 6 30, small gathering & several wines. Cuck Jones took us in his car to Woburn Sands Dinner - good soup & fish - and then an hour's conf with T and M-C & now ready for bed at 10.30. Teltman insisted I see the post medics, who gave me some pills & ovaltine. Will prob sleep like a log tonight as am very tired after several nights poor sleep. I & M-C & I discussed what program is for rest of week. I ~~to~~ stay here until Sat. They prob going in to Eden tomorrow night or Wednesday. Al said or asked me if I wanted to go home

with him next week & I think he was quite serious. But we pointed out some things he yet hadn't seen which will take more than a week in pure. - Note, I've not received any word from Cookman commenting upon my recon that I be allowed to stay as long as I think was Tuesday May 18. - An excellent night's sleep. I heard two alerts - dumbly in my sleep. There was a fairly heavy raid (20 planes) over London on Sunday night which we missed. What it was last night I don't know yet - The weather has been lovely for four or five days now. Brilliant sunshine and mild temperature. Even the English are surprised at it. There was a Colonel Lyett over from Eden at our table last evening. He comes to get every week for a day, representing liaison with MI-8. When I introduced myself - he knew all about me in detail.

The British have desecrated all BH person  
 alike pretty widely. Also Mr Low said  
 he of course knew of me, etc. - Iltman  
 gave me pretty good news about what is  
 going on in Wash on the controversial  
 discussions. We shall probably do things on  
 F both over here under George & back at  
 AH which is good. - Bus called for us & we  
 journeyed to BPP. Worked all day there with  
 a break at lunchtime. Very interesting show in  
 F watch - spent all pm there. Home by bus at 6:30  
 Good dinner after quick bath. They found a coun-  
 dress for me & maybe somebody to press a suit! A  
 great achievement. Took walk after dinner  
 most lovely countryside. I've never seen beautiful  
 trees, evergreens are especially lovely. The weather  
 continues excellent - full moon up by time it  
 was getting toward dark. Worked on telegram to  
 AH & discussed same with other two. Bed at  
 midnight. Aveline again & a pink pill from  
 J's medica.

Wednesday May 19<sup>th</sup> - Good sleep up at  
 St. Onell's (with bits of ham & onion) & not  
 recall. Yesterday a dear old lady (Dorothy  
 a spinster) stopped Ted & gave him a bottle of  
 cough medicine - he's been coughing very hard.  
 This morning she asked him how he was &  
 his reply indicated much improvement, which  
 he attributed to the cough medicine. Said she  
 "I just couldn't allow such a lovely pair of  
 eyes to be dimmed by so bad a cold!!"  
 To BPP by bus (incidentally, BPP owns &  
 operates its own service, which it had to  
 set up in order to get personnel to & from  
 work-scattered as they are over the  
 countryside - & the service is good.)  
 Spent day in #IV I S going over G BPP  
 & allied subjects. Spent considerable time with  
 Webster (Int), Shinar (Int), Ingleby (Break),  
 Talks with De G - outlining my future  
 steps. Can't see Nas Hag also. Lunch  
 as usual with De G et al. W=C left

for Ida in a m & T early in p m so am  
left alone here. Returned hotel via bus  
at 6.15 Arrived in time listen WC  
broadcast from Wash, speech before  
Joint Session. Marvellous orator. - nice  
dinner, at table St Henderson & his.  
Betty, too from B/P Walked briefly  
& to bed early. There was an alert  
last night but I was only dimly aware  
of it Ida has had a good many since  
I left there on Sunday - would have  
liked to have been there on Monday  
night as understand lots of fireworks  
Hyde Park guns Good sleep, I hope  
Thursday. May 20 - Yes, good. There  
was another alert - it seems that if  
any <sup>enemy</sup> planes are over an adjacent zone  
they sound the alert here. Though the  
bed is like a board (almost, compared  
with what I'm used to) I sleep soundly -  
probably the pink pills & the Oodine:-

Had quick & somewhat warmish bath  
thus a m. Travel finished, even as to battle  
in the evening just before dinner but I pre-  
fer a m. & it paves one more redundancy &  
messy. The luck is to get into bathroom  
in time. Bacon for breakfast plus the usual  
 oatmeal porridge Worked steadily all day  
at B/P At lunch met Gen Davidson (M) &  
and Brig Home, from a few weeks ago  
where he is? In on British staff. Both  
very cordial. This session went up after I  
attended to Fall day & news at the  
achievement. Saw - won't be for out time  
Very compact compared to ones & news out  
by Wrens Lovely message from Elizabeth  
through Mardman. I suppose Helge  
prepare summary telegram and copy  
must send it off tomorrow. Expectation  
to see C party for 24th. In her - courtesy  
of Gen Rumbough. Tactful re letter  
briefly. Yesterday talked briefly to 11:-

in Sdm = one wage of no import, no mail from home. Home at 6.30 & read Times, which the Chef saves for me. Incidentally he is a 1st class cook. The food here is really excellent & my ideas of British food must be revised. The soups are always delicious, the meats & vegetables always nicely seasoned & tasty, maybe this is seasonal place, but the food is far better than at Park Lane. I had pint of "half 'n' half" (half "mild", half "bitter" beer) which is rather low in alcohol content & not so good to my taste as our beer, which they call "lil" "lager" & which you can get only sandy. I know "stout" is rare. A drink called "mother-in-law" is (1/2) stout (1/2) bitter - hence the name. Saw some good tennis briefly today & yesterday on Rpt courts. Two girls playing today were really 1st class.

fast & hard hitting. Yesterday saw mens doubles - very hard & fast. I counted 7 or 8 station wagons & a dozen large buses today on station at Rpt - perhaps the full complement of transport but am not sure - my cold is improving very slowly - this evening my head well stopped up but otherwise OK. I think this bathing in bath tub not so good for me as shower - probably catch more cold every time - no matter how speedy I make it as have no chance to use cold water afterwards - glad I bought Kleenex - supply is getting low though can't buy it even at PK where it is reserved for female members of US force also. Gussel was right when she suggested B.O.T.P as I've had occasion to rue failure to do so. - Got my laundry back today - 2 shirts, 2 pair shorts & 2 undershirts, 3 pair socks, 2 handkerchiefs

! for pyjamas. cost 3/6 = app. 65¢,  
 which is very fair. My suit to be  
 pressed (since Tuesday) not back yet.  
 I was regarded as being foppish. I  
 guess - nobody doing that nowadays  
 apparently - and they look it. I must  
 say, especially at B/P. On the whole  
 I'd say we are very much cleaner in  
 home & office - but then there's been a  
 real war here now for 3 years & there  
 isn't any labor or material for clean-  
 ing, painting, paperhanging, etc things  
 have to do as they are until the end  
 of war. - hot such bright sunshine today  
 I believe our spell of 1st class weather  
 will soon be over. Warm enough yet,  
 & I didn't need sweater today even  
 indoors. - As usual, I itch a bit, be-  
 cause I feel the need of a haircut.  
 Where to get? - I'm afraid I will  
 need to get some money from Wash

or borrow some from Al, who assured me he's  
 plenty. The \$7 p. claim is not enough to  
 enable me to live at Park Lane - where I  
 spent more & where other things are con-  
 siderably more expensive, such as 80¢ for  
 pressing a suit. If I make it on the 17 I  
 shall do very well. Can do it at Wolburn  
 Sands easily enough, I think, though am not  
 sure what the cost per day is yet. I got a  
 check from Al for £10 before he left & I  
 will have to use it as I left £15 foolishly  
 in my folder at the embassy before coming  
 up here, failing to realize I would not be  
 back there for couple weeks. I shall man-  
 age somehow, though I hate the feeling  
 of uncertainty that comes with shortage  
 of funds. I have only \$30 of \$100 Travel  
 checks left & \$19 in cash at Embassy &  
 the £15 mentioned above. - Saw a form-  
 ation of 18 planes flying NW tonight -  
 Tomorrow is our 26<sup>th</sup> anniversary & in

feeling quite a bit lonelier & tonight  
lots of people downstairs in the pub =  
apparently the congregating place for W.S. =  
Brown Sands although there are here (as at  
all other small towns) several pubs all  
well behaved places though, & so on with  
its dart games & tables. Here they operate  
tables only for news - if had music etc  
would have to pay extra tax - "entertain-  
ment tax" Learned today that British up to  
1926 paid income tax out of current income  
but it was found to be impractical & they  
changed to our present system! - I saw  
two wood-burning-fuel trucks on the road  
today when on a short walk after dinner  
I'm looking affairs & puffing & blowing  
- Had a nice long chat with Mrs Malone,  
who runs the Swan, this evening. She  
brings the hot water for my overtime. Has a  
son in Army & a daughter in the Sand  
Army. To bed at 11:20.

Friday May 21st. - Wakeful until 2:15 when  
decided to take pink pill. Damn this morn-  
ing! Guess the long days without physical ex-  
ercise responsible for poor sleeping, as can't fig-  
ure anything else as cause. Of course, what  
I'm seeing at WSP on Fri is very thought-provok-  
ing & the thinking of our set up & its shortcomings  
and what we shall have to do on Fri works of  
& when we do - Today is our 16th wedding  
anniversary, and I'll try to get special work  
to Elizabeth thru maidment but am somewhat  
embarrassed to ask favor - Writing this while  
waiting for bus to go to work & am sitting on a  
stone smack at the center of W Brown Sands,  
by memorial to last war dead. The children  
going by on way to school - Did get nice msg  
off to Elizabeth thru courtesy Jiltman & Deb  
All day continuing on Fri intricacies of set up  
here. Quite complex organization & very de-  
tailed record keeping to ensure that nothing  
is overlooked. Checks & cross-checks &

again. And the most amusing names for things & processes. The "Cat", "Kitten", "Hank", "Parker", "Dogs Body", "Horrors Graveyard", etc. etc. Each section with a jargon of its own. Built up as the words & needs dictated. Even the other sections can hardly understand. —  
Worked all day until 6.10 Dinner with Mr Low & Mr Martin (who works at some secret political activity center near Wolbourn Sands) & had pleasant chats re origins of names of places hereabouts. Leighton Buzzard for ex comes from hay-town. Beau des Bures. Towns ending in "ham" = home, bury = borough. Towns ending in "by" = "Rugby" for ex. are old Danish & there is a line of towns on the east coast which end in "by" & which mark the limits of the invasion of the Danes. — Long walk with Low after dinner, then pint of beer & bed. My bill for week to be prepared. — I telling hotel people will be

away over weekend. To bed at 11.15  
Saturday, May 22nd — Good night's sleep  
Bus to B/P after breakfast. Short talk with Jiltman. Car to take me to Sta for 10.54 train. Uneventful journey to Fins & taxi to Fins where no mail & 1 short telegram from Cord to me re seeing Turing & getting his OK on X6/953 — when can't give him any details re haircut at the Club. <sup>the H. REC. 1st time Wash!</sup> proposed modifications. Lunch with Taylor & M<sup>c</sup>C at Red Cross, then to Dammolous where prepared tel answer to Turing matter & summary of weeks work. Also complaint re hair failure gave even outline of news re negotiations in Wash. Letter to Elizabeth which gave to Taylor to mail at Fins. — D & I took underground to Bakerloo Station. Very long escalators down deep. Just made train in most uneventful journey to Lislehead. Walk from Sta to his house. Out then to watch cricket & have it explained to me what we call "rooters" & rooting is called "barracking" here &

is just never done. When the bowler does his pitch the crowd - maybe thousands - remains perfectly quiet - an hush as - here is what I called it. Not considered cricket to cheer or yell. After a good play there is restrained applause. Game is fairly interesting but not nearly so fast or exciting as baseball. I think Americans would regard it as deadly dull. Back home to meet the folks - daughter - Margaret - unknown - "Y" - so named as unknown quantity before arrival; her schoolmate who lives with the D's - Pauline Metzger - and her D, in uniform - some hospital and or other. They are all very friendly and pleasant. The girls rather pretty. Mrs. D with gray hair & very nice face - Dr. Fred Grad - A couple of gin & bitters & then dinner at about 8. Listened to 90'clock news, chat with D re official matters - he gave me paper of proposed basis of talk

with Taylor, W.C. & self on future relations in neutral & allied fields. To bed at 11:15 & a nice bed in the D boys room - he being a scholarship student at Westminster & apparently a very unusual and good student, good athlete, good at music. Sunday, May 23d - up at 8:30, breakfast of a very fine soft-boiled egg, cereal, tea, b & b. Then in taxi to D's golf club - Tunnel Road Hill & County Club. A couple of friends of D's - nurse partners & D & G the other. A lovely 16-hole course in which D & I won by 1 point on the 16th hole. She was really very picturesque & quite difficult. Considering my lack of practice it was off with embarrassment but got over that quickly when I found I could still hit the ball fairly well. Played in my ordinary clothes & old pair of shoes. He slipped just a bit on 1st drive (remember that George B fell flat on his back his 1st drive here.)



My driving as usual pretty good but about shots and putting poor, as usual Anyhow I wasn't a duff & felt pretty good about it - A mug of beer & taxi to home. I paying 9 shillings - only 3 miles ride but taxi out in the country - well I guess it is cheaper at that than it would have been at home = Dinner, good food & I was pretty hungry Read paper a bit & had or tried to have nap from 3 to 4 then to go with D & the girls to the tennis courts where am now sitting this & watching them play They pretty good - all of them The 2<sup>nd</sup> is a young woman named Cunliffe who is grad of London School of Economics We had some talk re Barbara's coming over to take post grad course there & Y coming over to Washington to study - exchanged of girls, which wouldn't be bad idea for both - forgot to say we had tea & be

fore going out to tennis (Dinner at 1 & tea at 4 They eat often - not too much at a time - & a good idea) D is a lively man for his age & is apparently good at all games He could easily train me at tennis if they had good tennis balls (which are now unobtainable) the game would be very fast It is quite fast as it is the young D girl is an excellent player, left-handed She & Pauline are pursuing secretarial course in Edin & will soon be finished Probably get secretarial work in Foreign O If not for war would have gone to university - learned later from Ted that I had been on <sup>British</sup> international hockey team in his younger days -- After tennis, back home after a mild beer at the tennis club where I wanted to buy the, need for ed. I was but was against the, also had lunch for a few minutes, chatted with the folks, helped work on a cross-word

(perhaps ~~to content~~ ~~to know~~) famous women  
 of 19<sup>th</sup> & 20<sup>th</sup> Centuries), then dinner or  
 rather supper: ~~much~~ like at home, the  
 cold cuts & pick-up things but good D  
 and I did the dishes - there is no such  
 animal as a maid any longer except  
 among the very wealthy I suppose. Even  
 Gen Davidson told us when we made our  
 official call that he helped out in the  
 housework at his home. Davidson does  
 as a rule, too. The D house is arranged  
 for easy housekeeping, it having been designed  
 by Mrs. D with that in view when it was  
 built in 1927. After that (I was then about  
 8.45) listened to radio for a bit, the pro-  
 gram being much like one of our Sunday  
 evening gag & pun varieties, with a short  
 playlet thrown in, a bit of music, etc.  
 D mowed the lawn - after the golf &  
 tennis - and he over 60. Much joking  
 about his having to be careful not to get

laid out or pass out before reaching pen-  
 sion age as according to their Civil Serv.  
 rules you must begin to draw pension  
 in order to get any & if you die before  
 that the family gets nothing at all!  
 I guess the C.S. personnel do not contribute  
 toward retirement fund as well, but this is a  
 point to look up for myself - what would  
 happen if I passed out before reaching  
 retirement age? Does family get only  
 what I put in or more? - To bed at  
 about 11, having agreed to stay overnight  
 & go in with D in the morning - contrary  
 to previous plan that I return Sunday  
 evening to B/P. - Didn't sleep well, I  
 guess too much ultra-violet in sunshine  
 all day. Began to rain in the night.  
 Monday, May 24<sup>th</sup> - up at 7.15, Shower  
 & dress. Forget to indicate had a bath  
 before going to bed night before. When I  
 asked if shower possible was promptly

had yes - attached to nozzle of bath  
 tub. The water had no pressure though  
 & it was a very very poor excuse for a  
 shower as we know it at home. Clean  
 however & felt better after haircut of day  
 before, which (as usual) reduced my  
 "itchy" feeling when needing haircut -  
 Breakfast of bacon + dry cereal, tea was  
 still raining so took umbrellas to station  
 Got into town still pouring - but gently -  
 somehow the rain doesn't fall hard  
 here as it does home (Right now it's  
 raining but you can only tell by looking  
 out the windows - no sound of it) [Am  
 writing all this on Tuesday P.M.] Got to  
 D's office, left my bag there, walked to  
 Embassy, saw T + A + Eric there, had  
 few minutes. Had much catching up on  
 what all A had telegraphed home since  
 last time I saw him. A short one from  
 from Corderman giving barest outlines of

results of discussions on E there (later found  
 to be very sketchy + omitted altogether  
 fact we were to do research + ops on memo  
 to be sent over - this being - my opinion very  
 important) - no mail Paid Eric 1 £  
 some for extra cost of cable for flowers  
 Rushed to get 10 40 train to V3/P, paid my  
 own way for 1st class round trip 24/10, which  
 is about £3.00 for 50 mile journey. Consider-  
 ering this determined to get seat in 1st  
 compartment, which I did. Unavoidable  
 & was met by car at Bitchley, taken to  
 Park & began work at once. No telegrams  
 from Wash. I can't understand why so  
 slow in answering the several have post  
 from there - Today finished up study of  
 (except 1 + 3)  
 E ops, & a whole of a business. If I can only  
 digest all my notes! Also spent a short  
 time with Prof Vincent who was set up about  
 a month ago as Coordinator of research  
 etc. Will learn more about his job later, but

he seems very capable man was prof of  
 languages (Italian esp) at Cambridge &  
 has been here about 2 years — Also talk  
 with Feltman & DeGey, making up sched-  
 ule for rest of my time here. Brief talk  
 with Leon Johnson who's back from Italy &  
 other parts. He will probably return to India  
 via US & I've invited him to stop off & see  
 us — Chilly & wet all day, so kept my  
 sweaters on. Back to hotel at 6:30, met  
 Col. Syrett again up for his Tuesday visit  
 to B/P. Invited him have drinks with me —  
 set & talked till dinner time (7:30). Told  
 me of his crypt work in near East last war  
 & for some years thereafter. Nice dinner  
 after which I immediately went up to  
 my room to write b + b letter to the Den-  
 notions & one to Prof. Adcock for loan of  
 his clubs plus gift of the 2 golf balls  
 I brought with me from Washington.  
 Hope he will be pleased. Everybody says they

are worth their weight in gold about same  
 as regards tennis balls. Into bed at 9:30  
 as I was tired & (hoping) sleepy. But soon  
 as got into bed got to thinking about how  
 our Navy been acting re our seeing N things  
 here & got pretty well riled. The more I thought  
 about matter it had been agreed I was  
 to see B/P Nav F books & Haq. DeGey told  
 me former was off as Trans had sent work  
 from Wash. Sorry etc, not anything B/P had  
 wanted, dictated by our Nav Wash. I  
 can't understand — unless old Redman put  
 in his own after hearing how our Gov had  
 messed things up & did not propose get  
 involved. I shall have it out with  
 Wenger when I get back, as consider-  
 able reflection my own status & trustworthi-  
 ness. Had fitful sleep & dreamed a dream  
 involving this subject apparently as substance  
 was being double-crossed by chap who  
 symbolized Navy. Got up at about 1 a.m.

+ took 2 small pills from Washington cache but didn't do much good. Awoke early & not at all refreshed. Guess this work is very exhausting mentally & I hope to get through with it soon. All quiet every night so far as alarms are concerned. - Another thing, not enough relaxation & change from daily grind has me keyed up, I guess. Am not worried about a thing in the world so it can't be that which is making poor sleep. [Another funny thing is that I've noticed that on days when I am "tense" & have "hives" or "goosebumps" I sleep well in night but when don't have them, sleep not so good. Haven't had hives for many days now wish I could solve this mystery of myself. I - Well, so much for that.]  
Tuesday, May 25th - Up at 7:30 to have early breakfast & go to B/P in car sent for. Col Sycett got to B/P at 9:15 and started in to arrange the many notes I've collected.

thus far. Tiltman not there yet. Sycett & I in talk re my future activities & when Col Sycett was going to Beau Manor. He has read syllabus & wanted to know how come he had it been asked about it - as that comes in his province. I was quick to explain schedule only made up last evening & intention to consult him not yet able to be carried out. Tiltman & Maj O'Connor (Edith Hastings relief) came in & I had brief talk with O'Connor. Seems to be nice chap. Explained situation re Sycett & Beau Manor to Tiltman & DeGhey & Walter Burdick up with Sycett. Plan is for Taylor, M.C., & I & two myself to make visit with Sycett next Monday. Went then further talk with Prof Vincent who explained IT Hog. Sent silly, practical as these people engage in - to run a good system. Then to Wing Luke Jones for preliminary outline that I could help re. Then to lunch where met Admiral Sycett,

me chief of Admiralty Staff + Admiral. Services, also on same staff. De Grey put Syfret on left side + Services on his right. Wrong because Syfret has 2 bars plus the rods, whereas Services has only 1. Anyhow De Grey put me next to Syfret + we had very interesting chat. Syfret on my left. Birch (looking terribly seedy) at other end of table opposite De Grey (the clothes the civilians wear around here are awful - frayed, dirty, unpressed. But I guess it can't well be helped). Wonder what they'd be like in normal times, though I suspect Birch would look seedy at all times.) After lunch had session with Dudley-Smith until 4.15, then resumed with W. Cuth Jones, until 5.30. Can't have a whole day tomorrow for that 3 alone. Good stuff there. Jones seems exceptionally able. From textile business home at

6.30 and quick to the bath to get in ahead of rush. Had good bath + washed my hair. How much more gray it has become of recent weeks! Mostly silver now at temples, I note. W. Cuth had more on top - rather becoming I should think. Had pint of half + half, took it up to room + have been writing on this diary since then except for 1 hour out for dinner. Nice soup, good fish + french fried potatoes, apple tart. Yesterday we had a very nice piece of, steaked french fried! It was 9.15 + soon time for bed.

Wednesday, May 26th - Just a few night. Got up with crick in my lower back - likely some slight kidney business or maybe the very hard bed. Nice breakfast of a fine tasting omelette, with bits of ham and onion. My brown suit came back from tailor yesterday.

supposedly pressed - but not as we do it. Had it look over a week. However, 'tis very much better than it was. Now wanting for bread & I note the cross-roads signs here are some of the names. Fenny Stratford, Stony Stratford, Gopley Chase, Newport Pagnell, Woburn Sands, Woburn, London, Bletchley - funny names, all except London & Stratford. After yesterday's rain today it is very bright sunshine and warm. Think the sunshine is too bright to last. I had on my longies yesterday & felt pretty comfortable so put them on again today 'maybe too warm' - Have a heavy schedule today though. But 3 tomorrow night am invited to dinner at Tiltmans. Here comes the bus - 7:15p. Waiting for dinner. Had a very full day & am behind schedule again as I did not finish but 3 at all & the schedule is all away again. But most interesting stuff

met some very interesting chaps today, winding up with a Prof Norman on radar. Lunch today was rather formal affair as "the Chief" appeared rather suddenly on the premises - something special brewing I guess. De Grey put him at head of table & I on the C's right as guest of honor. I was particularly nice to us & we had pretty good talk re educating some of our lesser allies & dangers thereof, security measures, possibility of his coming to US, poss of Corderman's coming over here. Word about purple wage giving signs of suspicion of seceding (Sp and + parts situation - I must look into, he said). Had V mail letter from John - dated May 10 - and also one from F - dated May 12. F has had but one letter from me - a V mail. Apparently my 1st letter posted in British PD never arrived yet & doubt if it will. But his written very few letters & hope she understands

I've not been able to write much. This pace is  
 terrific for me, especially so because of this -  
 rather poor sleeping. Feel fine otherwise, though  
 tired most of time - Dinner now - ~~to read~~  
 a good soup, lamb chop (or veal), mashed  
 potatoes, many beans, & a "sweet" - plum &  
 custard. - Took short walk with me last  
 listened to radio 9.00 o'clock news. Must  
 go over my notes for today, see to tomorrow's  
 schedule & possibly catch up on it - but  
 I begin to doubt it. Must also go to bed  
 fairly early - have had slight humming-  
 ache all day. The bright sunshine of this  
 morning disappeared about 4 pm & it is  
 dark with overhanging heavy clouds. I  
 was to phone Taylor tonight but will pass  
 that up till tomorrow - some sort of mes-  
 sage for me from Wash which he doesn't  
 know whether to send up here or not. And  
 a message from Elizabeth, I believe, which  
 is being forwarded looking eagerly to be re-  
 cept here. Got my cig & candy ration today

Thursday, May 27 - (Written 25<sup>th</sup>) Not  
 much to report of unusual nature. Good  
 night's sleep but not enough - catching up, I  
 guess. Worked hard all day until 4:00 &  
 then decided to knock off for couple hours  
 in sunshine as it was lovely out & I had  
 finished up. But study was to be guest for  
 dinner at Tiltman's, so rested in T's office  
 in wicker chair & almost fell asleep. To  
 T's house where had nice dinner and  
 pleasant chat, some history on E, until  
 10:30 when bus was to call for me. When  
 didn't show up at 10:35, walked to  
 BP & boarded it but it never left till  
 11 - not yet dark. Arrived hotel at  
 11:30 in deep dark but not dark yet.  
 Turned in soon. For an hour or more  
 could hear planes passing by - must  
 have been big raid on Germany some-  
 where. Will be interesting to hear news  
 soon of what part.



Friday, May 28. = up at 7:30 after very good sleep (with aid of pink pills - T's medico provided) Breakfast + packed bag as was going to Lulu today after trip to Oxford. Prepared to stay 2-3 days then return BPP for 2-3 more days. In office where prepared telegram Corderman re failure to answer one from here at least 10 days old. They seem to be very very slow in getting answers across + quite embarrassing to me. Just after preparing draft was notified one was coming in from there so decided hold up mine. But since Mr De Grey + I had undertaken to make trip to Oxford + car was waiting decided to go on + not wait. I had decided previously to go direct from Oxford to Lulu but this changed plans + decided to return to BPP to see what action

might be necessary on Wash telegram. We left BPP at 11:30 and had a very nice motor trip to Oxford, about 50 miles Southwest of BPP. The weather excellent and the countryside very lovely. Saw many very old houses on way. Arrived Oxford where drove up to Mansfield College, hq of Quaker HOK's show on compilation. Hok met us at door + took us up. Had a brief preliminary chat then to lunch. Walk of about 10 minutes to main hotel, through most interesting part of Oxford, Hok pointing out places. A lovely city + I'd like nothing better than to stay there a month. But because so much govt work being done there now in practically all the colleges, no visitors are permitted. Had nice lunch + walk back to Mansfield by different route Oxford

comprises 23 colleges plus several  
denominational. Mansfield is Con-  
gregational, built about 1870, Man-  
chester is Unitarian, built later than  
that. Had an excellent tour through this  
place - very well organized, quiet, effie-  
cient, with large output & no fuss &  
feathers. Staff practically all women.  
Tea, of course, at 4.30 & we left soon  
after to visit Ox University Press where  
De Grey knows the head - Dr Johnson  
who took us into his office & chatted  
with us for 30 minutes. What an office!  
Johnson lives in it, for his  
cot there & says he hasn't left the  
place since war began. Shelves  
from floor to ceiling lined with old  
books all printed Oxford. One  
very large section nothing but  
bibles. I had been building  
up the collection for the Press.

(Am sending this on train enroute to  
Leam.) The whole office reeks of the  
dust & dusty past - its most inter-  
esting. De Grey says I'm quite a  
collector of old items - anything con-  
nected with books or printing. The 1st  
Oxford printer began in 1487! There was  
a tablet listing all the heads of the Press  
since that date, down to last incumbent,  
1919, about 25 names in all. Also a  
list of the typefounders & another of the  
engravers. Oxford Press is now the  
largest printery in the Empire. The  
outer office looks like nothing on  
earth or anything like an office in  
the GPO. I marvel at the contrast.  
But the Press need not hide its head!  
For quality & quantity either. Johnson  
told me normal capacity is 70,000  
books a week! I would have liked  
to see the works but no time asked.

to go back. Left at 5.30 and took a different route back. The lady driver was not familiar with this route & we got 'lost' several times, no highway markers! All have been taken down & not yet replaced. Saw some more even lovelier country & old houses, some going back the 15<sup>th</sup> Cent. Arrived BPP at 6.45 & took look at tel from Wash. Nothing to get excited about but was amused at tone of superiority at one spot. If Cordorman comes over here bill learn better. Letter from F here, via Maidment & another enclosed which had been originally sent V-mail correctly addressed but returned as "unknown"!! F complaining of lack of mail - but I've not written much. I'm now enroute on what is called a "Parliamentary Train" - it stops at every station, a hangover from a

law passed long ago requiring passage of all trains. I understand. Left BPP at 7.20 and due at Euston Stn at 9.00. Will be too late to meet Al & Del at officer's mess, as agreed, so will probably get dinner at Park Lane if feel hungry. But I still have bit of a funny ache despite good physio last night. Think will be over tomorrow though. This train has its advantages though. For one thing it goes slowly enough so can write fairly legibly. Secondly, thus far though we have paid for 1<sup>st</sup> class seats we having never had them - the trains are so crowded. But apparently people avoid the Parliamentary or else it is at a time when few are going into Eden. I had good chat with De Grey today. According to his version of Rowena we can't claim most of credit & I shall want to talk to Field back re

this Dr. G says it tip came from French who punched 1st page of us book & also by looking over shoulders learned how system worked. He also claims credit for discovery (accidental by Pat Bartley & deduction by him) of recip nature of book. Says we made a punch of something & when I mentioned work sheet in paper basket he said no. Also talked about our respective org & I admitted seemed to me we were greatly overstaffed for what we do. I am impressed with volume work done by these people per capita, under heavy physical handicaps & I wonder if they aren't really much better writers than we are despite our machines, mechanization, fine offices, etc. In a technical sense I think we are way ahead of them but in a practical sense, judged by accomplishments,

these amateurs (most of them really are that in my opinion) have very largely surpassed us in detail, attention to minutia, digging out every bit of intell possible & applying high class thinking & originality & brains to the task. Their key personnel are of much greater capabilities than ours, I think, & the place abounds with dons, professors, & highest type businessmen who are used to getting much done in a quiet way, without fuss & feathers. A very great deal of handwork & the volume is done even at the top. Their papers look dirty & messy, their card indices are terrible to look at - but they have the data on them & they know how to use them. For as we would not put up with the printed slip produced by Typex - so ragged printing, it looks primitive. But they manage

with it OK. They paste slips on back of a version + save paper. They pass important info on dirty little slips of paper archits + they don't seem to get lost somehow. The rooms they work in are dirty + messy + cluttered up. Their toilets are few + terrible! But they get things done. And one should see the cups they drink tea from - well dishwashing facilities are nil + it's a wonder to me these sub-rampant trash-worth-around they must have their tea of course - at 10.30 + 4.30 - + it's better than the coca cola habit.]

We are wearing Pdu now + will cease Saturday May 29th. - up at 7.45 + am now waiting for breakfast. I am last night a bit late. Tax to Park Lane where room had been reserved for me - a lovely double.

one at 25 shillings but worth it. My change in plans got me in to Pdu too late to get dinner at the Off mess + I did not think it worth the 8 shillings to get dinner at the Park Lane mess + I was not hungry + still had bit of a tummy ache. Decided to do without eating as there is no place I know of where could get just a bite, and have walk instead as it was lovely evening. Tried to reach Del + Al but neither one around. Was accosted by two or three street-walkers in the dusk in Piccadilly, which I walked from Park Lane to Circus and back. Tried get Del + Al at 11.30 but neither in yet. [By the way one of the hazards of walking down streets in blackout is that one will surely step on dog dung as the local dogs are very poorly brought up + Londoners don't seem to try to control them. Del Lyckett, to whom I have just read this + of whom I asked

if it was a fair criticism said he had not noticed this. Al said neither had he but Del agreed vehemently with me. [I am writing this enroute to Beauvoir, about which later] [By the way the two street ladies were - in the dusk - fairly good looking but I did not get close enough to verify.] Back to hotel where took nice bath & went to bed about 12. [Funny thing I learned later that Tel & Al were both working at the Embassy until 11 but it never occurred to me to phone them or walk over - even to see if any messages or mail. A curious psychological blind spot & wonder what its significance is.] Had very good sleep.

Saturday, May 29th -- up at 7:45 to get an early start as had to be at Selfridges Annex at 9. [Train is going to now.] A Sig C

affairs to which I'd been invited by Gen R. all day tour of Sig C local installations for information Sig C officers in posts near Gen. Had interesting tour through Signal Center & Photo establishment, etc but not through any sig intell or crypt. Lunch as guest of Gen Rumbough, with about 30 others, at Mansfield Hotel where Gen Lee (C to SOS-ETO) has his private mess. We had a very lovely luncheon, as good as any could get in peace time in Wash at Mayflower Spicers luncheon including napkins (have I mentioned these are rare now & are called sermettes, & if you ask for napkins the gal's blush is that is word they use here for menstrual cloth), nice silver & sparkling goblets. We had cocktails first. Then grape juice (not grapefruit juice), good soup, survey of beef & rice (excellent) & potatoes, peas, real white or almost

white flour rolls, radishes & delicious sweet pickles, & a very fine open-face pie consisting of pumpkin base with cherries topped by layer of strawberry jam. After short interval during which I pushed by cab to Embassy to see what doing & see Ted & Al for few minutes, took cab to next place on tour & continued with party until 5:15, then back to Embassy to read messages that had come in & been sent. Filed per diem voucher. Time passed very fast & it was 6:30 before I knew it - & had no time to go to hotel to wash up before going to Am Sig C Cosm dinner, to which I'd also been invited. My tummy was all better this morning so felt I could enjoy food. There were over 200 Sig C Officers & Kinew Devers. CA-ETO came, together with Dir

of Signals, British Army (Major Gen Fladgate), C Sig O of Home Forces (Gen Phillips), C Sig O of ETO (Gen Rumbough) and all heads of ETO Sigs Branches. Symon, Fitzgerald, Stice, Shearer (who didn't recognize me until told him who I was, he said I'd put on so much weight), Jersey, Dixon (Master of ceremonies), Coulisk, Mickelson, Garland - all old friends or acquaintances. There were only two guests not in uniform - a Mr Blackstaff of British PD & myself. Felt a bit embarrassed but have become philosophical about it all. We had another excellent dinner (at 1/2 it was expensive of course but well worth cost) Scotch & potato, soup, real sirloin steak - & a large slice!! - etc. I have the menu as memory. Then some entertain-

went after very brief speeches. Dixon made curious slip when he introduced Lieut Gen Devers as Lieut Colonel Devers. Of the entertainment the best by far was a Sgt Travers who was on singing staff NBC or CBS & who has a marvelous baritone-bass of much power & appeal. Affair was over by 10:15 & I walked back to hotel to see if Tel or Al in his absence so went out for short walk, back at 11:00 found Tel in his room, went up & talked with him until 12:15. He & Al very much disgusted with wage from AH to me which makes it seem that all the wages we had been pending back made no impression & were so much waste so far as concerns an understanding of what is going on here. After that went out for few minutes short walk in the blackout, walking up & down in front of hotel on Piccadilly. In the deep

Bull's Head Quorum (Chorm)  
Sutherland slate 97

shadows of entrances to shops were dark figures of (occasionally) prostitutes on the pavement. Would speak softly to me as I pass by - In bed by 12:30 and good sleep.

Sunday, May 30th - Up at 8:30, breakfast after bath - kipper! by good & it was good. Packed up my belongings as decided no use keeping expensive room I'd not occupy rest of day at next & then fit I'd prepare to go back to B/P direct from Beaumont which we were to visit this day. Taylor & I walked to Embassy where found several more messages, one giving me slight bawling out in polite fashion - & really laughable. Can't understand why should ask for such detailed info re intercept set up - they had leadership in I field by agreement & intended to exercise it! Well, if they are qualified to exercise it why don't they ask the questions?? Spent practice



collected 2 weeks  
per diem

99

ally all day at Embassy up to 5 p.m. going over messages, preparing replies to ones that had come in. Lunch at Office Miss at 1.30 with Ted + Al who had just returned from overnight stay with the Democrats. At 5 went to St Pancras Station to get train for Beaumaris, large wt. str. of War Dept - called W O Y G - pronounced "Woigh" - War Office Y Group. Col Lyett, whom I've mentioned before is head of that activity (among others) and it was at my request that he arranged for visit, coming along with us. Compartment arranged + reserved for us in first class, with snappy Captain of ATS there as RTO representative. A 3 hour journey which passed quickly. I began immediately plying Lyett with questions + writing notes in my book. He smilingly said had heard all about my great ability at that

sort of thing + thought I should have been a barrister. Got lot of good info though on his org, where it fits in general scheme, his official relations with B/P + other groups, etc. After I had exhausted him I started in on this diary, catching up to point about middle of p. 96 when we reached Loughborough, where Mr (Capt) Cude) Ellingworth met us with big official car + good looking driver to take us to our hotel - The Kings Head, where we had rooms reserved. When I got to mine found signs of occupancy + wondered a bit but merely assumed things inadvertently left behind - such as for houseleppers under bed, tooth brush I could see 'twas much occupied but on regarding the group below I thanked Ellingworth for courtesy in providing me with a sleeping com-

-pamon who, I hope, was good looking  
 much laughter etc but I failed to  
 report findings to management & forgot  
 about the matter until return after  
 midnight, when doorman advised that  
 I'd been given wrong key & that my  
 belongings had been moved much  
 laughter again. After quick drink  
 we journeyed to an ancient inn in  
 Beaumont (about 2 1/2 miles from South  
 borough) called the Bull's Head.  
 Quorn Very interesting place, full of  
 people in the pub - nice crowd. We  
 had good dinner - nice table, white  
 linen etc. Place to die: Sit & a  
 lasty tour around - from 9 to 12.  
 A fascinating part up & too long to  
 explain here. Must say a few words  
 about the central house - was formerly  
 ancestral home of William P. Herriek  
 father of the poet Robert Herrick & it

is a relic of glorious days never to  
 return. Immense central hall with  
 grand staircase, elaborately carved  
 wood banisters, doors, door frames,  
 sideboards, chests, etc. Beautiful  
 silk papered walls, high ceilings,  
 massive fireplaces. Date of 1st  
 castle way back but modern recon-  
 struction (1870. about) though I saw  
 things which went back to 1690. In  
 the courtyard the restored figurehead  
 of the warship commanded by Admiral  
 Cornwallis (relative of the Jan) which  
 Ellingworth had found in one of the sheds.  
 Beautiful grounds & trees & shrubs.  
 Original estate about 2500 acres but  
 W.O. rents, only small part. After the  
 tour sat down for chat in E's quarters  
 & had coffee, talking till 1:00 a.m.  
 Then returned in black to our  
 hotel where went to bed at once.

Monday, May 31st. — Had good sleep till about 7 when trucks going by (we were on main street) woke us + I dozed until 8. Breakfast after bath Had again a nice kupper! We then journeyed to station again + went into some things more thoroughly. Al had undertaken to give cocktail party on his wedding anniversary + on account special circumstances he left ahead of us, at 12.30 I had promised him to come in to help to attend but finding train connections difficult decided to go direct to B/P in car with Syrett. I hope Al will forgive me but I am so pressed for time I felt I just had to get back to B/P today. We had lunch (Taylor, I, Syrett, Ellingworth + Wirt (his deputy) again at Bulls Head Quon. Then we turned to station to pick up things

then a very nice motor trip of 1 1/2 hours to B/P, arriving at 4.30. (Taylor went back to Eden by train from Loughborough) On arrival B/P found plenty to do, calls to make, talks with Daltry, Hank, Kay, Jerry, message to answer, etc. Glad I came back. Worked fast till 6, then with Syrett in car to Woburn Sands. Had my room shuffled + hope the large double bed is a bit more comfortable than small one Kart had. Larger room, too I bought double scotch for Syrett + self, + we talked till dinner time. Left, played a bit of "bowls" with him until 9 pm. News. Have been writing this since 9.15 + it is now 10.05. So many things to do + I've not yet written the letters I should + I know F + mother will be frantic but what alternatives can I do? Shall have to wait.

REF ID: A60517  
 'till 11 ~~thought as it is~~, looking  
 over papers & preparing draft of  
 important message to Wash  
 Tuesday, June 1. - Worked until  
 10:30 and then went below to have  
 drink with Col Lyett. We talked  
 till 11:15. Then to bed and had  
 an excellent sleep in the big bed.  
 Up at 7:45, breakfast 8:45,  
 then with Lyett in special car  
 to B/P, arriving 9:15. Started in  
 work immediately, on message to  
 Wash. Juring came in & had  
 discussion with him. Got him  
 to agree to give OIC on X61753,  
 which shall wire Wash on tomorrow.  
 Mr Vitter phoned & I made  
 date for 10 - but didn't get to  
 him till 11 a.m. Filtman & I  
 discussed message to Wash & he  
 approved my draft DeLhey, Merr.

Johnson, Thompson all approved.  
 As directed its encoding & trans-  
 mission. Now comes the danger  
 I hope not. Shall await reaction  
 with considerable trepidity then  
 to Mr Vitter 'till 1:15, lunch,  
 returned M-V & worked in Block  
 A 'till 6. Rained hard good  
 deal today. Prof Boase lent  
 me raincoat. Home at 6:30,  
 rushed to take bath. Have  
 been working ever since except  
 for time out for dinner, 7:30 to  
 8 p.m.

Wednesday, June 2 - up until 10:30  
 getting my papers in shape, wrote a  
 letter to Elizabeth and one to mother  
 which I posted this morning through  
 bag to maidman. The young lady sec-  
 retary to Filtman had to talk to the  
 mail people to get them to take them

Had good sleep and was up by 8 a.m.:  
 nice kupper for breakfast. To B/P by  
 bus and worked steadily all day. A  
 message from Corderman, much garbled  
 and had to ask for repeat. Sent one re  
 Furnig's acceptance of X 61753 mod-  
 fications. Josh Cooper, head of Air  
 Section has awarded high honor on  
 King's Birthday - Commander of St. Michael  
 and St. George, next to Order of the Bath  
 Had good sessions with some of his people  
 today & finished up with Capt Jester in  
 John Alfred phoned to ask whether  
 I'd be ready to depart on coming Monday  
 and I protested to make it Wednesday a  
 week from today. Said he was trying to  
 get passage via Lisbon - and in tonight's  
 news see where British Civil plane from  
 there to London was shot down - Leslie  
 Howard among 13 passengers. I wonder  
 what Alfred will do now. It's just one

of the hazards, I guess, and am prepared  
 to take them, too. Al & Iel to come out  
 to B/P on Friday for last look. I must  
 try finish good deal tomorrow & Sat-  
 urday. Doubt if I can though must  
 see some people in Edw. before departure  
 such as Williams at W.O. & Johnson  
 of R.F. Besides promised conference  
 with Ryan & Shearer may be news of  
 George's return will change depart-  
 ure date as all here are of opinion  
 we should wait until he returns. =  
 Fish dinner tonight & good. Have had  
 two Britishers as table companions  
 past two days, they from Northampton  
 & taking a week's holiday. One is  
 adm. supt. of hospital, other a  
 druggist. Both rather nice and  
 intelligent men. Interesting discus-  
 sions with them. Short walk after  
 dinner & a retired business man I'd

nodded to in fact <sup>here</sup> waited me in  
to see his garden. Lovely flowers -  
phlox, delphinium, roses, Mrs. Lumsden  
snapdragons, periwinkles etc And a  
fine view of surrounding country, side  
from one corner of the garden. - Back  
to hotel, listened to 9 o'clock news  
- forgot to mention that one of nice  
things at the Swan is that the food  
that is meant to be hot is invariably  
hot & the plates are always  
heated, too. Good food all round &  
must reverse estimate or preconceptions  
of British cooking. - Filtman  
away today, also Dunder - Smith whom  
I must see without delay re a  
disturbing answer received from  
Arlington to query I made re sec-  
urity of strip. Looks like more id  
story work has been going on some-  
where. - Rained pretty nearly all

day yesterday and today Quite  
chilly & was glad to have my  
sweater on Had to borrow raincoat  
yesterday from Prof. Boase but to-  
day got out my own. - Now 10:30  
and must go to bed. Will try to make  
early bus tomorrow so as to get  
very good start. Much to do - All  
out of my PK cigarettes this evening  
& had to buy British - quite ex-  
pensive. 2/4 for pack of 20, which  
is about 45¢! And punk cigs at  
that, compared to ours

Thursday, June 3. - Set my clock for  
7:30 but was sleepy and didn't get up  
until 8:15, after my shaving water was  
brought. A good sleep from 10:45 to  
5 and then dozing until 8:15. It is  
still rainy, cold, and overcast. - No  
special news in paper this morning  
but all papers giving headlines to

I believe missed being on  
 story about passenger plane shot down  
 yesterday. Long notices re Leslie Howard  
 and 20 B/P on an earlier bus. Teltman  
 there. no messages. Phoned Embassy &  
 got Taylor on phone to call Col. Symon  
 to tell him would not be able to see him  
 until next Monday or Tuesday. Teltman's  
 secretary brought back letters I'd  
 posted yesterday to go in B/P pouch  
 to Maidment, she telling me that people  
 here said couldn't take those letters as  
 they'd not been censored. Received one  
 from Elizabeth written May 1st, via that  
 same pouch. She ecstatic about the  
 roses which came on 21st but saying  
 nothing re the number, which I suspect  
 was 2 dozen, not exactly 26. Spent a m  
 session with May Thompson's show on  
 Dig. ml + JMA. Afternoon with Free-  
 born on IBM, then Int'l Exchange.  
 Miss Rodgeron phoned to ask when I

would be coming to see her. Others have  
 told me how anxious she was to see me  
 Home at 6.30 and brought couple round  
 search for Mr. Clark & self, he the  
 oldest living C.L.S. member, going back  
 to 1916. He is quite a talker. Got him  
 going on old history. Says Falkland  
 story a myth also story re Callaghan  
 preceding Jutland, also Hobbs & Bredan  
 story - Fish for dinner again but very  
 good. Felt very sleepy after it & came  
 up, lay down, fell asleep for almost  
 2 hours. Now 10.30 pm - Came all  
 out of matches, lighter fluid, & have  
 but 2-3 Binks' cigars, no pipe tobac-  
 co. - Asked Taylor to bring me my cig-  
 ration tomorrow & hope he does. -  
 Williams of W.O. in Ldn phoned  
 me today, to want to make date to  
 see me. Set next Tuesday -

Friday, June 4 - Up at 8 after good sleep. Poached egg on toast for breakfast, in addition to the usual porridge, i.e., oatmeal. This is day that Al & Jil are to come up for final conference. The rain is gone, I think, but it is rather cool. The sunshine will warm it up today. I hope. I'm putting on a small filler at the village center memorial, waiting for the bus. At one corner is a men's comfort station. In the large towns these are very well kept places, with an attendant - far different from the usual European type of thing, and these places are free and well patronized by the populace, high and low. - Bus coming = 7 pm. Had a very interesting day. Expected to find Al & Jil there when I arrived at 9:45 but they nowhere around. Word came later that they'd be unable to make 8:15 train and would be on 10:42, which gets

in at 11:50. Hence went into Research section under way Morgan. Interesting to see on Sturgeon with him and young Tuttle, nice looking youngster from Cambridge - math every bright. Iunched with them at 12 & learned Al & Jil had arrived so joined them in Dr. Grey's office, with Tiltman. Decided to answer Al with the four letters for him - one at a time, after 1st one sort of afterthought - "Oh! yes, another one for you." It went off very nicely & Al was tickled. They brought two bottles of port, one for me as present to Tiltman, which was nice. Either present to me. Dr. Grey had some <sup>school</sup> alumni from Eton in for drink. June 4 being Eton observance day over the world, I guess. Stachey there, too, as Etonian. Then nice lunch Harry Johnson here a final day & farewells as he is off to U.S. on fast ship - After lunch, which was



rather than consuming "had conference on recent agreement," discussing details. Al, Tel, De Gray, Tiltman, & self finished at 4 and then to Page's show on ISOS, which I found most interesting. Return here to -  
 -morning - See Miss Radgerson & had a reunion. Prof. Vincent phoned to ask if I'd like to go to Cambridge with him on Sunday, have dinner at one of colleges, stay overnight. Slightly invitation & told him would let him know definitely in the morning. Had tentative plan to return to Eden with Al + Tel tomorrow but think I won't now. Maybe return there from Cambridge but more likely return here Sunday night & wind up affairs here - Al brought me cigaret & candy ration, by gum & I needed the former as I was all out of everything. - Al spending night at Bedford Arms Hotel in Woburn, Tel at some place in Brighton Buzzard &

no chance for us to get together this evening. Hear that Eric is coming for US and if coming week, maybe we'll be along too. - Not a word, a Georgistum, or Tavis. - no word about anything from A.H. - no answer to my long telegram. Think they are acting pretty badly all round on Sig matters - Al + Tel went from 4-6 to take another look in from room that I must go again, too. - Had hot bath as soon as got to hotel this evening & now in my room with part of half'n half, waiting for dinner & writing this - no chance today to get those two letters to Eden to mail. E + mother will be upset. I know, especially mother. Probably will get back home before letters anyhow. - Still cold and rainy all day and it seems never will clear up. - [Following written Sunday a.m.] - After dinner this evening read papers a while, then

listened to 9.00 news, after which  
 my two British table companions  
 + I went to visit a tiny pub  
 about 1/8 mi away, I having been  
 told it was a bit unusual + that  
 the beer was unusually good there.  
 We walked up in the rain and  
 went in. It certainly is a tiny  
 place: "Royal Oak" by name - but  
 spotlessly clean and well-filled.  
 The whole pub room not much  
 bigger than our sewing room at  
 home. Watched 4 people play the  
 inevitable dart game which was  
 explained to me in some detail +  
 which is quite different from the  
 sort of game played in U.S. with  
 darts. - Bought two rounds  
 of beer, which was good, +  
 then back to hotel and soon to  
 bed. - Had an alert during the

night, which woke me but I was  
 asleep again before the all clear  
 sounded as I didn't hear latter  
Saturday, June 5th Up early +  
 had very nice kippers for breakfast.  
 To Bp on 8.30 bus to get an early  
 start again. Saw Vincent and  
 accepted invitation to go to Cambridge  
 with him (I heard it was that place  
 which was visited by Bombers last  
 night). We are to leave Sunday  
 afternoon by Vincent's car, spend  
 night in college, returning Monday  
 morning. All not feeling too well +  
 decided to go back to Ldn on  
 noon train. Miss Bartley had  
 phoned night before to invite all  
 three of us to luncheon today -  
 her home not very far from here.  
 But we felt pressed for time +  
 transportation difficulties made it

118  
 admissible to beg off, which duty  
 was delegated to me. Sorry to  
 miss the very attractive lady.  
 Worked very busily all day &  
 by 3.30 felt fagged, so came up  
 to Diltman's office & rested in  
 my chair for 1/2 hour, after which  
 I felt better, then continued to  
 6 p.m. - Finished 1505 & 15K, saw  
 May Alexander on I-mil. His wife  
 was in Calif. for 2 years & most  
 anxious to go back permanently to  
 U.S. - Dinner invitation of our  
 Capt & Mrs. Adams (the buds  
 of 2 weeks) at "The Hunt" in  
 Langston Buzzard. Went there with  
 Adams & Tel who is staying there.  
 Met the lady who is most attract-  
 ive, with brown eyes, light colored  
 hair with coppery tinges through  
 it, fair complexion, nice figure (at

119  
 with the rather common Bulky  
 type of ankles) and a sweet  
 smile, pleasing personality I  
 imagine her to be about 22 but  
 may be mistaken <sup>(It is correct)</sup> (Forgoing is  
 intended as memory guide for  
 our Mrs. Adams at 11) - had  
 dinner, after which we sat in  
 the lounge & talked until my  
 bus came at 10:30. - Home at  
 11, still not dark, gave word  
 I was leaving the Swan in  
 morning. Packed up my  
 things. In bed by 12:15 but  
 somewhat wakeful - asleep  
 by 1:00  
 Sunday, June 6<sup>th</sup> - Up early  
 (7.30) finished packing,  
 breakfast, bus at 8:35 &  
 now at B/P Winding up  
 affairs. Tel from Alt. yester-

day which I've not seen yet but general contents of which I phoned Ted by Al Elizabeth says won't write any more on view my imminent return. I am to get data for research started on E. - Had talk with De Grey on this point & am to see Ubbelohman this a.m. - Following being written on train enroute to Stoke-on-Trent, Tuesday morning I had a quick conf with Ubbelohman and arrived at tentative agreement re coop on E work for A.H. - He asked me to draw up brief on it, which I pushed through in a few minutes before lunch, at which Ted & De Grey present - Immediately after it Prof Vincent & I started in BP private car for Cambridge, despite ominous weather and dark clouds - it had been raining pretty hard all morning and

it was still not finished. The car is a quite old one but was among the most expensive models in its day. I was a bit apprehensive at Vincent's handling of it, as the road was very wet and the car did not steer too well and Vincent kept driving at high speed - sometimes as much as 60 and for considerable stretches 50-55. The roads are seldom straight, often very narrow, and you can't see more than 100 yards ahead. However, he didn't get us dithered or in a week and we got there safely, passing through some of the loveliest of English countryside. Cambridge is 50 miles from BP, and we were only 1 1/2 hours en route - One of the places we stopped up to see is "Byron's Pool" - a small pool in the village of Grantchester by an attractive old bridge. Here Byron used to come often to bathe. An old house at the edge of the pool was occupied much

later by Rupert Brooke, whose poem "Slaughter" tells all about the village, the vicarage, the pool in which Byron played, etc. - one of Brooke's boats - En route also we saw one or two concentration camps for Italian prisoners and it is curious to see these P/W walking about on the roads, quite unattended or perhaps with a guard far off in the distance. Vincent, who has the paper in Italian at Corpus Christi College, stopped for a moment to talk with a group of 3 nice looking P/W & startled them very much, they being quite shy. - When we reached C.C. Vincent drove into a court (having a key to the gate), we parked the car and went directly for a walk to see the various sights. Cambridge comprises some 22 separate colleges (just like Oxford) many of which were founded as far back as 1250 or 1260. Some were founded after the Great Plague by the Guilds, in gratitude for the survival of at least a few in the community. Oxford is a bit older than Cambridge and Vincent laughingly told me that current gossip <sup>at the former</sup> tells that Cambridge was founded by those who were expelled from Oxford. - The atmosphere of Cambridge, which I drank in in great gulps, gives one a feeling of "solidity" - the solidity that is England. Here stand in quiet dignity and great strength buildings devoted to learning, and democratic institutions and the dignity of man for nine centuries - still going strong. - I could hear Barbara's voice saying, in the current slang, "solid", with the "click, click" after it. Now she would love it. The colleges are scattered over miles of territory but most of them are adjacent to the river. Cam - a quiet, clear, narrow little river with the most charming

ing borders of grass on either slopes, and quaint bridges connecting the college buildings with the playing fields directly across, or connecting two main buildings belonging to the same college. There are, of course, in addition to the college buildings, "university buildings" which are common to them all, such as the main library - the most modern structure of all and with the latest improvements. V said that the shelves were open to the students who were free to browse around - We saw Queen's with its very old buildings but "modern" dormitory (1800 or thereabouts), and then Kings, with its famous chapel, the best example of Gothic architecture in the world. By the way the formation or disposition of the buildings comprising the colleges is quite standard: opposite the main gateway, with its flanking old

houses stands the Chapel, on the right are the "faculty" or tutors' class rooms, on the left the students' halls and quarters. The side on which the gate is when you have classrooms, I guess, but am not sure of this. The tutors and students quarters are separated into small, two-story sections, so that passage from the 2d story of a students quarters to the 2d story of another students quarters can be had only by going down the staircase to the ground floor and out into the court, then up the next staircase - V said it was most extravagant use of stairs and space - but they started off in that way (monastic - cell-like) and of course they must keep that tradition fast - In each students building is the "buttery" - a room on the ground floor, inside, through which orders for food & drink are placed & filled - There was much

floating on the river today - many loads  
 in RAF uniforms, with their guns. Some  
 lay on the river's banks, locked in  
 tight embrace. - We saw also St John's  
 which has two women sets of buildings,  
 one "Old St John's" on one side of the  
 river, the other - "New St John's" - on the  
 other side, connected by an ancient  
 bridge with a "fallen arch" - which has  
 been falling since Columbus' day. - We  
 saw Newnham College - one of the two  
 for women (the other is Girton), and  
 I learned later, that Oliver Sacks' wife  
 later was sent very recently, the  
 Principal (= President) there. - The 22  
 colleges are autonomous but no student  
 can be admitted into any one unless he  
 has first passed the entrance exams &  
 has been accepted by the University, or  
 rather has been admitted into the U.  
 The governing body of the U - the one that

sets up and guides the policies - is called  
 the University Council and is composed  
 of graduates who are elected by the graduates.  
 Then as to the educational policy there  
 is another board - the "General Board"  
 which is composed of representatives  
 from the various faculties sciences,  
 languages, philosophy, etc. - The two  
 bodies are kept in touch by means of  
 the Secretary, who is the same for  
 both. - The Govt. provides some funds  
 for the University - the Scientific Sub  
 are "University" for example and the  
 funds for the colleges come from large  
 endowments, they own enormous  
 lands, villages, city properties, etc. from  
 which most of their incomes are derived.  
 - The head of the U. is called the Chancellor  
 & his a mere figurehead now - present  
 one is Stanley Baldwin. The real head  
 is the Vice-Chancellor and the present

incident is the Master (= President) of  
 Queen's College. His office goes by  
 rotation to the heads of the various  
 colleges. - Saw also Clare College, and  
 Pembroke. Saw "Hobson's Water Supply"  
 provided by the chaps who originated the  
 (English) expression "Hobson's Choice" - about  
 which will have to talk later. - It rained  
 a bit, very gently, as we were going about.  
 Stopped for a few minutes in King's College  
 Chapel, where afternoon service was in  
 progress. Choirboys singing nice. The  
 old stained glass windows have been  
 removed for safety as Cambridge is right  
 near the coast and is well within the  
 bombing area. Saw lots of guns & a.s.  
 battery positions around, saw road  
 shelters, saw water supply, etc. - After  
 walking about couple hours went to  
 small hotel & had nice tea. Then  
 some more sightseeing & then to C.C.C.

where we were shown our old chambers.  
 I was put up in the Visitor's Room - it  
 must have been for distinguished ones be-  
 cause I looked over the Visitor's Book  
 The record began with Jan. 1, 1926 & there  
 are some of the people who occupied the  
 room since then: Winston Churchill, Stanley  
 Baldwin, Samuel Hoare, John Buchan,  
 Anthony Eden, John Galsworthy, <sup>W Jacobs</sup> Philip  
 Sassoon, Fieldell Hart, J.C. Squire, Gordon  
 Selfidge, Lord Birkenhead, C.W. Dreyfus,  
 and many many others famous in the  
 educational field. There were only seven  
 Americans all told & I recognized only  
 one name - Henry Harris Russell, of Princ-  
 eton. I wonder who Tracy J. Castel of NY,  
 Butler Hallahan of Bryn Mawr, Edw.  
 S. Mason of Cambridge, A.O. Soughton of  
 Phila., J. de Wolf Terry of Norfolk, and  
 Gerald A. Kelliamy, et St. C.B. are? -  
 Well, it was quite an experience sleeping



in that old, old high bed, with a view looking down into the churchyard with ancient tombstones! - There was a "man" to take care of me. He took out my things & laid them out carefully - my shaving things, my scissors & nail file, etc., my pyjamas laid out, and in the morning I'm sure he would have bathed and dressed me if I hadn't beaten him to it. - A "modern" bathroom (about 1870 or thereabouts) with a separate room for the toilet. - Despite the age of the building - around 1500 - it is clean and comfortable. - We went to see Vincent's own "office" or private chambers where he is professor. A most delightful place even without the furniture in it - a large study, a small bedroom, a tiny kitchen, & a lovely view into the "yard" or "court." - Rested a few minutes, washed up a bit, and then V &

I went to the dining hall of Cal. to sit at the Master's table or High table. Met the Master (Sir Will Spens) before going in to Hall, where there were about 2 dozen others - all professors or lecturers in their gowns - plus three British generals and one air marshal. Had a spot of whiskey & then filed into dining hall where the boys were all waiting patiently at their chairs at two long enormous tables, spottishly scrubbed oak with no luan at all. Grace was said by senior lecturer - in Latin - the same as has been said there since the founding in 1450. - We sat down & had a rather simple meal & it's excellent. Soup, Scotch salmon with a perfect sauce, green peas, baked - no browned - potatoes, - and great big fresh strawberries, whipped cream, and plenty of sugar. On my right was Prof Mac-

Crowdy, advertised in newspaper at Johns Hopkins but now professor of psychopathology. We had an interesting talk about psychoanalysis. He knew W.A. White & others I knew. On my left was Prof. Thompson, hotel price winner in Physics and made CMC in birth day -ברים last week. Had a very interesting chat with him as he is in Physics - knows the Comptons pretty well Thompson is the son of the J.J. Thompson, one of the greatest physicists of all time. After that we went for coffee, etc in a room called the "Combination Room" - where people "combine" and I was placed on the master's right, as guest of honor there. In the other room I sat ~~at~~ on his right as place of honor was given to one of the generals on his right, the other on his left. - Coffee, port (vintage) - V. said that people at C.C. were worried

now because the circumstances of post war had changed. He explained in 1944. I had very interesting chat with the master about his daughter (43 - brown eyes) and my thoughts about B coming over to England after the war for post grad work. His idea that if London School of Economics stays at Cantidge, OK but if not, better for her to attend Oxford. After that we all adjourned to the master's private quarters where we met Lady Spew and two others. One with whom I had had tea & husband (Army) who is prisoner in Hong Kong. Had whiskey - soda time & started till 10. Had nice talk with Lucy Gussell (General) who is C.O.C. of whole East Angles. A very affable and interesting man, with whom I discussed war situation. Back to our court with V & I walked round and round for about an hour.

talking mostly about Shakespeare. Been  
chaps. He's done some work on Rossetti  
who was cool-coo in a big way along  
a trend somewhat similar - We went  
to our chambers at 11 and to bed -  
after I spent about 1/2 hour looking at  
visitor register - Had good sleep -  
Monday, June 7th - Up at 8, took  
quick bath, dressed. Breakfast was  
served as in the next room - private  
quarters of a professor Carter (biology)  
who is away. It was charming room  
& a delightful breakfast over a gas  
log fire (a bit chilly this morning). -  
Got our things & made our departure  
about 9:15, taking a different route  
back. Bright sunshine and quite a  
nice day. Lovely countryside again.  
Stopped for few minutes just before  
getting to B.P. to take look at Vincent's  
house = old Julev (say about 1600) with

its thatched roof, new ceilings, and  
altogether charming. Mrs V's daugh-  
ter out so didn't go to meet them -  
Cursed. B.P. about 11 and on to  
another conf with Waldman till 12  
Commandment to my papers as coop in  
K had to be made in view receipt of  
text of telegram from Alt which I'd not  
seen until then. Worked madly at  
it till 1.15, clearing up other matters  
too, lunch. - Got anxious to make the  
3:30 p.m. train, which reached us. We  
expect return for first hours on Friday  
as Trans will probably be back then  
and we must see him before return to  
Wash. - Got to station and instead  
of hopping aboard the extra train which  
was about to pull out, discovered too  
full, decided to wait 15 min for the  
regular. Too bad - as the regular was  
1/4 hrs late - and then we had to start

up all the way! - James Acree + we  
 had to "queue up" - took about 1/2  
 hour waiting. Then to Park Lane where  
 Al had reserved room for us. Jo + I  
 are together again in a nice double  
 room on 7th floor. - Went to Mess for  
 dinner, meeting Al + Eric. Had couple  
 cocktails followed by enormous dinner  
 Chapeau + juice, soup, roast beef, York  
 shire pudding, roast potatoes, peas, -  
 spinach, salad, strawberry shortcake,  
 (rolls, butter + peanut butter). Then to  
 Embassy to look over telegrams. he wait  
 for Del or me + only one snippy tel  
 for me. News for Al the whole day was  
 mended as therefore bawling out, which  
 Al answered + was got fixed for. -  
 Back to hotel at 11 and to bed, after  
 intermittent discussions with Del. -  
 Al has cents in his pants and wants  
 on leaving on Friday - at the latest

on Saturday. And I am going to be  
 pushed most faithfully to make it  
 then. Have conferences scheduled for  
 Wed and Thursday. Nick, maybe  
 back to RFP for final farewells, a  
 bit of home to do some shopping - but  
 how to do without coupons? -  
 To bed at midnight -  
 Tuesday ~~Monday~~ 8th - Good sleep but  
 dim recollection of many dreams.  
 Showed, nice bath, + turned over to  
 breakfast (good fresh fish, turkey). -  
 Routed to Embassy to send telegram  
 off, get transport warrant for this  
 trip, got to Hutton station in good  
 time to get a seat, and here we are.  
 Five hour subway run for 2 1/2 hours -  
 its now 12:45. And train gets into  
 Stoke - on Trent a bit after 1 p.m. -  
 [Walter + Del]. We were very lucky to have  
 seats on the train as it was very crowded

We should have got seats near the head of the train, having 1st class tickets & the 1st cl compartments were up front, but they were all taken by the time we reached the Fuston Station & people were standing in the aisles up there so we went to the rear of the train. The difficulty here is that the trains are no longer nowadays that when they come to a station passengers who are to get off at that station must be in that region of the train which will be alongside the platform. We were supposed to be up front therefore as the cars for Stoke were there. So as the train came near to Stoke we began walking up toward the front of the train - no easy task with people standing in the aisles, luggage on the floor, etc. & the train rocking (as it is now!) At that, when we reached

Stoke we had to jump down to the ground - about 4 feet as the car we had reached by that time was still not at the nearest edge of the station platform. - We were met at the station by an RAF Officer, of sweet appearance, with a car which took us to Cheshire, about 6 miles off, through somewhat rolling country. [I think train is doing about 70 now.] At Cheshire we turned off onto a little country lane and private road to the home of one of the local squires who had given up his place to the government for a Y station & himself is now a Group Captain in the RAF (Albu). We were met at the door by the C.O. - Wing Cmdr. W.S. Swanborough, a tall & hefty man of most affable disposition - I had to give up at this point as train.

was rocking too much, so this is being written Wednesday night. We had lunch with Swanborough - "just a bite" it was supposed to be but it turned out to be quite a repast, with port at the end. Then a tour through his establishment, which I & I found extremely interesting. Mr. Josh Cooper, C.M.G., made a special trip from BPP to be with us - an act of great courtesy in view of his very busy life. - At 4:30 we were served tea, ham sandwiches, bread & jam, jelly roll. At 7:00 we were served a fine dinner, preceded by "gin and french", followed by coffee and port. It was a very lovely evening and the spot was ideal.

calm, quiet, the fragrance of roses in the air and the wonderful color of purple rhododendron which abounds in the vicinity. At 10 we took our departure, in the official car which Swanborough placed at our disposal with a driver - to go 20 miles to Stafford where our hotel accommodations had been reserved for us. The driver went about 55-60 all the time, over the narrow, winding roads, and the ride was a bit of a thrill in that respect. Cooper came along & when we arrived at the hotel he insisted on buying us <sup>double</sup> Scotch & sodas - two pounds & would not let us pay anything or return the courtesy. - In bed at mid-

right, we having left word to be called at 8, with morning tea - which duly came at 7:30, by a maid who brought same and drew aside the blackout curtains.

Wednesday, June 9th. - A good sleep but with funny dreams - which I couldn't recall. The idea of morning tea is a very sound one! I had to coax Ted to partake. He said that Red rather have had the extra 1/2 hour sleep & to be wakened with a bromo-seltzer or a large glass of orange juice instead. But I maintain that hot tea is much better than either or both be mixed. - Breakfast, at which I missed a kipper because the waiter

brought me bacon & fried potatoes & I didn't know there were kippers, damn! - The train is just across the street from the hotel & we mounted at 9:59, fortunately getting seats. The train just hustled along - 70 miles an hour & I don't see how or why those light cars stay on the rails. - I bought a copy of Punch, read that through, then borrowed my neighbor's Jones & read that through. By that time we were back in London. Got cab right away, then directly to hotel. Lunch at Red Cross - no mail. One long urge from Cordeman at last answering - a long-delayed reply that should have come several days ago. - Went over

my papers, as Al had already  
 wired we were both coming  
 back at once, leaving here  
 Friday night! The lot to  
 do. - First thing was to get  
 in touch with Fulton who  
 was in town - to communicate  
 contents. Judge & I had a  
 devil of a time getting him -  
 he had been at the Embassy!  
 - Dinner at the Mess, with  
 Eric, who leaves tomorrow  
 night. A very nice dinner  
 with good steak! - Went over  
 with Eric to his place to  
 collect some liquor he was  
 turning over to Tel. - Tel  
 was out to cocktails with  
 some friends. I forgot to  
 say that Drummond had  
 Al, Tel & me, to cocktails

at the East India Club again  
 as a farewell. I <sup>was</sup> weighed  
 again - found I'd lost 12 lbs.  
 from May 4 to date. Which  
 is not bad at all. - Eric  
 then came over to my hotel &  
 poor Tel came in -- I had a  
 bath, washed about 10 ft. of  
 socks & here I am, ready for  
 bed & next to last night in  
 London. - Am due home on  
 Sunday if all goes well.



Wednesday, June 9th.  
 Thursday, June 10th. - [Written on the  
 train enroute to Park, Friday, 10 pm.]  
 There has been no time since Wednesday  
 evening to write and I can not recall  
 where I left off in the preceding  
 section, which has already been  
 sent off. I think I left off about  
 Wed. afternoon, my struggles to lo-  
 cate Filtman and finally doing so.  
 Also I think I mentioned that we  
 three went over to Dransnow's shop  
 and he took us to East India Club for  
 final farewells and drinks. At least  
 a date for the next, the kind of date  
 to see somebody about getting quarters  
 at Lansdowne Club. I left the car  
 Piccadilly near Park Lane Hotel. I  
 sat down for first minutes on a bench  
 in the park. soon a guard came  
 and asked if his friend's quarters  
 I had not so pronounced to pay just

Then washed up a bit at hotel and walked to mess for dinner. Had a date with Eric there after which we went to his room, he being ready to leave tomorrow on his journey to U.S. He had 2 full bottles of Bourbon (Segrams @ 6/6!) one nearly full of Canadian Club and a bottle of sherry which he was selling to Tel. We carried this over to our room and after chat of some 15 min he was about to take his leave when Tel came in. He had surprise for him as his trunk had arrived - but he'd forgot his key on leaving Wash and it had not arrived here yet - maybe at bottom of ocean by now. We had a drink & Eric left soon. I had a bath and then Tel and I had a couple more drinks.

Pleasant talk re Eric & that mostly business and to bed at 12.30 sleep  
Thursday, June 10th Up early as had date with Mr. Williams at 10.0. at 10:30 and had several things to do at Embassy, such as file vouchers, clear up papers. Spent most interesting hour with Williams going over his show. Was accorded high honor by being taken into sacred room where everything was so simple, without any special formalities such as we would have. It is chief of the section and has three or four officers under him. I learned later from Lyett that by changing the personnel of cipher office in W.O. are civil since Cromwell's day; that one of the responsibilities of the Permanent Under-Secretary of State for War is to guard the state against

possible machinations or conspiracy by the military and that because of this duty he has direct control over all crypt staffs in and out, and therefore practically all the key personnel are civil servants. The appropriation for the Army is an annual affair and if not following the Army is automatically dissolved, into no provision for the war or officers. An annual reminder like our own, I guess. — After visit to William shop had date with Col. Syrett, whose office is in new Annex (The Citadel) to W.O. and scores of feet underground. He took me to the United Services Club which is a rather exclusive one: no reserve or volunteer officers are admitted; no allied officers are admitted; even among the

regular army, navy, air force, branches only the combatant services! No paymasters, no quartermasters, etc! And only the senior chaplains in each of the three services are admitted as honorary members! As a gesture of great friendship and because they are constant, a few Norwegian officers have been admitted and King Haakon is frequently seen there. The place had more gold braid and high insignia in evidence than I'd ever seen before. — But the food was rather poor. Syrett told me that until the war this club had reputation for the best food in London. The place was quite crowded and I was surrounded by admirals and brigadiers etc; — no smoking allowed in the.

dining room! In the main lounge we had coffee and could smoke.  
 - Left Lyell at 2:30 as had date at 3 with Rumbough, Lyman, et al at FITUSA. Tel and Al came along, to say their farewell, at least Al, with me. Had three quick conferences there on three subjects, then was taken to packed precincts of crypt set up in Selfridges Annex - and through the whole works, including the appeal X61753 - Interesting show and glad to hear good reports of my gadgets.  
 - Diner at here, with Eric who left at 7:30. Tel and Al along. Went over to Embassy after dinner & got off long last message to Cordeman. - To hotel at 10, Tel to write letter, I to pack. Also Al. - Al sent down some ice

& soda and Tel and I provided the liquor and we each had two. I got all my packing done and quite ready for bed at 12 - tired out.

Friday, June 11<sup>th</sup> - Up at 9:15 to get ready (start again as had these conferences scheduled, my bags to get over to AIC office, by per drum to collect, etc. - Saw Lyell at W.O. again, at 9:30, with W. J. Felding and Col. Bloomfield, re call-signs & from here. Then at 10:15 to Air Ministry for deli with W/C Johnston, who was to show me their latest portable gadget - and I saw it - again without fur in feathers. Somewhat satisfactory as they ask no quid pro quo. - Call 10:45 date with Tel at Embassy to go to Finance D, where I collected

few days & converted some into a  
 U.S. checks. - Got 11:30 to E's  
 office, with Del & Al to pay our  
 farewells to him, to see Davis.  
 De Grey and Dickman there too.  
 - Very pleasant chat with C and  
 then we took train, Dickman, it.  
 De Grey to Officers mess for lunch.  
 Del went to Park Lane to fetch  
 the bourbon. I bought 1/2 lb  
 for all. We had most pleasant  
 time, they staying until 2:30 or  
 3 pm. Del and I went to shop  
 in Bond Street, to buy some  
 tickets for family. - Capt. Boyd  
 having provided me with the  
 necessary coupons out of his  
 own lot. I hope E, B. & John  
 will like what I bring them.  
 - Back to Embassy, where  
 went thru c/o office, I having

packed. Boyd - did not do for  
 weeknights. She - does last night  
 to OSS put up, where W. Artman  
 is running gadgets. Was possible  
 with great honors there, and spent  
 about 3/4 hour or more with them.  
 - Back to Embassy for final fare-  
 wells there, then to mess for  
 final dinner. Gave Jo and Ellen  
 each 1.05 - they having been so  
 nice to us, George having put us  
 in their charge. - At 7:30 we  
 reported to A/C Hqs, got our  
 tickets etc. - All very well organ-  
 ized. Bus to Euston Station  
 our bags all labelled and all  
 handled for us - went to placing  
 them in sleeping compartments  
 in the special cars provided.  
 Am in bed now bringing this up  
 to date and it's now 10:45. We

have to be on by 5.20 a.m.  
 so will be wakened at 4.45, an  
 ungodly hour. With good luck  
 we may be able to take off early  
 tomorrow as no people waiting  
 there.

Saturday, June 12th - Up at 4<sup>45</sup>  
 a.m., wakened by porter bringing  
 morning tea - a very fine custom  
 which I think would be wise to  
 adopt. Shaved & dressed quickly. It  
 is quite light now & we are passing  
 through some of loveliest country in  
 Scotland. I doctored train at 80  
 miles/hour as we are a few minutes  
 late. Now getting in & will cease  
 for time being, to resume on plane,  
 or at Prestwick. - 8.00 a.m. Lun in Hotel  
 at Park run at airport for ATC. We got in  
 to Kell-manor (I think it's spelled) at  
 5.40 a.m. (The train goes on to Glasgow)

and a beautiful morning. The sun was  
 just coming up and the sky is almost  
 cloudless. The train was very comfort-  
 able, and the compartments for single  
 occupants are much like our most  
 modern ones at home, with bed running  
 transverse, wash stand, hot water for  
 shaving, plenty of it. - At  
 Kell-manor were pushed up by ATC  
 bus and after about 10 miles run came  
 to Park. Few words of instruction  
 to report at desk at 10.00 a.m. maybe  
 some news than me going out. - Break-  
 fast at 6.30 and had excellent out-  
 meal, powdered egg, toast, jam, & tea.  
 Now taking it easy in hotel lobby &  
 actually had few minutes of sleep in  
 comfortable chair. - 1.45 pm Had a  
 shower at this hotel at 11.15 and the  
 funny part of it was that there was  
 no cold water - nearly got scalded!

At 11:30 the bar opened and I brought Al two double scotch + soda, he bought one so we each had three and felt fine at lunch, which was good. Sat out on the upper deck veranda - saw watching planes take off and had a most interesting sight. The sun is warm but there is a cool breeze. We are now waiting to get aboard. I have passed through Customs, etc + had a momentary anxiety when they asked for my exit permit about which I had not the faintest notion as nothing was said about such a thing when I signed out at the A.G.'s office in Ldn. At any rate my credentials seemed O.K. + they did not raise a fuss about it. - We were given to understand that we land at Iceland

for an hour or so to refresh but I know for certain. I sat on. There are the usual rumours! This place is quite crowded now with incoming and outgoing people - a busy airport! - This morning wrote a letter to Huggel. H, what address I learned just yesterday. Also his post card but Al had I wrote out + sent to him + to the Heddens. - Al + I went aboard at 2:00 and put our suitcase bags on but were told to get off and wait. At 2:10 we were told to get aboard, with all other passengers. There are 26 seats but only about 12 passengers. It is a Douglas C-54, just like the one we came over on. - Warming up engines from 2:15 to 2:45. - Were off, and now over the water at about 2000 ft.

2500 feet ~~up~~ <sup>up</sup> - I put  
 on my sweater & overcoat and am  
 quite comfortable, though still  
 strapped in with safety belt. -  
 4:15p now & we are about 10,000ft up,  
 high above the white clouds. Occasion-  
 ally we pass through one higher than  
 the general level of clouds & the  
 plane shakes a bit. - Still not  
 allowed to smoke. - The water  
 looks very calm below but there  
 are many white dots - white caps  
 which are probably pretty good  
 sized waves. - They're just put  
 on the stream bed. - It got very  
 warm all of a sudden & if it keeps  
 up will have to take my coat off.  
 Still not allowed to smoke - appar-  
 ently not permissible until the  
 cabin tanks are empty of fuel. -  
 When I should think would make

the situation more dangerous - not  
 less. - A C.A. man sitting beside  
 me says the same. By the way, he  
 has on exactly the same pair of slippers  
 just that I am wearing. - 5:15p.m.  
 Just clouds, white fleecy ones, scattered  
 below, through which can be seen the  
 greenish blue colored ocean, and nothing  
 but a heavenly blue sky all above  
 and around. - Looking down at a  
 certain angle, toward the right of the  
 plane I see on the clouds <sup>below</sup> the shadow  
 cast by the <sup>plane</sup> surrounded by a rainbow  
 circle, just a bit bigger, just enough to  
 contain the plane's shadow. A  
 very interesting sight. I've seen one  
 before when flying above the Pan-  
 ama Canal. - Brilliant  
 beautiful sunshine. - Still no  
 smoking, and we've been flying  
 now for some or almost 3 hours.



7:45 p. ~~now~~ ~~was~~ ~~can~~ flying steadily for 5 hours & no sign of land yet. No white clouds but generally overcast. Very smooth passage thus far. - no smoking allowed. - 7:50 Land has been sighted! About 35-40 minutes more to go before landing. - 8:30 p. we have just now landed & are coming to a stop. - <sup>at Weehawk (Camp Turner)</sup> Meeks Field, <sup>hours</sup> out of the rock, almost literally, has a most forbidding and barren aspect as one lands. We were driven in a staff car to the officers club & what a surprise awaited us as we opened the door. And what a lovely dinner we had! And here is the signature of the all-negro officer. ~~of Box~~ 10:40 Back at the airport, Meeks Field by staff car over the rough road. Plane not ready yet so Al & I went to passenger waiting

room where we found ping pong table & played 2 fast games which I won. Rumor that we may go direct to New York nonstop. - 19 hrs at least - but this just a rumour. This room is very hot but outside there is a very cold stiff wind blowing. It would not be so cold if it weren't for the wind. Rikjavik is across the bay, about 20 miles off. I can see mountains all around, most of which have snow at the tops & those which haven't have their tops hidden in the clouds. - 11:15 p. We are now aboard the plane again, waiting for signal to start revving up prior to taking off. News is confirmed that we are going direct to New York, expected arrival 6:30 a.m. local NY time. (All times given above are London time, which is 2 hrs ahead of Greenwich. The local time at Meeks Field is two hours earlier than London time so we have passed

through - 2 fine zones we coming from  
 Postwick to Iceland. It is local time 9:75  
 here or 11:15 London time or 5:15 p.m. New  
 York time So 5:15 p.m. to 6:15 a.m. would  
 make flying time 11 hours and 15 min.  
 Well see how close we come to it. Every-  
 body is now aboard plus a lot more mail  
 occupying last six seats. - Announce-  
 ment that there would be no smoking  
 at all to New York. - 11:37 start taxiing  
 toward runway. 11:44 started down  
 runway. 11:45 we're up off the ground.  
 Climbing fast. - <sup>Sunday</sup> 10:15 a.m. (Edw) time  
 it's quite light now We have been  
 flying 10 1/2 hours so far. I slept  
 at least 6 hours of that time I  
 woke several times and looked  
 out. It was never completely dark  
 and I could hardly tell whether  
 the rosy color in the sky to the  
 right rear was the setting or ris-

ing sun! It was most confusing. In-  
 that add the 1/2 moon visible about  
 1/3 of the way up from the horizon. -  
 We passed over very large ice fields  
 and icebergs, over barren rocky  
 country which showed no sign of  
 life so far as our cold sea - must  
 have been Newfoundland. - I woke  
 several times with the stifling heat -  
 very hard to control it evidently. I  
 was alternately hot and cold but  
 mostly the former. - It is now 10:20 by  
 my watch, hence it must be 11:20 a.m.  
 New York time and if what we were  
 told is correct we should be in New  
 York in about 2 hours. - Not a speck  
 of land is visible now only a vast  
 pool of water in which one can only  
 see very slight ripples - it's very  
 calm down below & the plane is  
 very steady. - As a matter of fact

it's all quite deceptive. The noise of the props is so like the noise one hears aboard a big ship, and the absence of scenery rushing past one (as on a train) makes it seem that we are just crawling along at a snail's pace, not 200 miles an hour. - 10:45 a.m. We have just been handed the usual customs forms to fill out. - Have been told we may land at Presque Isle or New York. At last, smoking is allowed! - 11:30 a.m. Latest dope: The ice field we passed was not at our first approach to land & in vicinity of Nova Scotia. We then crossed Gulf of St. Lawrence. In 1/4 hrs. we land at Presque Isle, have breakfast, then on to N.Y. where we should land at about 11:30 or 12:00 N.Y. time. - Depending on how long we stay in N.Y. we should get to Washington in early p.m.

- We're flying over Maine now, above the white clouds which are very thick but occasionally can see through them, at the farms & forests below, ribbons of roads, rivers, and a lake here and there - It's 12:10 p.m. (Edin) time now and I'm pretty hungry. The purser made hot chocolate an hour or so ago, which had to be thrown out as the milk was sour & it tasted very funny, quite disagreeable in fact. 12:45 p.m. We are about to land at Presque Isle. It is very thick out & can't see anything. Going down now. Seat belts fastened. 1:08 p.m. We're on the runway now & taxiing toward the hangar. It was a very hazardous landing as the ceiling is practically zero. We couldn't see much land until right down out of it. It's raining hard & the weather is foul! - We may be held up here some time. 1:10 p.m. on the dot & we are at a full stop now. Total time in

4:30 p.m. ESDT - started warming up  
4:42 REF ID: A66214  
the air from Iceland to Presque Isle was  
13 hours and 35 minutes. - Bus took us  
to passenger terminal. Customs man took  
up my passport - says it can be returned  
to me in Washington on application, State  
Dept. A fine breakfast, two fried eggs +  
bacon, tomato juice, coffee, toast. - Told  
all flights cancelled + we'd have to  
stay overnight. Possibility of getting  
out on N.E. Airlines Commercial plane  
got a car + went there over bumpy  
roads. Plane to have left at 3:10 p.m.  
was cancelled just as we got there +  
so got reservations on 7:15 a.m. one.  
Then back to terminal, where I shaved  
+ felt better. Al + I then phoned home  
+ glad to hear voice of Elizabeth + Barb  
etc. John still asleep. Told her  
would phone from New York to-  
morrow - Went next door to hotel.  
De "Link" - for transients + got rooms

4:42 start making run  
4:43 plane takes off  
for the night - a brand new temporary  
building very nicely furnished. - Had  
a very fine shower bath after which  
we were notified to report to terminal  
at 3 p.m. as there was a ship now  
available! - Had a fine dinner, tomato  
juice, delicious thick steak, french  
fried potatoes, peas, corn, canned  
peaches, coffee. - Then repacked my  
gear + went to terminal building.  
Sure enough - a plane getting ready.  
Took long time to load up - a cargo  
plane, converted from regular C-54  
passenger plane. We don't have regular  
seats - but what they call "bucket  
seats" along the walls. Not too un-  
comfortable. 4:30 p.m. local ESDT  
the warming up began; 4:35 taxied on  
to runway; 4:42 began the run;  
4:43 up off the ground! - At breakfast  
this morning the Captain of our ship told us

REF ID: A60517  
that we were pretty likely to have made  
a good landing as the information had  
had from the control tower was that the  
ceiling was 1200 feet whereas in fact  
it turned out to be about 200-300. Had  
had a difficult time. - As we are flying  
along now - pretty high - I can't tell how  
high because below us at 100-200  
feet are the pure white clouds, so  
thick you can't see a thing through  
them. It was dark + raining on the  
ground but up here the sun above the  
clouds is very brilliant. - 5:25 p. still  
unable to see through the clouds. Quite  
comfortable riding as yet. - The Corporal  
(Thurston) who runs the Hotel De Ville  
at Prague Isle was assistant manager  
of the Ambassador in Washington + also  
managed the Blackstone there! - We  
are scheduled to stop in New York and  
it takes about 3 hours to make the run.  
5:45 p. We are now just out of the cloudy

area + the fields below are beautiful. Can see  
main highways with a few tiny bugs -  
automobiles. The sun is warm + bright.  
6:00 p.m. now passing over <sup>Portsmouth N.H.</sup> Boston  
7:05 p.m. " " Hartford, Conn. - Beautiful  
country 7:41 p. Just touched the  
ground. + taxiing to port. - 7:44 we  
stop. - Upon dismounting went into hangar  
+ phoned Elizabeth. There was supposed  
to be a medical examination but since  
the medics had gone home the chap  
just asked us if we'd seen him. So  
Cl + I said we probably had, and  
the chap said "OK. I won't ask any  
more questions" - 8:32 p. in. Warming  
up + taxiing to end of runway - 8:37  
We start down the runway. - 8:38 we're  
off the ground + climbing so fast I  
have to keep swallowing. The plane  
is about empty of cargo + there are  
only three passengers all told!

We should make the run to Wash-  
ington in  $1\frac{1}{4}$  -  $1\frac{1}{2}$  hours. Al had me  
to tell E when I called her to tell  
Winnie to have Martin's ready &  
that he was hungry - which I did.  
It's dusk now & humid & hot outdoors  
when we took off. Not bad inside the  
plane but I imagine it will be bad  
when we land in Washington - we with  
my winter suit on & heavy overcoat.  
All my belongings are here - including  
my sticks. - I was made a member  
of the short-stokers fraternity this  
afternoon at Prague I'de by two  
young lieutenant a/c's. 19:53. We are  
approaching Washington now  
and should be at the airport  
in 5 minutes. - Coming downstairs  
now at 19:57 -

e W. Wavelton

Anthony Eden Feb 1, 29

Henry Norris Russell, Princeton

A Marshal Portal

John E. Hallworthy Apr 1928

Americans

Jacy Jaechel

Butler Hallahan

Edward S. Mason

A. D. Sington, Phila

Henry N. Russell, Princeton

J. De Wolf Perry, Norfolk

Herbert A. Villiamy, U.S.A

young birds  
 approaching Washin  
 and should be out the airport  
 in 5 minutes. - Coming downstairs  
 now at 19:57 -

h Churchill (London S in Sept 1927

Philip Sassoon - Jan 16, 1927

Duff Cooper

A Bernstoff

Stanley Baldwin Mar 1927

J.C. Squire

Samuel Hoare

John Buchan

Dorland

H. Gordon Selfridge

8 Mar  
1926

W

1<sup>st</sup> W.P. Ferrick  
1859  
Inspector

...  
... Hallabam  
Edward S. Mason  
A. D. Lington, Ph  
Henry N. Russell, Ph  
J. De Wolf Perry, Ph  
Abel A. Pulliamy, Ph

young house  
approaching Washen  
and should be in the  
in 5 minutes. - Comig do  
now at 19:57. -



CONTRIBUTIONS IN THE FIELDS OF  
COMMUNICATIONS SECURITY AND COMMUNICATIONS INTELLIGENCE

1. As Principal Cryptanalyst (1939-1940), Head Cryptanalyst (1941), then Director of Communications Research (1942 to date) I have had technical and staff supervision over a large staff (in 1945 amounting to almost 10,000 people) of cryptographic and cryptanalytic personnel working on many complicated problems in communications security and communications intelligence before and during World War II. My specific contributions in these two fields are briefly summarized below.

2. My contributions in the Communications Security field during the years 1939-1945 include practically all the systems and devices employed during World War II for cryptographic purposes by the Army and the majority of the systems and devices employed for the same purpose by the Navy and the Department of State. A detailed statement is attached covering the following:

a. Converter M-134 and M-134 A, covered by patent application (Serial No. 682,096) filed by the Chief Signal Officer in my name as inventor on 25 July 1933. This machine was the predecessor of the Converter M-134 C (Sigaba) and represented the first invention of electrical control, as distinguished from mechanical control of a set of cipher rotors in cascade, thus getting away from the regular or metric stepping of the rotors. During the important years 1939-1941 this machine was used for enciphering the bulk of the highly secret and confidential administrative traffic of the War Department in communications with the Headquarters of Overseas Departments, Corps Areas, Defense Commands, and headquarters of GHQ Air Force and 2d Air Force. In addition, it was extensively used by the Signal Intelligence Service in forwarding traffic from our intercept stations in Honolulu and Manila. It was also used during 1940 and 1941 for communications between the War Department and the U. S. Military Attache in London. In 1941 the War Department provided a number of these machines for the Department of State, for use in secret and confidential communications between the Secretary of State and the American Ambassador in London and these were used from 1941 to 1944 for that purpose. It was also used in a special circuit for a number of months in 1942 for direct communication between the President and the Prime Minister in London. After these machines were taken out of War Department service a number of them (29 or 30) were provided the Office of the Coordinator of Information (later OSS) for secret communications between Washington, London, and other capitals where the OSS maintained headquarters. Some of these machines are probably still in service.

~~SECRET~~

b. Converter M-134 C, covered by patent application (Serial No. 70,412) filed on 23 March 1936 by the Chief Signal Officer in the name of Friedman and Rowlett as joint inventors, arose as a result of studies having the aim of improving Converter M-134 A. About 15 June 1935, Rowlett conceived the idea of using a set of rotors in the M-134 A. Rowlett and I then jointly developed the idea by setting down on paper various methods by which it could be applied in practice to the M-134 A. All of these methods were disclosed to the Navy, then engaged in attempts to improve their own unsatisfactory Mark I ECM. The Navy took one of these methods and incorporated it in the design of their Mark II ECM, work on which was begun in January 1938 by Navy contract with the Teletype Corporation. This was done, however, without advising us or anybody else in the Signal Corps until March 1939, when the Teletype engineers brought to Washington the first completed set of drawings of the Mark II ECM, at which time Rowlett and I were invited to the conference with the engineers. A first model was built and delivered on 3 February 1940. Further development was on a completely joint Army-Navy basis and on 19 June 1940 the Signal Corps added its order of an initial 85 machines to the Navy order. On 17 March 1941 the first 10 machines were delivered to the Signal Corps and were given a prompt service test, proving the machines highly satisfactory. In successive contracts the Army procured a total of 3392 machines and almost 2000 were in service by March 1944. The Navy also procured a larger quantity. In the Army the machines were distributed to all commands down to and including HQ of Divisions. They were also used in all important fixed headquarters in the Communications Zone, in all theaters and in the U.S. Whenever and wherever the late President went during the War, the Sigaba went too, on the Presidential Train, at Hyde Park, Yalta, etc. For further information regarding its value in Joint Army-Navy communications, see the detailed notes attached. We know that neither the Germans nor the Japanese were able to solve our Sigaba traffic, though we were able to solve their high echelon traffic, obtaining intelligence of great diplomatic, strategic, and tactical value. In view of the foregoing, the Sigaba contributed materially to our success in the war.

c. Converter M-228 (Sigcum, Sighuad), covered by patent application (Serial No. 443,320) filed on 16 May 1942 by The Chief Signal Officer in the name of Friedman and Rowlett as joint inventors, was a cryptographic machine to protect teletype communications, by providing for automatic off-line or on-line (keyboard) encipherment, transmission, reception, decipherment, and printing of messages (in a single operation) at the rate of over 360 characters per minute, with high security. On 12 March 1942 the first two models, constructed at Fort Monmouth, were given a satisfactory service test. On 18 June 1942 the Navy witnessed a demonstration of the machine and decided to procure 200. By 5 June 1944 a total of 3200 machines had been manufactured and 1488 in service, including 200 by Navy. In May 1943 the machines were used in the United Kingdom to link together all U. S. Army headquarters

~~SECRET~~

~~SECRET~~

in the Defense Teletypewriter Network and these machines were used to encipher a tremendous volume of messages, including raw material for cryptanalysis from all intercept stations. Most of the traffic that was sent by radio teletype was confidential, but on land lines secret teletype messages could be sent by this machine. A modification (Sighuad) permitted use of the machine for transmitting weather data (secret) by the Air Force in two theaters; the same modification permitted use of the machine for secret messages between certain headquarters in Washington. In April 1944, the War Department approved a policy under which the machine could be turned over to the British for use in Combined Communications.

For further information on these machines and additional items relating to contributions in the Communications Security field, see detailed account attached hereto.

d. Cipher Device M-138, covered by patent application (Serial No. 300,212) filed on 19 October 1939. Thousands of these devices were manufactured. For several years this device formed the basis of the Strip Cipher System, which carried a large part of the secret and confidential communications of the Army, the Navy, and the State Department. In the Army it still serves as the back-up system for Converter M-134 C (Sigaba) and as the primary system for Posts, Camps and Stations as well as for circular messages to military attaches. In the Navy and in the State Department it is still used to a considerable degree for secret and confidential traffic.

e. Throughout the years mentioned, in my capacity as Head Cryptanalyst and later as Director of Communications Research, many problems in security were brought to my attention and I believe that my long experience in the field formed a solid foundation for mature, sound judgment in arriving at practical and satisfactory answers thereto. Some of the items that may be mentioned here are the following:

- (1) In 1941, as a result of my special study of the manner in which Army and War Department cryptographic communications were then organized, I evolved and developed the idea of the "Cryptonet" system, which has worked in a highly satisfactory manner in practice.
- (2) The studies and development of Converter M-209, over 100,000 of which were produced and distributed in the Army and Navy.
- (3) The "Stop-gap" or temporary-expedient system of double-loop key-tape encipherment of teletype transmissions.
- (4) The "one-time tape" or Sigtot system.
- (5) The development of voice security equipment, including the "Sigsaly".

3  
~~SECRET~~

~~SECRET~~

- (6) The development of the "Synchronous Polarity Reversal System" of Cifax, which is based upon an important modification (by Lt. Colonel Rosen) of the principles disclosed in my (secret) patent application (Serial No. 478,193) filed on 3 June 1943.

f. I also was a member of the Ad Hoc Committee, consisting of two Navy and two Army members, appointed in 1944 by the Joint Communications Board to look into the matter of communications security in all non-military departments and agencies; the work of this Committee resulted in the establishment by President Truman of the Cryptographic Security Board, consisting of the Secretaries of the State, War and Navy Departments.

3. My principal contribution in the communications intelligence field, directly applicable to our operations in World War II, was in connection with the solution of the Japanese cipher machine (purple system) employed by the Japanese Foreign Office in its highly secret communications with its Embassies and Legations. As Principal Cryptanalyst in the years 1939-1941 I was in charge of the cryptanalytic staff that studied this problem from February 1939, when the first traffic in that machine appeared, until September 1940, when we were able to hand in the first translations. By careful analytical reasoning, long and arduous study of the external cryptographic phenomena exhibited by the messages, by correct reasoning, and a wide knowledge of cryptographic mechanisms we were able to fathom the mystery underlying the functioning of the Japanese machine and to construct, without ever having seen the original itself, machines which would duplicate the functions of the Japanese machine. So far as I am aware, this is the first time in cryptanalytic history that a machine of such cryptographic complexity was completely reconstructed by pure analysis.

As to the importance of that solution I need only refer to the disclosures of the current Joint Congressional Investigation of the Pearl Harbor Attack by the Japanese and to certain statements contained in the Chief of Staff's letter to Mr. Dewey. While the solution represents the achievement of a cooperative effort by a number of people, it was made possible by good coordination, and proper technical direction of a fair number of skilled cryptanalytic personnel who were selected and trained by me and who worked under my direction for over 18 months as a harmonious team. I do not believe that this machine was solved by any other cryptanalytic organization. We know that the very competent British organization failed in its efforts to solve this problem, for we gave them the solution and a machine in January 1941. Nor did the German cryptanalytic staffs who attempted it gain any success.

During the succeeding years, 1941-45, the Agency accomplished many feats in cryptanalysis, too numerous to mention. The diplomatic communications of many countries were read, some almost in toto; the

~~SECRET~~

~~SECRET~~

secret communications of the Japanese Army and Air Force were read to a considerable degree, contributing greatly to our victory in the Pacific. In my capacity as technical adviser to the Chief of the Agency, and having Staff Supervision over all the technical operations of the Agency, I was always consulted by him and acted as advisor to all Chiefs of Divisions and Branches in these operations. The extent to which the Agency engaged in the research, development, and use of high-speed analytic equipments to facilitate the application of cryptanalytic techniques and processing is worthy of mention, and my technical advice and collaboration was used in all these cases.

4. From my earliest days of duty in the Office of the Chief Signal Officer I have taken a deep interest in the preparation of texts for use in training military personnel in cryptography and cryptanalysis, and the War Department has published a series of such texts which were written and prepared entirely by me. I regard the writing of this literature, which was extensively used at the various Army Signal or Communications schools, and in the Army Extension Courses, as one of my very important contributions to the war effort. I believe that this material represents an important contribution to the science of cryptology, because for the first time its basic principles and techniques, hitherto scattered in a most chaotic, disorganized manner in foreign literature, were set forth in a scientific, logical, orderly and clear manner; and consistent, adequate and scientific terminology used in this work. Upon them were also based a long series of graded exercises, with approved solutions, also prepared by me, which were used in conjunction with the texts by thousands of enrollees in the Army Extension School, in the various schools throughout the Army during the war, in the special schools in cryptography and cryptanalysis at Fort Monmouth (later at Vint Hill Farms Station), and at Arlington Hall Station itself, to train thousands of new employees. All or most of these texts were also used by the U. S. Navy, the U. S. Coast Guard, the Federal Bureau of Investigation, and the Department of State; copies were also officially furnished the Canadian and British Government.

It was at my suggestion that the War Department, on 11 October 1930, formally established the Signal Intelligence School in Washington, for training Regular Army officers in signal intelligence operations. I served as the Director of that School, in addition to my other duties, organized the 2-year course given, and directly supervised the instruction. The fact that of the nine Army graduates (there were two officers from the U. S. Coast Guard and they also worked in the cryptologic field later) seven came to occupy top-level positions in communications intelligence and communications security work during the war.

In addition to the foregoing, numerous technical papers were written by me in my spare time; these were usually published by the War Department as secret or confidential documents, or they appeared

~~SECRET~~

~~SECRET~~

as articles in the Signal Corps Bulletin (restricted). Two of the most important of these works are entitled "Analysis of a Mechanico-electrical Cryptograph", in which I set forth the basic principles and techniques in the solution of cryptograms produced by electrical rotors in cascade, and "The Index of Coincidence", a revision of an earlier paper under the same title, in which there appears for the first time in cryptologic literature applications of statistical theory and techniques, later to become of great importance.

~~SECRET~~

PROPERTY  
OF

WILLIAM F FRIEDMAN  
3932 MILITARY RD  
WASHINGTON  
15  
DC

1946  
October

S M T W T F S

1 2 3 4 5

6 7 8 9 10 11 12

~~13~~ ~~14~~ ~~15~~ ~~16~~ 17 18 19

~~20~~ ~~21~~ ~~22~~ ~~23~~ ~~24~~ ~~25~~ 26

27 28 29 30 31

Col Cook's Quarters

71 Karl Koenig Weg

W-14604

Office

Tel Frankfurt military } 21989  
  } 23210

APO-757-(Frankfurt)

Approved for release by NSA on  
06-05-2013 pursuant to E.O.  
13526

## Log

- 2 Oct - 0530 Left Wash (Wed a.m.)  
 - 0750 Arr Westover Fld, Mass
- 3 Oct - 1400 Left " "  
 - 1935 Arr Harmon " Stephenville  
 (2735 local time)  
 0035 GMT 4 Oct
- Sunday  
 6 Oct - 1200 Left Harmon Fld (7 1/2 hrs)  
 - 2145 Arr Fagans (local time)
- 7 Oct - 0015 Left "  
 mon 0925 Arr Orly Rd Paris (7 1/2 hrs)
- 9 Oct - 1015 Left Le Bourget, Paris  
 Wed - 1200 Arr Amsterdam  
 1245 Left "  
 1530 Arr Copenhagen  
 1615 Left "  
 1830 Arr Stockholm
- 6 Oct - 0815 Left "  
 Wed - 1315 Arr Paris
- 7 Oct - 1100 Left Orly rd Paris  
 Thurs - 1315 Arr Eschborn, Frankfurt
- 27 Oct - 1800 Left Frankfurt - by rail  
 Sunday
- 28 Oct - 0815 Arr Paris - Gare de l'est  
 Monday

Paris → Fagans 1785 Fagans → Stephenville  
 1712 Stephenville → Wash 1194



Articles taken on  
Trip to Europe  
October 1946

- 9 Undershirts
- 9 Shorts
- 2 Long underwear
- 3 Pro pyjamas
- 1 Turkish towel
- 1 Wash cloth
- 2 Hand towels
- 14 White Handkerchiefs
- 1 Silk gray "
- 1 Brown "
- 1 Blue "
- 9 White shirts
- 6 Ties
- 9 Pro socks
- 1 Flashlight
- 1 Clock, small Swiss

- 1 - Handbag, black
- 1 - Valapack
- 1 - Musette bag
- 1 - Hat
- 1 - Cashmere scarf, blue
- 1 - White scarf
- 1 - Overcoat
- 1 - Brown 3 piece suit, suspended
- 1 - Gray 2 " " "
- 1 - Pr Sherked trousers, belt
- 1 - Blue spot coat
- 1 - Gray vest
- 1 - Wool sweater
- 2 - Pr shoes
- 1 - Cap, wool
- 1 - Pr rubber overshoes
- 1 - Pr spats
- 1 - Bathrobe, brown wool
- 1 - Toilet kit, silver back  
brush, comb, safety

Tuesday

1 Oct - Left home at 1930

Ari ATC 2010

Checked in etc. Word that

plane was coming from Westover  
 Airport, Mass. but had not yet  
 started. Much delay in view.

Met Col. Mike Marcus - what  
 a character. Barbara + he

argue. At 2310 word that  
 plane had just left Westover.

ETA 0123. I sent family home 2300

<sup>Wednesday</sup>  
 2 Oct 0125 Plane arrives. Briefing  
 with parachutes - my 1st experience

with them. Notified of 2 hr delay  
 in starting - for servicing plane

0300 - notified heater system  
 out of commission + would be

further delay. Col. he still un-  
kited but pleasantly so, only  
too talkative.

0530 - We board + engine warmed  
up - until 0545 - we take off for  
Westover field, minus heat. I put  
on my spats, wrap blanket around  
me, over harness + sleep lightly  
for 1 hr about. At 0750 arrive at  
Westover. Good breakfast - 2 eggs,  
spiced ham, 2 cups coffee, doughnut  
Latest news - be back at 1200 - but  
no place to go so hung around ATC  
terminal. Lunch at noon. On re-  
turn, information we leave at  
1500. At 1500 changed to  
1730. At 1700 changed to

next day at 0900. Then a rather hectic scramble to find room for night. No space in hotel at Springfield (3 men got one + last room). I inquire about BOQ on post + am told "of course - but no heat." "OK if enough blankets" I reply. Car takes me + 2 others (Healey + Wolfe) to BOQ. Sgt there says quarters but no heat. "Heat in 3rd bldg up the road." So why not? We get assigned 3 nice rooms at \$1.<sup>00</sup> per night. Now 1910 + dinner at mess at 1730 so I lie down + fall asleep at once. Had asked Wolfe to wake me. Pretty nice meal

at 754. Brief walk, then  
 phone Washington. All OK.  
 Tenant 1823 must give post-  
 session for 15 is Judge's decision.  
 Concrete floor laid in 1823  
 basement. 393 - not yet sold  
 but a Mrs Powers very much  
 impressed. Asked E to phone  
 Mrs Healy, Wolfe, Isbell.  
 Short walk. Henry take a  
 bath + get good sleep.  
 Room quiet, bed very comfortable.  
 This afternoon saw movie  
 "Gallant Journey".  
 My feet warm at last - two  
 pairs woolen socks + spats.  
 One pair from ~~the~~ <sup>the</sup> ~~shower~~ <sup>shower</sup>  
 + to bed at 9 and read Sat  
 Eve Post a while. Not interesting.

3 Oct 46 Thursday. Woke at 0645,  
 shaved, dressed, walked over to mess  
 had nice breakfast checked out  
 of BOQ + walked to Terminal. Latest  
 dope - off at 1100 instead of 0900!  
 They hope. - Still some work to do.  
 1215 - I walk outdoors + just happen to  
 hear loudspeaker noon news tell of  
 crash of plane taking off at Stevens-  
 ville this a.m. 39 passengers presumed  
 to be all dead. I immediately place call  
 for home. Line busy for 10 minutes. E  
 there, hadnt yet heard of this crash  
 but did of one out West last night.  
 Told her to phone others + to take out  
 \$5000 more term insurance. - Under-  
 stand lunch to be served on board here  
 1330 and we're all ready to go  
 1350 - We go aboard with Hanson

1400 - We take off. Cruising altitude to be 7000' - It's a beautiful sunny warm day. Everything OK.  
1915 EST - 2115 local at Harmon Field

Arrived after a very pleasant journey during which had a chance to go up front & see controls etc.

Had a very nice dinner @ 45¢ - broiled ham, thick slices & lots of it, mashed potatoes, salad, dessert. To bed early in room with 5 others. Didn't sleep because I took coffee as an experiment. It worked. - We were told we'd be awakened at 4 a.m. & would take off at 5. - We weren't & didn't.

4 Oct Friday - up at 0700, shaved, dressed, walked to terminal. nice breakfast - ham & eggs. News - flight delayed - on a/c bad weather.



1200 - Still no news - take off indefinite.  
Took walk in warm sunshine. Mountain  
on which AOA plane crashed yesterday  
& scene of crash quite visible - only 12  
miles away. Talked with pilot of our  
ship about it. Says he usually goes over  
that hill - 2500' high. The AOA ship left  
at 0500, still not light. Apparently could  
not gain enough altitude to go over & tried  
to turn away - or else something went  
wrong with controls or possibly ship hit  
a downdraft. Crew (5) + Passengers (31)  
all killed. On way to Germany - wives of  
service personnel & several very young  
children. Waited around terminal all day.  
Saw C.G. helicopter come in and land -  
help in getting bodies out, if any. I

talked with Chaplain who went up to scene. Says all but 2 bodies burned to death - no remains of others. Plane was fully loaded with gas. - There was a USO camp show crew here on way to Greenland. I had chat with one of them - magician Karl Rosini. Talked about Houdini & Dimminger, who he says is very daring - takes long chances. - Had dinner at 6 & went to movie - terrible Roy Rogers picture. - Back to terminal - no more news re flight. - My shirt is a mess & I can't get at my baggage - will have better next time & wear colored shirt & take enough clothes in my bag. - These long delays most exasperating.

5 Oct - Saturday - Had a good night sleep. We were not awakened at 4 or even at 8. Got up and

dressed, over to breakfast at 9:30  
and still no signs of departure.  
Latest info is that we cannot  
possibly leave before 2:00 tonight  
and probably won't until tomorrow.  
Got my baggage out of the plane,  
took nice shower, changed to  
fresh linen & feel better. Put my  
brown suit away & am wearing  
my checked slacks & blue sport  
coat. - No news & no newspapers.  
After rather poor dinner went to the  
movies & saw indifferent mystery  
detective story "Deceit" and then to  
Officers Club where Sat. night dance  
was on. Had a couple of drinks with  
our crowd & danced one with Max  
Dunn in slacks etc under the hostile  
stares of the officers ladies.

6 October (Sunday)

Turned in at 0130 after a walk to the Terminal where I learned we were expected to go out at 0500. Didn't sleep too well at noisy barracks + guys coming + going all night. Wasn't called until 0930 + told departure to be at 1030. Hustled to dress + get to Terminal. Was pretty sore about having to pay \$3<sup>00</sup> a night for the bed - a hold up game if ever I saw one. Made a protest but did no good. Think I should report conditions there. - We took off at 1215. Plane was tail heavy + we had to do some re-adjusting of baggage + moving forward. Would have had a seat (double) all to myself.

but a guy (Dr Martin) came  
+ has struck by me. He's never  
flown before apparently + is  
pretty nervous about everything.  
Had a pretty rough 20-30 min-  
utes at one time when we went  
into a thunderstorm. Rest of trip  
very quiet. Arrived at Logans  
at 1945 my time = 2145 Logans  
time. Had a rather poor meal but  
cost only 25¢. Boarded plane  
again at midnight + took the  
~~air~~ <sup>air</sup> at 0015. Very quiet calm  
trip so far, at 9000 ft. - Tried to  
get some sleep but couldn't - high  
altitude bothered me. Every time I  
was on verge of falling asleep, would  
wake up with shortness of breath.  
Trip very smooth all the way

despite (as I learned later) very bad weather most other places. -

0925 Arrived at Clerly Field. At once phoned Embassy to try to talk with Lt Stewart. He was out but did talk with another man who knew me (2-3 civilian here working with Maj.

Eastley (SSO). - Bus on to ATE Terminal in Paris where I run into Capt. Russo, who turns out to be great help. Get billet at Hotel Napoleon Bonaparte, lunch there with Russo. Spend afternoon getting plane reservation to Stockholm, after seeing Eastley & Stewart at Embassy. Much ado about cash - francs, dollars, scrip, getting my travelers checks cashed at

Air Express Co. - took 1 hr to get  
\$80 converted into 9416 fr @ 117.70  
per dollar. - Fortunate in getting  
reservation on plane to Stockholm  
for tomorrow p.m. - Bought &  
paid for ticket - 12,400 fr =  
approx \$105. - Sat in front of  
Cafe de la Paix for a couple  
of hours with Capt Russo, I  
bought cognac for him, vermouth  
for me, two rounds costing 270 fr  
with tip included. - Dinner at  
Hotel Nap, now 8<sup>30</sup> pm & I  
must go right to bed - Haven't  
had a good night's sleep for  
several days & none at all last  
night. - Comfortable room &  
bath but not fancy @ \$3<sup>10</sup>

Tuesday

8 Oct - up at 0700, shaved, bathed, to breakfast at 0800 with Capt. R. Then taxed to Am Embassy to see about tel to Stockholm but had to send it at my own expense. Maj. Shanley said to send it collect as they had no funds here for postage but when I went to Tel Office in Emb, no collect telegram accepted. Capt R got some salve for my itch - hope it works. Talked with Maj. Easley + Lt Stewart + then time for lunch. no taxis available so we took a hack + poor horse was made to trot down Champs Elysees. Cost \$50 fr for 2 mile ride. After lunch packed my stuff, checked out of hotel + went by taxi to Air France terminal at Station des In -



valides. Went through all the formalities - police, customs, etc then waited for bus to Le Bourget. Left at 1415 and hectic ride to " which took about 35 minutes. Went through more formalities - money Declaration, Customs. Waited in station. Plane was due to depart at 1530 but by 1600 nothing happened. At 1630 announcement that plane from Stockholm delayed - no news why. At 1645 plane comes in & we are told to wait - no news re departure. At 1700 we are told no flight today - tomorrow at 1800 & to be at Les Invalides at 0900. Back we go by bus to Les Invalides - and we wonder where I will get room for the

night! Air France would find us rooms - but I had only 600 fr + no place to cash travelers checks or get more francs. I take a chance + go by taxi back to Hotel Napoleon B. + was lucky - had another room on same floor. I simply explain flight cancelled + clerk gives me 1 fr. I go up + take possession at once - will straighten matters out with ATC Billing Office later - which I fortunately was able to do. Waited around for Capt R - to get some more francs + have company. Soon he comes in - surprised to see me a bit as he had gone with me to Air France + we had every reason to think that plane would leave. Had

dinner together - then taxi to ATC  
 Rabbit 0 to pay for room + make sure  
 I had it. Then by Metro to Champ  
 Elysees - to sidewalk cafe where  
 we had a couple of beers, talking  
 until 2230. Walked to Hotel +  
 now 2315. Went to bed + be up  
 by 0630 - to get to Les Invalides  
 by 0845. - Flight headlines full  
 of another air crash at sea in  
 Far East, 21 died. - Seems as tho  
 there are many accidents this past  
 week + this. Doesn't bother me  
 though.

Wednesday  
 9 October - Up at 0630, breakfast 0730  
 and taxi to station. Wait until 0900 for  
 bus. Again ride to Le Bourget. Repeat the  
 formalities of yesterday but not in  
 detail. Plane departs 1015 - it is

a Swedish Air line plane (DC-2) with only 2 engines so we will have to stop at Amsterdam and Copenhagen. A very pretty Swedish hostess - highly colored blonde with thick + white complexion, blue eyes. - Good journey to Amsterdam, where we land exactly at noon. I have a bite to eat - chicken noodle soup + two sandwiches all excellent, for which I was able to pay in francs - 60. We take off again at 12:45. - The Dutch scene is very lovely - the irrigation ditches + canals dividing up the countryside into quite regular patches. See a good many red tile roof houses - some slate roofs. All looks spic + span. Very impressive + interesting country.

At 1500 we passed over Kiel. Beautiful afternoon, very calm weather for our flight. Countryside lovely. We are over water good deal. Flying at 7000 feet + I'm a bit short of breath, the only + slight discomfort. Had an excellent lunch served aboard. Good beer with it.

At 1530 we arrived at Copenhagen. Very new + modernistic airport terminal.

At 1615 we took off for Stockholm. Weather still fine. - Soon after we leave Copenhagen there is a marked change in the terrain. No more rectangles + squares of cultivated fields and small hamlets. Instead, a very ruggedly wooded region, rather rolling terrain, lots of lakes + swamps, only occasional house to be seen. Probably timberland.

begins here. - We are due to arrive at 1815 - about an hour from now. - Have just had tea (not very warm) and an excellent sweet roll such as only the Danes and Swedes can make. - When I got off at Copenhagen I purposely (+ unthinkingly) left my spats on my seat - and they were taken, probably by some cleaner at Copenhagen. Teaches me my lesson - I've been ever so careful all along - not left anything unattended or unlooked until now - and I lose a pair of very useful spats. - The stewardess is most chagrined, says she'll see

about them on her next stop  
at Copenhagen - but I know  
they're gone for good so far  
as I'm concerned. Will get  
a pair in Stockholm - those I  
lost were old + shabby any-  
how & one button was half  
gone. - Were now at 5000' + my  
breathing is somewhat easier, our  
speed now 155 mi/hr -

At 1735 we are at 3000' + travelling  
more slowly - now ETA is 1830.  
Full moon already above horizon  
though still daylight. Pretty scene  
with sunset on left + full moon  
on right. - Exactly at 1830 we sight  
at Stockholm airport. - I have  
never seen such a fairyland-like  
scene as that I saw on approach.

wing and flying over Stockholm -  
the thousands of gleaming lights +  
reflections on the water between  
the islands. Most beautiful view  
I've ever seen from the air at  
night over any city. - General Kess-  
ler had sent the Legation car with  
driver to meet me at airport - as I  
had asked + it was good to be met.  
Customs formalities etc - they wanted  
to tax me for extra cigarette but the  
Legation driver talked to Customs  
chief + I got off without paying  
the 3 crowns they had demanded.  
Drove me to Hotel Rensan, where a  
room for night had been engaged  
- a nice room with twin beds +  
a fine bath. Forgot to say that  
driver phoned way. Conradi.



at airport + I talked with Boris there - good to hear his voice. He invited me to my having dinner with them so I washed up quickly at hotel + on going down met Boris, daughter Ingrid + son-in-law Coradi a very nice looking young man. Boris took us to the famous "Gilde-ene Frieden" - where E + I had dinner ~~the~~ evening 18 years ago. - A very nice dinner and then I went to my hotel + to bed early as I was pretty tired. The itch bothered me a good deal but I got to sleep fairly quickly + slept until 0800.

10 Oct - Thursday - A pretty good sleep + hard to get up but I'd agreed to meet Coradi at

0945 to call on General Kessler.  
Not time enough for breakfast  
by the time I'd finished shaving  
& bathing so I skipped having  
any breakfast. - Had a very nice  
visit with Gen K & then was  
driven in legation car to Boris'  
office. - Here in Stockholm they  
also drive like mad & it's hectic  
riding in an auto. - After a  
few minutes with Boris showing  
me around the plant we were  
driven downtown in a tiny  
German car with chauffeur  
to largest department store  
where Boris took me to lunch -  
my breakfast, too. - Started with  
sour cream - excellent idea.  
Good fish & excellent sauce.

After lunch back to B's office  
 in his new Lincoln, wonderful  
 car. Spent couple hours talking  
 + left at 16.00 to get my belong-  
 ings at hotel + check out. Had  
 room for only 1 day as space is  
very hard to find here, too. →  
 Drove out to B's country place -  
 a wonderful estate about which  
 more later: - <sup>The place</sup> ~~is~~ <sup>is</sup> out for me and  
 An exceedingly  
 warm welcome from Annie,  
 looking very well. - B's father  
 here, over 87 years old; a nurse  
 who looks after him; a young  
 woman whose job is to teach  
 crafts to the women folk on  
 the estate (about 250 people  
 work + live on the place!), and  
 B's youngest son Gunnar,

just graduated in forestry - a tall, strapping young man looking not at all like B. - Early dinner very simple, as Annie had to go to Red Cross meeting. - But I talked Swedish history for an hour or two afterwards + then went to crafts class conducted by the young woman. Also went through the building where class is conducted - more about it later. - Back to main house + talked some more. Retired early - 2215 as I was tired + again bothered by itch - + about a dozen bites of some insect - look like jigger bites but can't be that. - Am wondering

what I picked up at the various ATC places I stopped on the journey. - Good thing I had my inoculations!

If this Feb doesn't let up soon I'll have to see a medic now 23:30 + my to bed. Will have breakfast in bed!

11 Oct - Friday - My alarm went off at 0800 as set but I didn't get up - a rather restless night. I was troubled with the itch + had had tea for supper + the combination was too much. I read until 0100 or 0130 and had difficulty in getting to sleep. - Also worrying a bit about things back home. At any rate, at 0930 Boris came

up with a tall glass of orange  
 juice and at 0945 Anne with  
 a breakfast tray. - I felt quite  
 embarrassed with all the allentia  
 Tea, toast, marmalade, and thin  
 slices of cheese. - Rd Bois of  
 my itch + agreed to go to see  
 doctor today. - Took bath (hot)  
 and as usual caught cold. -  
 I just don't dare take tabs.  
 Began APC tablets this afternoon  
 + think I have it under con-  
 trol. - Bois + I took a tour  
 around estate this morning  
 Lots of interesting things on the  
 325 acres. - Lunch abt 1200 +  
 soon after we drove to Sunderland  
 to see medico. - He said it was  
 an urticaria. allergy - from

the bite of some insect - probably lice! Gave me 3 prescriptions - two internal, one external. - I  
feel lots better tonight already  
& hope I am over it - Drove  
with B to the shores of a lake  
that leads directly to the Baltic  
this while waiting for pharmacy  
to make up the prescriptions.  
Back home by 1500 + I took  
a nap - slept for 2 hours  
solid. - Forgot to note letter  
from E this a.m. - killing of  
sale of 393v military rd. 110  
& great stuff + much relief.  
Will be able to "turn around"  
financially now. - Supper  
at 1800 - hard shell crab  
fixed in delicious style +

several other things, especially two  
jams, one made of "field berries"  
+ another of

- B + I spent three hours dis-  
cussing technical matters, then  
looked over + admired many  
features of their house - all of  
in most modern style + must  
have cost plenty to fix up.  
Now 2015 + time to burn in.  
Annie made me a hot drink  
of elderberry brandy, honey, +  
hot water.

13 Oct - Sunday - Spent all day  
yesterday (Saturday) indoors  
nursing my cold. up at 0900  
and downstairs to breakfast.  
At noon, more guests - the Hoop's  
oldest son Karl Wilhelm, with



one of his professors at the medical school & another visiting prof from Buenos Aires, both very nice men. Also Ingrid and her husband Major Coiradi later - in time for supper. It was a rather nice day, a bit chilly out & I was sorry to have to stay indoors. Took a long rest in the afternoon. Fairly early to bed but read until midnight. Up at 0845, breakfast at nine and at about 1100 we all went to visit Gipsolun Castle, started in 1300 something. There were rune stones found in that vicinity & I got Boris to take a photo of me standing beside one. The castle quite interesting.

and is a sort of national picture gallery now - about 1200 portraits there. - Had tea at an Inn nearby - very clean and nice. - Back to Sundsvä + sat around talking a bit - then a short rest. Dinner at 1700 - excellent food. - Boris had insisted on putting in a long distance call to Ed + it came through at 1830. Quite thrilled to hear Ed's voice but not too good transmission. All seems OK at home. Barbara off to Boston + then New York. J.R. at Thaca. - In the evening B showed colored slides of his trip to U.S. etc - very fine pictures. - Now 2230

and must go to bed at once  
 as I've got to be down to  
 breakfast at 0745. My cold  
 is much better tonight but I  
 have some headaches - probably  
 from all the medicine I took.

14 Oct - Monday - up at 0700 +  
 down to breakfast at 0745, feeling  
 pretty rocky with my cold. Drove  
 in to town and first went to Leg-  
 ation to get some knowl to buy  
 ticket back to Paris. Cost \$105. +  
 Spent a few minutes there and  
 then to other building of Legation  
 to call on Mr. Hogg, who is now  
 in charge, in absence of new  
 Minister Dreyfuss + the  
 Charge d'affaires. Hogg +  
 I had met before at Berlin

don two years ago - the time I  
almost got to Sweden but didn't  
because the powers that be deemed  
it unsafe for me to go + Capt.  
Carlson went. Situation still  
rather precarious. I am to see  
Hjerp again tomorrow. - Then  
back to M.A.'s office where we  
picked up Gen. Kessler who  
came along to go through the  
Hagelin plant, his first visit  
there. - Lunch at the NK  
Dept Store where B + I had  
lunch before. But this time  
May + Mrs. Conrade + two of  
B's executives. Very nice lunch  
after which B + I went back  
to the plant + I examined all  
models of machines until

about 5 p.m. Stopped to pick  
 up my laundry at Hotel Pusan  
 & found it pretty expensive.  
 About \$2<sup>50</sup> for 3 shirts, 3  
 underwear + 4 pair socks!  
 No hotel room yet for Tuesday  
 night - I leave Wed morning  
 at 7 at don't want to spend  
 night at Sundoo's as I'd have  
 to get up so early in the morning  
 make it to airport. My Con-  
 radi dug up 3 bottles of  
 liquor for me out of his own  
 stock & I am much embarres-  
 sed about same. These people  
 are doing entirely too much  
 for me & won't let me do  
 anything in return. - Drove  
 back to Sundoo's at 1730

stopping for a few minutes  
 to see B's father at his  
 apartment in Stockholm -  
 a place with a lovely view  
 of the water & the new big  
 bridge. - Dinner with just  
 Anne & B & then B & I  
 sat around discussing busi-  
 ness matters for several hours.  
 Putting finishing touches  
 on questions of interest to  
 me. - Now 23/15 & won't  
 have to get up until 08:30  
 tomorrow we go to opera.  
 Have had an interesting day  
 despite my feeling quite  
 miserable with my cold.

15 Oct. Tuesday - Up at 09:00 after a  
 very good night's rest. After

breakfast, B took me to see his new brick factory, which is under construction. Saip brick manufacturers are extremely conservative and his new factory leaves them more or less aghast at his novelties. But B says it will be efficient enough to pay for itself after but 5 years - which means about \$800,000 to be made in that time. I found the place interesting but a bit beyond me - much tipping of hats when B comes round + very good feeling between him + the people on the place. - Home again + I began packing. Decided to take a chance on a quick bath despite the lack of heat in bathroom, which is how I caught cold first, but seeing that I've had no bath for several

days, decided I just had to chance it. - (Apparently no bad effects, as I am writing this on the next day aloft in plane to Paris.) - Dinner at 1230 and then completed dressing and packing. - B, Annie, + I left at about 1400 for Stockholm in the Lincoln. Nice ride to town despite bad weather - raw, cold, and rainy. - B + I went to B's office, where I was given souvenirs: a beautiful tiny alarm clock (travel-size) for E; a knife with his initials for John; a book for me. - At 1630 I went to NK (Enko) the big dept store, to meet Annie + buy some trinkets. - Bought two scarves (head) for the Hagelin's cook + maids, very nice things. A half dozen beautiful hand-made hand-



parchiefs to take home. These are true Swedish, made originally in a nunnery in the far north but now made by the townswomen where the nunnery used to be. Expensive enough - 9.75 each = \$2.75, but nice. - Annie then insisted as she had all along, on buying a gift for F, which I insisted must be inexpensive but true Swedish. So she bought two ash trays of a variety called Argenta (inlaid silver in green pottery, designed by Swedish artist named Wilhelm Kage. It will be somewhat of a chore carrying the package back but well worth it. Then Annie insisted on buying a scarf for Barbara with typical Swedish design + figures. - I bought a nice box of candy for the evening, as we were going to the

Opera. - At 1720 we left NK, got a taxi to go to cocktails at the Higgs' - he in charge of Legation now (as I think I mentioned once before). Lovely big apartment, met there Mr. Higdon, SSU representative + had brief talk with him + Higgs re Swedish crypt outfit (total 400) staffed with good many J's, E's, S's, + couple R's. Higgs gave me copy of recent Sw white paper, re our talk on Monday. Higdon told me he had it on most excellent authority that B built machine for Fish - which was great surprise to me but probably true. Gen + Mrs Kessler at party + Mrs. Revndal (wife of Charge) + two other ladies. Mrs. Higgs nice but not looking too well - says she has had case of "Hives" (like I have) - Also Major

and Mrs Couradi, Boris, + Annie  
Of course, at party. - Had one nice  
old-fashioned + some snacks. - Left  
at 1830, to Opera Restaurant where  
we had a lovely dinner, with moderate  
drinks + many "skalls" among B, A,  
the Couradis + me. - Then to opera to  
see Thais - a very fine performance.  
We sat in an excellent box in the first  
balcony, surrounded entirely by very  
fine looking people. Incidentally, I  
am much impressed by the fine  
looking Swedes, well groomed and  
well-dressed everywhere. - I enjoyed  
the opera immensely although of  
course I didn't understand a word  
of Swedish. - The company very  
good + the leading baritone gave his  
last performance before sailing to

U.S. where he joins the Metropolitan  
There was some excellent dancing +  
baller work. - I had never seen

Thais + was glad of the chance. During

the two intermissions we circulated

in the foyers + examined the building -

quite ornate + impressive. - The per-

formance lasted until 2300 or 2315 +

then I said my farewells to the

Conradis. B + A then took me to my

hotel - almost the last room available

in the whole of Stockholm + obtained

for me only after diligent search by

the Legation. I found it a very

small hotel, about 3<sup>d</sup> rate (B

called it a "flophouse") but very

clean. It was after midnight

that I turned out the light + tried

to get some sleep. Had to be up

by 0600 to get to the air terminal.  
 I forgot to say that I had an almost tearful farewell with the Hagelins - they are such charming people & I hope they will really come to Washington this spring, as BTA promise.

16 Oct - Wednesday - up at 0600, with my two alarm clocks & the hotel attendant waking me - but I didn't need waking as I hardly slept. - Too much noise all night for one thing & early morning stirring about in the very narrow street outside my window - But I must have slept some as I recall dreaming a bit. - Got a taxi & went to the "Flygspanlin" - arriving there by 0640. - Checked in & got

weighed in - overweight by several kilos (what with all the liquor Courade insisted on presenting me). Handed the clerk a hundred kroner note - which he had much difficulty in changing, to get out 22.50 kr for excess of 6 kilos @ 3<sup>75</sup> per K. - Got on bus + we left at 0700 on the dot. Arrived at airport soon, checked in, + had some breakfast. - Then went through customs + money control - no trouble. - Changed all my Swedish money to francs. - Boarded plane at 0800 + took off at 0815 on the dot. - This is a big Douglas C-54 type, capable of holding 40 passengers but there are only a dozen or 13 of us, including a well-made up actress - French Imp-

pose. She has a rather extreme dress on - slit down the front all the way to her navel. I think. I'd like to get a good view of her with her coat off. Rather good looking, slender + artificial blonde. - The plane is very clean + well managed. Coffee has already been served + soon lunch. - We have excellent flying weather, sun is out, we are at 7000' + now passing Malms. Very comfortable but my feet are, as usual, cold + I miss my spats. - I must see to my accounts now + get those straightened out, to see how they balance. - Well, I'm short only 12.20 kr = \$3.42, which isn't too bad. - At 10:30, lunch was served - Hot consomme, potato salad, some nice

cold salmon, two sandwiches, banana.  
I ate pretty well. - My feet are still  
very cold. - I got a blanket +  
wrapped it around my legs -  
much better than. - It is now  
1245 + practically the whole of  
the journey has been above dense  
white clouds, so could see nothing  
of the ground. - We are going  
down now into the clouds + I  
can't hear very well - my cold is  
what makes equalizing pressure  
pretty difficult. - We are under  
the clouds now + can see the ter-  
rain very well - But I can't  
hear well again. This is my  
first experience with hearing or  
ear pressure difficulty. I hope it  
passes soon. - We arrived on



the dot at 13:15, as scheduled. Went through the usual formalities - of money, customs, etc. in rapid style & then got on bus for Paris station des Invalides. - Talked with an American business man from New Haven on bus & with two young Jewish refugees who have been wandering around for several years in Europe, trying to get visas to America. Sad stories & pretty spunky girls. - At station about 14:30 & took cab to ATE terminal, Place Vendôme, to find them in the midst of moving. But made my arrangements for flight to Frankfurt tomorrow & then cab to Hotel Napoleon Bonaparte for billet for the

night. - All fixed up at about  
1530. - Phoned May Easley at  
Embassy to get message to Earl  
to meet me at airport tomorrow.  
He got through on the phone +  
I hope to be met. - Left my  
room, took a drink of my  
Cognac + lay down until  
1800. - Quick dinner, when I  
saw Howard Westlerode, in  
on his way to Washington. Brief  
talk, short walk to Arc de  
Triomphe, bought some roasted  
chestnuts + back in my room.  
Now 2030 + will turn in very  
soon. - Bought French paper  
with headline news about  
Gronin's suicide. - Must be  
up by 0600 to get bus here  
at 0700.

17 Oct - Thursday - Up at 0600, after a fairly good night. The three cups of coffee in the morning still had their effects late at night! - Bus left Hotel Napoleon on time, we got to Orly fld by 0740 only to be met with announcement that our flight would be delayed until 1000 because of bad weather at Frankfurt. Another delay at 1000 to 1100, so I took opportunity to write a letter to E and to walk over to Air France terminal to send a wire to the Nagelins. 15 words cost 122.1 francs. - We took off at a little after 1100 and are having a very quiet + calm trip at 5000 feet. - Visited the cockpit + the pilot of my car trouble yesterday -

day & he said he'd go down very gradually to give my tubes a good chance. - On the door where they usually post the names of the crew members some way had written under Radio-operators the name "A. Graham Bell" asst radio operator "G. Marconi" and under Flight Engineer "O. Wright". When I showed the names to the pilot he laughed & said that that "was intended to boost the morale of the customers". !! - We are right on the course & on time - scheduled to arrive at 1315. - Sun is out & all clear below all the way. - I have been talking with an American girl from Boston on her way back

to Frankfurt from London where she visited with her parents who had come over to see her. - A very nice girl working for FEA at Höchst + has been in ETO for three years. - She says Europe is no place for a young girl. - On the dot at 1315 we landed at Eschborn, near Frankfurt, where I was much pleased to find Earle with car and driver. - Got my bags and took the young lady along with us as she lived close by the Earle in Höchst. - Jean was out at some party so Earle + I had a couple of sandwiches + a drink or two fixed by one of their two maids. Sat around talking for a

a couple of hours then I went up to my room and took a nap until 1800 when I was called for dinner. - nice to see Jean & had a nice dinner. - Charlie Hiser + Jessie Dent came over + spent evening with us. - Spent an hour in E's radio ham station + got talking with a ham in Baltimore but just as I was getting ready to ask him to phone a message to Washington his signal faded out and we lost him. - To bed at past midnight, slept fairly well but not enough as Fark woke me at 8:00 to go to office.  
 18 October - Friday  
 - Breakfast at 10 @ Farben building while I saw Ed + trench.

Two pieces pottery present from  
Anne H to EST -

Artist: Wilhelm Käge

Name: Argenta

It <sup>for some op. ~~had~~</sup> works on Siemens <sup>to fine machines</sup>

1 - No trained personnel for maintenance

2 - " " operating personnel

3 - Physical circuits <sup>most important</sup> not suitable

4 - When tape used to send radio

intermixing of letters & figs very  
difficult. (German telegraph system + G. to be used for  
oil tank type also caused trouble)

5 - Signal O.K. + taking down  
to Regt. 3 Buys, 9 Regts, 1 each + 2 at HQ

6 - Siemens with VHF O.K.

7 - M-log from Regt to Gen  
for classified life O.K.

not a great deal of trouble in  
maintenance of new circuit had  
nobody at all.

1 Oct	Travelers checks	\$ 1.00	
	Cash		<u>50</u>
			\$ 50

1 Oct	Cost trav checks	\$ 3.38	
	Cash to ESF	5.00	
	Shoe repairs	.75	
	Parking	.25	
	Lunch	.50	
	Misc	.42	
		\$ 10.30	\$ 39.70

2 Oct	Breakfast	.40	
	Lunch + dinner	1.50	
	Room	1.00	
	Misc	.66	
		\$ 3.56	\$ 35.14

3 Oct	Breakfast + paper	.55	
	Carboid cigs	1.40	
	Candy, coffee	.64	
	Dinner	.45	
	Telegram	1.30	
		4.34	31.80



4 Oct	Breakfast	.45	31.80
	Lunch	.45	
	Dinner	.45	
	Bar	.75	
	Sandwiches	.20	
		2.30	29.50
5 Oct	Breakfast, lunch	1.50	
	Bar	1.75	
	Billet for 3 days	9.75	
	Box lunch	.25	13.25
			13.25
6 Oct	Breakfast	.45	
	Misc	.40	.85
			15.40
	Supper at Lagens	.25	
	Cigs	.05	
	2 Stamps	.10	
			15.00
7 Oct	Bot frames (585)		5.00
	carry →		\$ 10.00
	[Trav Checks \$450]		
7 Oct	Cashed	80	
	[Trav checks \$370]		
	Recd in fr @ 117.70/\$ - 9416		585
	Borrowed from Capt P		1000
			5600
	Taxi fr	50	14601
	Drinks	2.70	
	2 Etchings	5.00	
\$105 =	Ticket to Stockholm	124.00	1000
	Tips	50	1000
	Misc	85	
		13355	
Hotel	13355		
12 Nights billet			
@ \$13.00 = \$6.00			
	Recd 2246		
	{ \$US 10.00		
	{ Soup 25.40		

8 Oct	Tel to Stock room	267-	
	Excess baggage	375f	
	Tips	40	
	Taxi	240	Bal
	Lunch (scrip) 25	919	1327f
	Taxi	50	
	Tips	40	
	Taxi	52	142
		142	1185

9 Oct	\$10 <sup>00</sup> Scrip \$25.40	fr	1185
	Tips & taxi to pta	125	
	Lunch Amsterdam	60	1000
	Breakfast scrip	25	
	Scrip	\$25.15	
	FR	1000.	
	B	\$10.00	

19 Oct	Cashed one \$10 Trav. Cl	-	35.00
	from 20 " " "	-	Kr 167.75
	" " " " "	-	202.75
	Tips	Kr 4	
	Hotel	25.25	
		29.25	45.25

11 Oct	M.D. Sundaarte	Kr 5	157.50
	Group	" 11	

14 Oct	Laundry (K)	4.25	
	Ticket to Paris	376.00	

15 "	Candy	6 Kr 6	6.00
------	-------	--------	------

	Hakshief	6 @ 9.75	\$58.50
	Taxi		3.00
	Tip		1.00

16 Oct	Hotel Agent (7.20 + 2)	9.20	
	Postcards	1.50	
	Express wt	22.50	
	Breakfast	2.25	
	Taxi	2.50	

Forward	157.50
Cashed 3 checks \$20 @ 4.194	251.62
From B.H.	200.00
	<u>609.12</u>
Left receipts for H servants	23.00
	<u>586.12</u>
	491.70
	<u>94.42</u>
Misc unacctd for	12.20
Real in K. ones	<u>82.22</u>
Changed into francs Oct	
3.10	= 2,620.

On hand 1,000

16 Oct } Frames 3,620 fr
} Scrips \$25.15
} US \$ 10.00
} Tracks 260.00

17 Oct S\$ 3.00 }  
 Breakfast .50 }  
 Paper .05 }  
 Supper 1.35 }  
 Misc 1.05 }  
 4.95 }

US \$10.00  
 Scrip \$20.20  
 Tracks 260.00  
 Fr 3183.00

18 Oct → →  
 2120 Cabs, tips 304 }  
 3620 Del to Stock }  
 3193 Return 133 }  
 427 437 }

and then E + I went to his office  
in the IGF Bldg, where I made a hasty  
tour of his installation. Then Kaiser,  
Smetana and I went by staff  
car to visit the 114th Sig Svc  
Co which is located on the prem-  
ises occupied by a copper  
mine (now not being worked)  
at a small city named  
Sontra, about 80 or so miles  
north-northeast of Frankfurt.  
Had lunch with Capt. Gilbert  
Smith + his officers at their  
quarters - cooked by German  
women. A pretty good meal.  
She had lots better. After  
lunch we went over Smith's  
installation in the copper  
mine headquarters

building and other buildings. One of them, now being converted to a barracks for his men, was used by the Nazis as slave quarters and Smith described what a terrible place it was when they first took it over. - One item of interest: the German who had been the Chief Engineer of Construction and Operation of the mine was now on Smith's "payroll" - at one carton of cigarettes per month! This is twice as much as the man had been getting at his just previous job - and represents about \$75 per month in real wages. This man is

an experienced and very able engineer, can do almost anything technical in the electrical or mechanical field. - The basic medium of exchange here now is a package of U.S. cigarettes, which are valued at anywhere from \$50 to \$100 depending on what is bought. Nobody sees any German smoking an American cigaret - they simply are used as money and circulate as gold & silver coins would. I suppose ultimately some German gets to make them but as a medium the Germans will trade them unobtainable or unexchangeable items for cigarettes which they then use to buy

the necessities of life. What a commentary on our civilization! Now they are setting up barter markets under official auspices and cigarettes are used as the standard of value - a carton of them gets "55 barter points" a bar of U.S. soap is valued at 8 or 9 barter points, etc. - The ride to Sonutua and back was very nice, mostly over the auto-bahn which is in good shape + all the bridges have either been repaired or have temporary wooden crossings over them. The weather was nice and I enjoyed the trip despite

my cold, which is still quite bad but I have no fever. - We were a bit late in getting back and had to hurry as the Cooks and I had been invited by Gen + Mrs. Sanaham to a dinner party at their new home on the outskirts of Frankfurt. - There were others; Col + Mrs. Bayer, a British Brigadier, who is <sup>Roberts</sup> C Sig O of British Zone, and his aide (a Captain); and French Major General - who is C Sig O of the French Zone + his aide (a charming major). We were last to arrive as not only did we get a late start but also, in Earle's haste



to make time on the road we  
got pined by an American  
M.P. for speeding - and it took  
many minutes for him to make  
out the ticket by flashlight. -  
The cocktails + dinner were  
very fine. The Lanahans have  
four servants + a butler. When  
Mrs I first came they had ten  
servants but when it took  
12 dozen eggs a week to feed  
the family she had to cut down  
on the size of the household staff.  
The monetary cost must be very  
small, on the basis of what  
that German engineer says -  
but since the servants get their  
board it comes to a good deal  
I suppose. See ask Jean

about this & report later. - Got home at midnight & turned in, feeling very tired & not too happy about having to get up at 0700 again as USFET works on Saturday morning. Besides, I didn't turn in right away as I simply had to catch up on this diary - hadn't had a moment for that in a couple of days. - Turned out my light at 0130.

19 Oct - Saturday - Earle woke me at 0700. I'd had a pretty good sleep but not enough. Got dressed & went over to Casino at 14F Bldg for breakfast, as yesterday. - Then to office for a few minutes and then to

Gen. Sanabier's office to make a call, as per his request last night. Spent about two hours with him and with another caller, Mr. Thompson, a VP of AT&T Co, who had just returned from Moscow where he had attended the preliminary world communication conference. I was much interested to hear results of that, knowing most of the Americans who attended. Mr. Thompson remembered me from years back but I'd forgotten him. - I then returned to Earl's office, feeling very groggy from my cold. - Then took a ride downtown to pick up a mess card - and

I had to show his new driver  
the way - and I didn't know  
much myself. - Well, we made  
it anyhow + then returned to  
E's office; closed up + left  
with him for home + lunch. -  
A nice lunch; finished at  
1430 + I said I simply had  
to rest this p.m. - have been  
on the go for so many days.  
- I slept soundly until 1800  
+ now dressed, ready for dinner.  
Was not a bit hungry - in view  
of large lunch later. - After  
dinner we sat around and read  
a bit. Also, Luke played with his  
ham, set with we could get  
nobody in U.S. - Talked with  
an Irishman in Cork about

James Joyce - he not appreciate  
me of Joyce at all, thinks him  
a passing fad. - Turned in at  
2330 and read until past mid-  
night. - Slept well until 1030.

20 Oct - Sunday - Jean cooked  
us breakfast of bacon and  
scrambled eggs. - The cook  
had made "Indian" cake - I  
guess that's poppy-seed cake,  
which I liked very well but  
Earle didn't. - I had suggested  
that we go to see old Frankfurt  
today so that's what we  
did. I felt pretty miserable  
with my cold which is not  
breaking up very much but  
still I wanted to see the  
old city - now in complete

ruins and quite heartbreaking to see. - We met a German who showed us around one old ruin - said the damage to the whole area was done in 17 minutes. - Frankfurt was not bombed until about Feb 1944 and then in 3 nights 3000 tons of bombs were dropped, completely wrecking the whole city. - It's still a horrible shambles. - The old part of the city we visited in detail today is completely uninhabited and the air of desolation and absolute quiet was oppressive. - We took some pictures and wandered about in various areas for a couple of hours then came home. - I took

a bath and got into bed for a nap. - now 1800 and we're going to have dinner with the Boyers. - I feel a bit better tonight - but my head + ears are still stopped up. -

21 Oct - Monday - up at 0700 + to Frankfurt where I had a nice breakfast - ham + eggs. Felt lot better this morning - my ears not so stopped up + cold in chest clearing, with some coughing. Slept pretty well after nice party of the Boyers at the "Cogen" house - a club for colonels + generals, formerly the home of the general manager of IG Farben and quite a lovely place. The Landhaus was

also guests of the Bayers. We had a very nice dinner preceded by cocktails + followed by brandy. Got home at near midnight, after very nice evening out + feeling much better. - No mail this morning at office + at 11:00 we left for a visit to the "Tower" - one of Earl's installations about 12 miles from Frankfurt at Gross-Jeran, where I visited last year too. - Had a very nice steak dinner with Major Eugene Beard and his officers at their quarters. After that we visited the Tower + came back to office at 15:00. - miserable weather



Of this morning had cleared up somewhat. - On my return found E's letter of 10 Oct. - very glad to get word from home & see all OK. - Now

1830 + we are going to another dinner party in my honor by Col. Hines at Kronberg Castle - scare of the jewel robbery. - May see Red Corderman there. -

22 Oct - Tuesday - Up at 0700. - Had a pretty good time last night. As usual, cocktails before + drinks after a fair dinner. - A good orchestra playing U. S. jazz. - Red came (30 drinks) bringing Miss (formerly Sgt.) Dunlap. - The Castle is quite a place and I

would have liked to have seen the place during daylight. - Back home by midnight and to bed right away, my cold a good deal better by then. - Slept pretty well. - Jean made breakfast for us this time + we went to office. - At 0900 Charlie Hiss + May Smetana started off on our 2 or 3 day trip south as far as Munich to visit various installations I'd seen last year. - It started off bad weather but at noon we had the sun out. Later it rained a good deal and quite bad on the roads. - Got to 116th Sig Svc Co at Scheyren about 1800 where Capt. <sup>Sims</sup> Brownschweig is in charge. Had supper after a drink and after

that visited his installation  
& then sat around talking  
shop until 2-300, with a  
few drinks. It has taken  
a year to fix up the place  
& as yet there are no operators  
at all - such a shortage of  
men & materials. - Capt B  
gave me the guest room, a  
fine but comfortable room  
but I didn't sleep at all  
well as I'd had a couple of  
cups of coffee at noon (there  
was nothing else to drink  
when we stopped for lunch).  
Capt C is using a great  
deal of German labor &  
gets his material where &  
how he can - "scrapping"

when necessary. He's built up a very nice place. Met his officers too - one I'd seen last year at the same place W.O. Cagle. - Turned in fairly late & very tired.

22 Oct - Wednesday - up at 0730, breakfast - I'd sworn off coffee for good so had cold tomato juice for liquid & no hot stuff. Left 0900 we left for Munich to visit a prospective ~~new~~ site at Riem. A terrible day, so foggy could hardly see the road, and cold & very dismal. We didn't see much at Riem & got back to 11<sup>th</sup> at 1300 where

we had lunch. Said farewells  
at 1400 & started on long  
road to Anspach, where we  
are spending the night with  
St Col Abramowitz whom  
I'd known since my early  
days at St. Leonards. -

The journey was through  
village after village -  
as dirty, unkempt, filthy  
& dismal as any I've  
ever seen in France. - I  
got a hopeless feeling  
about a people who I  
would put up with such  
living generation after  
generation. The German  
cities all ruined & the  
German villages so dis-

reputable looking + so  
 hopeless in future prospect.  
 - Dinner at the Stramont  
 house - a lovely dinner  
 served in first class style.  
 I'd never met Mrs. A before  
 + was glad to do so. Hsieh  
 + I share the guest room.  
 Miss Smatana has a room  
 at the school. - Tomorrow  
 morning we visit the school  
 which is getting famous  
 as the model Sig C  
 school in the world. Its  
 now almost 2300 + Jim  
 Hsieh as will turn in.

24 Oct - Thursday - up at 0700  
 after a pretty good night's sleep.  
 Breakfast of fresh scrambled  
 eggs + toast. - @ Stramont

Then took us to his school +  
showed us around - a very re-  
markable piece of organiz-  
ing work done in 2 months -  
+ he very proud of his accom-  
plishment, for which I don't  
blame him. - A staff photo-  
grapher followed us around  
+ I expect to see some good  
pictures. - The Chaplain  
interviewed us for the post  
newspaper. - A 1st class show  
all round + one of which the  
Sig C is justly proud. -  
Then by auto to Bamberg  
where we interviewed the  
Sig O of the Constabulary  
HQ + lunch there - a full  
+ good meal for 15 £. - Then

a very long and tiring ride  
to Frankfurt. In all we  
did about 600 miles since  
Tuesday a. m. + I was very  
glad to get back safe & over  
rather poor roads. - I wish  
I could put down my many  
impressions + sights I saw - but  
am too tired now - maybe  
later if I can remember all.  
Got to Frankfurt at 18.30 +  
the Cooks were having a  
cocktail party for us. I  
had 10 minutes to shower  
clean up. Party was for  
office people plus the  
Bayers + I had a pretty  
good time - but very tired.  
It's now past midnight +



I must be up by 0700. - Had  
 a bath + will turn right in.  
 25 Oct - Friday - Up at 0700  
 after a rather poor night from  
 indigestion following my injudi-  
 cious partaking of nic-wads  
 at the cocktail party. To office  
 + breakfast of good omelette + hot  
 tea. Felt very groggy for an hour  
 + then began to feel lots better.  
 But my cold is still giving me  
 hell - lots of coughing + stuffi-  
 ness in my head + chest. Confer-  
 ences in the morning - with  
 Lt Lane on T-com matters.  
 attended bi-weekly G-V confer-  
 ence with Earle at noon + met  
 a lot of people + listened. - At  
 lunch met Col ~~Chapman~~ Maier.

whom I've known a long time.  
At 1330 another conference  
& at 1400 Earle's weekly  
staff conference. - Marion  
Doyle Campbell called me &  
a letter from her mother just  
as I was about to call  
her in response to word in  
George's message. - Have arrang-  
ed to have dinner with them  
tomorrow. - My air priority  
#2 came from Washington  
today but air priority bond  
hasn't been talking & I don't  
know where I stand or when  
I'll start back. Am anxious  
to return. - Discussed things  
with Earle until 1730 & am  
gone now. must get dressed

to go to another party -  
Red C. is giving for us at  
Bad Kaulaim, only 30 miles  
away! And Jim is tired  
already, to rest for the weekend!  
Midnight - back from the  
party, which was pretty nice. The  
Cooks, Hiser, Miss Dent, Red +  
Miss Dunlap. First at Red's  
house, a large + imposing  
German doctor's residence with  
many rooms but only one  
enormous bathroom. And the  
house had a funny, typical,  
unpleasant odor despite its  
having been thoroughly cleaned  
just this week. - Cocktails  
there + then to the Grand  
Hotel, where we had a very

ice dinner, cakes, liquors + dancing to pretty good music.

The party ended at 2300 + we had the long drive back.

News - Jim probably leaving here tomorrow + certainly by the next day. Will be very glad to get home. Gosh. Jim tried + its 0025 now + must be up by 0700 again.

26 Oct - Saturday - up at 0700, to office + breakfast. - much ado about getting me on a flight to Paris + working me all the odds + ends of leaving here, getting some gifts, writing b + b letters, telephone calls. Thought I might get out this afternoon but it now turns

out I leave here for Paris on  
the 1415 plane tomorrow. - Phoned  
Dr. McCloskey in Berlin had  
most cordial talk. She wants  
to be remembered to following:  
Dr. Brownell, Dr. Ward, St. Lively,  
Dr. Battlingill, Mrs. Friedman. She  
was very glad to hear from me - I  
called her at Red's request in-  
sistence after he'd told her I was  
in the theater. - how must try  
to get in touch with Marion  
Doyle Campbell. - Later - I  
had her over to the Rotunda  
for coffee + half hour talk.  
She more beautiful than ever  
+ looking gorgeously happy +  
very sweet. Sorry not to see  
her husband. - how 23 30 +

I'm practically all packed + ready to leave tomorrow. - Took a nap this afternoon after some shopping. I hope the few things I got are OK - how I hate to do that sort of thing because I don't feel sure of myself + my taste + knowledge of values. I wanted to take Jean + Earle out to dinner but they wouldn't + I guess they're tired out from all the festivities. - We had a light dinner here + just took it easy. I packed + think I've gotten all my stuff in all right.

October

November

S M T W T F S S M T W T F S

1 2 3 4 5 12

6 7 8 9 10 11 12 3 4 5 6

13 14 15 16 17 18 19

20 21 22 23 24 25 26

27 28 29 30 31

Hotel Napoleon Bonaparte, 38 Rue

Friedland - CARNOT 7420 WAGRAM <sup>4511</sup><sub>13</sub>

Maj Stanley + Lt Z.T. Stewart, Room 108

Am Embassy. ANJOU 7460 Ext 182

Capt Glenn - BALZAC 5400 - Ext 155

Office - Rue Fa Peruse, 29

Hotel - Ambassador - 16 Blvd HAUSMANN

Room 633

Suzanne Le Goff - JAS 9141

Col Earle F Cook - Office: Frankfurt mili-  
tary 21989 or 23210 <sup>146043</sup>

Aunties - 71 Karl König Weg, Zell

Orly - GOB 5141

Amb. Pro 7221 - <sup>allan 653</sup>  
Dachau 534

1800 hrs

Sunday  
27 Oct - Left Frankfurt by rail at

Monday  
28 Oct - Arr Paris at 0815

Saturday  
2 Nov - Left Orly <sup>Paris</sup> 1345

Arr Meeks .. Iceland <sup>Paris</sup> 1815 local

Sunday  
3 Nov - Left " 1300Z 1400 Paris 1400 "  
1500 EST, 1900 Iceland, 2100Z

Arrived Goose Bay 1600 local

Monday  
4 Nov - Left Goose 1410 local = 1910Z = 1310<sup>EST</sup>

Arr Upernivik 1835<sup>EST</sup>

Left " 2135

Arr Washington 2325



27 Oct - Sunday - Up at 0900 after  
a good rest. Shaved, bathed, breakfast  
and have finished packing. It's now  
1100 and the weather is very cloudy +  
looks like rain. Supposed to leave  
home at 1300 so as to be at Eschborn  
at 1315. - It's now 1800 and I'm  
writing this on board the Frankfurt-  
Paris Express train. For when we  
got to Eschborn Field we learned  
only then that the afternoon ATC  
flight to Paris had been cancelled  
because there was no plane avail-  
able! So Earle + I at once decided  
to try to get a reservation on the  
train. Luckily it is Sunday,  
traffic is light and I was

## Mistakes I made, and Errors of Judgment.

- 1- To fail to bring my electric razor
- 2- To fail to bring one uniform instead of the gray suit
- 3- To fail to bring two OD shirts instead of so many white ones
- 4- To fail to overcome <sup>my</sup> scruples + not use the currency black market in France.
- 5- To take the necessary steps after 48 hours to get my priority raised.
- 6- To fail to get at least 2 bottles of Shanley from Fasley.
- 7- To fail to bring along that small can of bicarbonate of soda, which I missed having when I was first over but didn't need thereafter!

able to get a reservation. - Then we went back to Earle's house, the Bayers came to visit and we spent the afternoon talking. Also Earle got in touch with a chap in Newark Ohio on his short-wave phone set & I gave him a message to send collect to Elizabeth - but just as soon as we tried to verify & check that the other end got the text & address correct, so much QRM came up that further communication was impossible. So I don't know if Newark got the message straight - if he did I will get it. I asked her to wire me at Hotel Napoleon Bonaparte in Paris &

Get this:

Zurky, F :

On certain phases of war  
research in Germany  
Gen Doc Div - Col Donald Pitt  
NIGHT FIELD.

Send Zurky D+E booklets  
on Russian language

tell me how things are. I'm  
a bit worried as I've had only  
one letter written more than 2  
weeks ago. But I doubt if I'll  
hear from that message so will send  
another from Paris tomorrow. - We  
left Earl's house at 1700, after  
saying my farewells to the Boyes.  
Jean came along with us for  
the ride & to see me off. This  
train is an all-American Army  
train & is pretty fair. I have  
a room all to myself (P-8 girls  
got me that). - We've already  
had supper - at 25¢ served  
in the usual Continental wagon  
lots style & good food. - There  
is plenty of heat on the train,  
too much of fear. - My

berth has just been made up  
 + I'll turn in soon although  
 it's only 2000. But the light  
 isn't too good for reading so I  
 won't be able to do that. I'm  
 just as glad to go this way to  
 Paris rather than by air - a  
 lot of accidents recently & only  
 about 35% of available aircraft  
 are in condition - can't get  
 replacement parts + good repair  
 crews.

23 Oct - Monday - After a most  
 uncomfortable night, because  
 of excessive heat on the train,  
 got to Paris, Gare de l'est,  
 at 0815. - There was no water  
 on the train - it had all run  
 out over night - so there

wasn't any for washing or shaving - and the toilet was very bad because of lack of water for flushing. - Got my baggage off + the porter found me a taxi quick so I went directly to the Hotel Nap Bonaparte + checked in: Got the same room (114) as before! Had a nice breakfast, after which I phoned Maj. Easley who was glad to hear from me again - nice young chap. I got from him the phone no. of Capt Glenn, who had been at Arlington ~~then~~ with Earl + is now at Sig.

nal center with Col. Ray-  
 ford. He immediately asked  
 me to dinner that night & I  
 accepted. He was going to make  
 it an Arlington Hall Reunion  
 about which <sup>more</sup> later. - Was so  
 tired I decided to spend all  
 day in bed so went up to my  
 room & got into bed, coming  
 down to lunch at noon.  
 There I happened to sit at  
 same table with an interesting  
 looking civilian in Army uni-  
 form. After talking with him  
 discovering he is the world  
 famous Dr. Fritz Zwicky of  
 Palomar, Observatory &  
 Prof. of Astrophysics at Caltech.  
 We found a number of



friends in common, including  
Col. Stratton of Trinity College  
Cambridge. - We talked about  
Eddington, Jeans, Milne, etc &  
I had a most interesting time.  
He is going back to Washington  
too & I hope will be on same  
plane. - Sent telegram home  
& later was outraged at the  
cost, £950.50 francs, more than  
double what it should be, but  
so on account of depreciated  
franc. I later found I could  
have sent it for normal cost  
through PX + Army facilities.  
Went back to bed & really  
slept for 2-3 hours, but felt  
pretty punk when I got up  
anyhow. - Bathed, shaved,

dressed + got taxi to Hotel  
 Ambassador to keep my dinner  
 date with Capt Glenn. - On the  
 way downstairs to get taxi  
 whom should I encounter by  
 Col. Marcus! A fond reunion.  
 Riding a taxi in the evening  
 traffic in Paris is a hair-  
 raising experience. Here too  
 they drive like mad! It's  
 really awful. - Got to Hotel  
 Ambassador + there found  
 following, all ex "A-Hallites":  
 Maj. Guston, Capt Glenn, Capt  
 Wallace, Lieut. Wiedeman,  
 Lieut. Stewart - felt like  
 singing a college reunion  
 song. - Glenn had reserved  
 a nice table, the food was

good + he had wine + champagne. - We all had a very good time. Lt. Wiedemann was funny at one spot - he is on duty with Office of Foreign Liquidation Commission in Shanghai but is in Paris on temporary duty. When he reported in he was asked where he was born: London. Where his home is: Honolulu. Where he is stationed: Shanghai. What is he doing in Paris: Temp Duty. The next question: "Do you speak English?"!!! - We finished dinner too late to go to see any show so Lt Stewart rode us in his jeep to the Champs Elysees + we

walked a bit, then went to the Officers' Club + had a couple of drinks. It was then after 2300 + they all took me then to my hotel, where I hoped to have answers to my message to E - but no answer. Went to bed + had very funny dreams what with the mixture of food + drinks, but slept fairly well nevertheless.

24 Oct - Tuesday - Up at 0800 + had breakfast with Col Marcus. A long discussion re the black market + currency situation - which is most intriguing + according to him a great reflection on the mentality of the leading

basis in the Army. - You just can't blame the soldiers for losing the game by any way or means they can. Some Frenchmen high up are getting away with murder. - The official rate of exchange is 117.71 francs per dollar but you can get 280 francs by dealing with any one of the black marketeers who accost you on the street. - This was proved to my satisfaction this afternoon - as will be related. - After breakfast I went over to the Embassy to see Esley, get a VX card, etc. I spent three hours there, also seeing a gadget

The State Dept maintenance man (Hirsch) fixed up for automatic operation of CSP 2200 on incoming tapes. - Saw Elizabeth Dampson (formerly from AH) + called Earl about her desire to transfer to Frankfurt. - He told me a letter from E had come yesterday + he'd sent it back to U.S. damn! - I walked to + from the Embassy along the Champs Elysees & a wonderful experience on a nice day. - Back to hotel for lunch + sought out Dr. Ducky - luckily finding him at a table where I could

sit. - A most interesting talk about his forthcoming experiments on sending a rocket to the moon - a fascinating man. He says that the atomic scientists have been getting more credit than they really deserve - the larger share should go to the practical engineers & chemical engineers who reduced the theory to practice - Some scintillating remarks about Millikan at Coltech. - I'd love to study astro-physics next year I will! - After lunch a talk with Col Marcus & much kidding

in his usual style with  
the girls at the ATC counter  
but he gets away with it.  
- Walked again to the Embassy  
to get my memo for a PX  
card (I'm in need of cigars  
etc) + there found the dup-  
licate of Ed's letter I'd rec'd  
at Frankfurt, forwarded  
by Boris with a note to  
me. - I'd found out that  
I would not be leaving  
tonight so invited Easley  
+ Capt. ~~Stain~~ to Opera to see  
Mignon - Stewart already  
was booked to go but he is  
getting the tickets for me. -  
Walked back to hotel +  
ran into Col Marcus



again + he agreed to go with me to get PX card, then to PX. - At counter some more large kidding + I asked me if the men to give me scrip + francs for a \$20 traveler's check to save me journey to Finance Office - I got \$10 in scrip + 1200 Francs, the official rate. - Marcus + I then took a walk to Quenne d'Iena to get my PX card + on the way we were accosted by a black marketeer. Marcus asked what he'd give for \$10 + he got 2800 francs !! Just five minutes before I

got only 1200 francs for the  
same amount !! I felt  
very much put out + incensed  
+ I had a further discuss-  
ion about the inequity of  
the thing. - Got my PX  
card, then walked to  
PX, got cigarets, candy,  
soap, razor blades. Then  
back to hotel where I've  
been writing this ever since  
+ thank goodness am  
about caught up on my  
diary. - I forgot to say  
that Esbey was good  
enough to sell me a bottle  
of Schenley + I've had a  
drink out of it - At  
1945 I'm to be at Hotel

Crillon to meet Zarley +  
 Glenn for cocktails, then  
 dinner & then Opera Com-  
 que to see Mignon. - Boy  
 I'm tired now & must  
 rest a bit!

30 Oct - Wednesday - Up at 0700  
 as I felt slept out despite  
 getting only about 5 hours  
 sleep. - As for last night:  
 I got shaved & dressed +  
 was ready to leave at 1815,  
 and seeing that I'd walked  
 to & from the Embassy four  
 times already I wanted to  
 take a taxi but there were  
 none so I walked again.  
 Got to the Crillon (which  
 is right next door to the

Embassy at a little after the  
appointed 1845. Found my  
Easley there but not Capt.  
Glen, as latter had a  
date too. - Also, no tickets  
available for Mignon or any  
other place so we decided  
to take a chance on getting  
into the Folies at the last  
minute, via the ushers'  
black market route which  
Easley said he'd heard of.  
We had a nice cocktail.  
Saw & spoke to Mr. Thomp-  
son of AT&T (I'd seen him  
last in Gen. Fawcett's  
office a couple weeks ago.  
With him was Mr. DeWolf  
of State Dept. who re-

numbered me very well. I asked him how he'd enjoyed his visit in Moscow to which he countered by saying "I see your secret service is working as usual." There were a couple other State Dept people whom I didn't know. - Easley then took me to dinner at the Hotel Vuillamont, where Elizabeth & I stayed a night or two in 1933. - A very good dinner with excellent steak (thin but in fine French taste), chocolate ice cream for dessert. - Then tried to get taxi to Folies, but none available so went by

metro - faster & very much  
 better all round in my opin-  
 ion - at least you don't get  
 scared to death at the  
 crazy driving. - Well, we  
 got two tickets OK - via  
 the ushers' black market  
 route, for which I had  
 to pay a premium but  
 not bad. Orchestra seats  
 they were called but were in  
 1st balcony, right in the  
 middle & very good - at  
 253 fr each plus 50 fr for  
 usher fees  $2 = 606$  francs  
 or about \$5<sup>50</sup>, which isn't  
 at all bad. - The show  
 was marvellous; one set  
 + act (Chinese). I can

only describe as magnificent  
 + like nothing I had seen  
 before. - marvelous costumes  
 throughout. - I bought a  
 booklet (220 francs =  
 \$2<sup>00</sup> & hardly worth it  
 but something to show at  
 any rate in describing the  
 Folies to E). - A couple  
 of tiny cognacs between  
 the acts cost \$2<sup>00</sup> !! -

It was a long performance,  
 from 8<sup>30</sup> to 11<sup>45</sup> & when  
 we got out no taxis still  
 in sight so home by metro  
 & said my farewells to  
 Esley. I was back  
 in my room by a quarter  
 past midnight, quite

tired but feeling very well.  
 Got into bed but took me  
 some time to fall asleep,  
 for some reason or other but  
 I slept very soundly from  
 about 0100 to 0630 - up  
 + had a bath, dressed,  
 then to breakfast, with  
 Dr Zwicky & some more  
 discussion. Called A+  
 Compton the arch-traitor,  
 "with Almighty God in his right  
 pocket & Jesus Christ in his left pocket."  
 He was quite outspoken  
 against the big name  
 Scientists. Said they'd  
 deceived the rest of them  
 re the proposal to dump  
 A-bomb, which was



worked in such a way as to lead the rank & file to believe it was to be dropped on an uninhabited atoll.

Also, that AHC Compton & others had tried to circulate (did) a manifesto in 1940 asking scientists to refrain from working on armaments - at some time

Zwicky was trying to get together people to prepare against Nazi menace.

Then everything was turned upside down & now AHC et al are in forefront of the "preparedness crowd". Zwicky is violently opposed to any organized

organization for preventing  
 future disaster - believed  
 only in individual efforts  
 but I had to cut the  
 discussion short since he  
 had to leave. - Will no doubt  
 see him again. - Asked  
 about my priority status  
 + learned I was probably  
 going to leave today. Decided  
 I'd part by whatever gifts  
 I was going to get, this  
 morning. Got some

frances from hotel porter  
 (190 per scrip) + bought follow-

ing: Scarf for JR - 800<sup>3</sup> 666

Total: Guerlain for SF 2000<sup>1666</sup>

5428 = Pepsin Powder - 142<sup>120</sup>

8457 = Debong - 1005<sup>885</sup>

Schaparelli - 1481<sup>120</sup>

There were many beautiful clothing & apparel articles for women but you need not only oodles of money but also "points" as most articles of clothing are still rationed. But, you can buy the "points" - again black market dealings but not under cover. The poor people sell their "points" & the shop keepers will sell you the necessary "points". It's all fantastic. But I didn't want to hazard buying & wearing things this time - I'm not as brash as I was in my younger days. - Had lunch & confirmed that I'm probably going out tonight - still N-6 on the list but was told to report at 1630 again. - Phoned Easley & as it was a lovely day out

I suggested he take the afternoon off + go with me to Montmartre, which we did. - Walked a lot; the pain was then no longer out + it got cold up on top of the hill at Saere-Coeur. - We rode up the hill on the funicular or "incline" at 2 francs each. A wonderful view from on top but clouds + darkness obscured a lot. - Had a rest + a vermouth at a very small, spotlessly clean cafe - we the only customers. - Back to hotel by metro + I reported in at 1700 - notified to "stand by for a call" - might be any hour or not until morning - a lot of indecision as usual. - Took a rest.

(my feet very tired) had a small drink + then early dinner. - now in my room, practically all packed. I think Zwicky will be on same plane. I have invited him to have a drink with me after he finishes his packing. -

31 Oct - Thursday - I had a wonderful sleep - in fact, didn't hear the alarm + almost missed my breakfast as I woke suddenly at 0815. - Rushed dressing + missed a badly needed shave but got my breakfast - with Zwicky again, continuing our discussions of last night. He'll come to my room + for about three hours we talked - I

enjoyed it more than I have for  
a long, long time - talking science  
& philosophy with a kindred  
soul. - He told me that in his  
opinion Frederick Nansen, the  
explorer, was the greatest man  
of his times - and why, but it's  
too long to explain. I would love  
to have a recording of Turck's  
remarks after we had a couple  
of drinks. I like him tremend-  
ously & think him a great man.  
Got to bed at a bit before mid-  
night, & as said, had a good  
sleep, despite the very exhilar-  
ating conversation. ] - After break-  
fast I shaved & got dressed  
all over again, took a short  
walk as I'd been told

at about 1000 that I was to be on call all day + at very short notice, which meant that I'd probably be going out today. I walked over to Ave Klüber + stopped in the Signal Office to say hello to Col Raynesford - we had about 20 minutes chat + he seemed glad to see me. - Back to hotel + found Zwick all in a dither because his name wasn't on the list + I told him what I'd been told. I then verified it to him by taking him to talk to the "desk", which said my name appeared but not his. He rushed over to the Embassy to see what he could do toward getting a No. 1 priority.

Had lunch (Zuricky not around yet) & talked with a couple of young ATC men. Talked about how it was important to learn the cause of air crashes. One of them suggested that it should be arranged that the control tower could listen in on all the talk inside the pilot's cabin on take-off & landing. The other pointed out the practical difficulties in working out the communication system. I then suggested that an automatic record be made on magnetic tape in a fire proof container. They thought it a good idea & I may suggest it to some authority when I get back. — Saw Zuricky when



I'd about finished + went to  
join him. He still in a dither  
& having a hard time locating  
who had his N° 1 priority paper.  
We went to the "desk" + there  
for 1st time I saw the "secret  
list" - with my name on it, but  
still no Zircky on it. - And also  
the name Kohler. I had made  
pretty good friends with the gal  
at the desk so I asked her to  
find out the full name of this  
Kohler, suspecting it might  
be our own Dr. Hans Kohler  
of Arlington Hall, who'd left  
in July to see his old parents  
in Switzerland. - And sure  
enough it was he, so I got  
his phone no. at the hotel

where he was staying, called him up, asked him to come over (not far away) and was he pleased and happy to see me. He's been in Paris two weeks - waiting a priority to come for air to desport back - he couldn't get a ship passage back at all until next spring. - Took him up to my room where he appreciated the heat (no heat in his hotel!) + we talked a couple of hours. - Zurich + Kobler both being Swiss I thought it would be nice to get them together so after a bit I went to look for Z - found him downstairs

and out of his dither - after long + arduous planning to Frankfurt + other places he'd just got his priority business straightened out. - I invited him up to my room + introduced the two. We sat around discussing science + scientists. Z a man of very positive + very outspoken views on persons + things. - High admiration for some people like Einstein + quite devastating about certain others such as Millikan + A.H. Compton, Debye (now at Cornell). - I went downstairs then to see if I could talk the Mess Office into letting me have Dr Kollman as my

guest at dinner. He gave me a long song + dance about how + why it wasn't possible but I persuaded him in the end + so the three of us had dinner together, we continuing our discussions. - Z has just about finished a book to be published in English under the simple title "Truth" + in German under a slightly different one. I got him started on telling us what it's about + he outlined it - a new approach to the basic problem of knowledge + what is "truth" - very fascinating + I think will make a great impress on the world's philosophy. - We talked on

until about 2200. - I saw D.K.  
to the hotel door (handing him  
one of my two suits of long  
underwear & he most grateful  
for everything.) [K's wife is  
Prof of French at MIT Vernon  
Samuway & must be quite a  
person - we must get together  
soon.] - I then to my room,  
took a bath & have been catch-  
ing up on my diary. - We were  
~~told~~ we might be called at  
0100 so I ought to catch some  
sleep. I am also told that  
what is holding us up now  
is "weather". Maybe I'll get  
off tomorrow - I hope!

1 Nov - Friday - Up at 0800, shaved,  
had breakfast. - no further news

\* I decided it was time to do something about getting my priority raised as it became clear that as soon as the weather cleared there might be a number of priority 2 + 1 passengers show up. So I went over to Signal Center to call Cook + through Glenn got a line through at once but Cook was out so I talked with Hissar who said he'd take it up with Cook. I then went through the Signal Center with Glenn + saw the "Blockhouse" from bottom to top. The Germans built it in 1940-41 as a Signal Center - four stories high, concrete walls 10 feet thick + roof of concrete, no windows + air conditioned. Back to hotel + in a few minutes news came of a brand new list! Dr.

Zwirsky's name on it but not mine which confirmed my worst fears. So I decided to rush over to see if Col. Raynesford couldn't do something for me. We called Hirsch again & he said they couldn't do anything there - for me - I'd have to see Ed Warner of AG here. - So I rushed back to the hotel to be confronted with the news that they had been looking for me - two people on the list with Zwirsky couldn't be located so they were going to put me on! But it was too late, the bus had left, the manifest closed. - Next best thing - wait around, I'd surely go out this afternoon.

and probably at 1500. I got myself all packed or nearly so, in the midst of which Jessie Dent called from downstairs + said she'd come to see me off. I finished packing + went down to see her + Lt Snow from Tank-fort, both here on leave. - By 1450 still no certainty but 1455 came word to get on the 1500 bus. - So I got my stuff down, no bus but a 6x6 weapons carrier. Jessie took my picture on board the awful looking truck + we said good bye. - I'd arranged by phone already with Capt. ~~Stann~~ + also with Maj. Easley to send word back



to Cork & Washington respectively that I'd left Paris at 1500. - Not too bad or cold a ride to Cork. - I get there, check in & am told I'm on Flight F-8, to Azores. I then go into waiting room - there's Zurichky still waiting, with chute harness on & ready to go, but waiting. The weather very foul. - Pretty soon I get out to desk to check in things & am told I was transferred to Flight E-2, the same one Zurichky's on, for reasons too complicated to enumerate here. But E-2 goes to Iceland, F-8 to Azores. However, it would be nice to be with Zurichky.

We sat down in VIP lounge & had a sandwich. Pretty soon I go out to check again - to find that E-2 was cancelled, bad weather! Don't understand how such things can happen! We had to get our things & go back to Hotel Nap again - & maybe not be able to get in there again. - Rushed to get the bus & just made it. Back to hotel & I was very lucky to get my room back after rushing up to the place & finding it hadn't yet been assigned. - Then came down & argued with the clerk. Poor Zurich though had to go up to 7th floor & no

elevator - they never work here.  
 So he has 7 flights to walk  
 [and no toilet on <sup>the</sup> floor!]  
 up & down. - I immediately  
 phoned people: Jessie to get  
 word to Glenn to get word  
 to Cook to cancel usage  
 saying I'd left, to ~~St~~  
 Stewart to cancel usage to  
 G-2 saying I'd left Paris;  
 to Dr. Koller to see what  
 his situation is & tell him  
 mine. - Have had dinner &  
 now am waiting for further  
 word. What a mess! Jessie  
 & Glenn asked to me join  
 them but I decided best to  
 stick close to hotel. Don't  
 dare leave. Jessie is coming  
 over to see me in a.m. if

Jim still here + if so, get the  
ATC here to do something to  
change my priority in writing.  
- It's now 22:30 + Jim in bed. No  
news, no change in situation. - I  
phoned Kohler + he came over. He  
Zurich, + I spent evening together.  
One of Z's former students named  
Hayes, here attending Karmen's  
lectures, gave us the last of his  
schnapps from Switzerland - each  
having an ounce. - I hope the  
weather clears in Iceland tonight  
so that we can get off tomorrow.  
2 Nov - Saturday - Up at 0740, showered,  
bathed, down to breakfast at 0815 with  
Z, after which we both went to see  
Major Skillin, who seems to be direct  
or of traffic for ATC. Z + I wanted

to get the straight dope on what the regulations really are as we both suspected some skullduggery at Oly in the handling of the priorities. One ship, maybe two, did go out yesterday - to Agnos - with some #3 passengers and since Z had a #2 priority he should have replaced one of those #3's. Also, I thought there were some #4's on that too +

I was first scheduled to be on that plane + got bumped off! At any rate I also wanted to see if May Skillin couldn't do something re raising my priority. He listened very carefully + I showed him the WJ telegram. He immediately said I should have had a #2 from the very beginning + why did

I wait so long in flashing the tel around - it was quite poetic. So he immediately began the motions toward raising my priority & gave Bolann assurance it would be done. He also bawled out the people at Coby for their manipulation of the priorities there & excused them (to us) by saying they were new, didn't understand & were lazy bitches - because it meant a lot of work in changing things around. Well, we went back to our hotel with the ~~best~~ assurance from him that we'd leave today on the E2 flight to Ireland at 1300. - We felt pretty much relieved as a result of our visit & I finished up.

my packing. Jessie Dent phoned  
+ I told her latest word. She will  
check this p.m. + if I'm gone will  
get word to Cook. I forgot then  
to call Lt Stewart at Embassy  
to tell him latest word but I think  
he will get it anyhow + will send  
word to Wash. - I also phoned  
Dr Kohler + told him whom to see  
+ to keep after people at ATC.  
The organization is pretty much  
disorganized. - We got the  
1100 bus to Orly, checked in etc  
and took off not at 1200 but at  
1345, which wasn't bad. I'm  
writing this now at 1430 - were  
over water now I think but can't  
be sure as we are in clouds. We  
are supposed to fly at 6500'

The plane is comfortable & clean  
I think we'll have a nice trip. It  
is scheduled to land at Waco on  
Sunday noon or afternoon & from  
there I have to try to hop a ride to  
Washington on a local flight. -  
The weather yesterday was foul but  
today it is quite good & the flight  
I had far very smooth. - One item  
of interest: just a few minutes  
before we were to board the plane  
one passenger suddenly realized  
that he'd left \$1500 in cash under  
his pillow at the Hotel Nap! He  
rushed out just in time to catch  
the bus back. We left without  
him (a Sargeant) & I hope the  
poor fellow finds his money. We  
have an extra seat in the



plane. - Well, we arrived at  
Meeks Fld, Iceland in 6 1/2 hrs  
flying time instead of 7 1/2 because  
we had a good tail wind. The  
trip was pretty smooth all the  
way. - Had supper of ham &  
egg at terminal. We were told  
we'd have to stay overnight here  
because there is no relief crew  
to take our ship out. It's one  
delay after another! So we got  
bills and after sitting around  
talking about 2 hours (I being  
surrounded by a group goggle  
eyed by his explanation of jet  
propulsion etc, a most interest-  
ing talker) we went to beds  
in a barracks-like affair  
constructed inside a

Overcast but the wind is terrific here but it is not cold. It rains all the time. -

3 Nov - Sunday - Up at 0700 local time. Slaved, dressed, trucked to terminal, breakfast of ham + eggs. - Got aboard plane, taxied down the field, monkeyed-around - and then came back! Engine trouble. In the terminal, whom should I see but Dr Kohler. A warm reunion. He'd just gotten in + his plane due to go out in an hour. I'll probably get to Washington before he do! Maybe we'll have to wait over in Goose Bay another night. - Talking about

disorganization - somebody failed to close & fasten the door to our plane last night. As a consequence the two rear seats (one mine) were drenching wet. Luckily I had another seat, first one forward, so could get that one & not be wet. - The weather is nasty out, heavy wind & rain. After about 1 hour, we went aboard again, tested the engines out - still trouble and this time we were told they'd have to take the plane inside the hangar - too rainy and windy to work on it outdoors. So back we went in the wind & rain, with our bags, to the terminal, prepared to stay at least

four hours, we were told. - Sat around for a 1/2 hour + then were told a bus would take us to the Hotel De Gink where we stayed last night. Soon the bus came + just as we were about to get on, word came that the trouble was fixed! - So again we board the plane + this time we take off - at some local time, in what looks like very soupy weather. Pretty soon we are through it + now the run is bright + the air smooth. - When we got aboard, the heat was on - full blast + almost unbearable, so the engineer had to turn it all off + now it is freezing inside. He is working on it + I hope he gets it fixed soon. - I forgot to

mention one funny thing that happened to me on the landing last night. We had put on our Mae Wests, had our belts all fastened & were coming down fast. Just as we were about to land, somehow the left-hand cartridge on my Mae West went off (I couldn't fasten the safety cord when I put it on, the string was too short, the flight clerk said when I showed it to him) & in an instant my Mae West was fully inflated after a brief explosive hiss which of course took me quite by surprise. - No harm done though & I simply opened the release

valve & deflated the thing.  
 Will have to watch that  
 again. - how were about eight  
 or ten hours behind our schedule  
 & I hope we won't have to  
 lay over again at Goose Bay  
 for any cause. - Hooray, the  
 heat is on <sup>seven hours later!</sup> again! - It's  
 now about 1430 Eastern Stand-  
 ard Time & we are due at Goose  
 Bay in about 30 minutes, how  
 over Labrador and does it  
 look rugged! And desolate!  
 A thin layer of snow over the  
 tundra & ice on the thousands  
 of tiny lakes & streams. - We are  
 beginning to come down now, my  
 ears tell me. - It has been a  
 very calm journey thus far.

- The ice on the lakes is not very thick & shows many cracks. Where the snow has stayed on the ice & where it has either melted or the ice underneath has gone there are myriads of curious, lacy & delicate designs. - The afternoon only marred a little bit by my recurrent hives! They served us a lot of fish in various forms in Paris. I can't think of anything else that would bring them back; - A good deal more snow as we go further south. - Boy, I'd hate to have to land down there now in that rugged mess. - We arrived at 10<sup>00</sup> local time

after a flight of 8 hours + 10 minutes. We were met by a nice clean bus + taken to the Hotel De Fink to stay overnight! Bad weather at Westover Field, the only one the Army will allow ATC planes to use, so despite the hundreds of possible fields we might use, with Westover closed in, we are stuck for the night again, and again we suffer at least a 12 hour delay. - Kohler gone, so he will get home a day before I do! What irony. - Checked in, got a room with Zurich + a Persian colonel who is M.A. in Washington. - We cleaned up a bit and Z + I had another long talk, this time about German developments in research before V-E day. I learned



a most amazing thing. They had not one but three different ways - all completed months before the dud - by means of which they could have exploded any aircraft within an <sup>area described by the</sup> inverted saucer with a base 30 miles in diameter + fifty thousand feet high. - Why didn't they use it? Here Z became quite eloquent + vehement + gave what in his opinion is the reason why a democracy of free men will always beat a dictatorship: fear of the consequences of possible failure. The German scientists were afraid of their lives if the theoretical + experimental devices didn't work out in

practice as promised. They would have to guarantee the success of the project - the fear of failure being to forfeit their lives. That was the principal reason why all three separate groups of German scientists withheld their discovery from the Nazis. A secondary reason was that many of these men weren't too sympathetic to the Nazis and weren't too anxious for them to win. And a tertiary reason was that these men couldn't get the support of the big-name German scientists like Heisenberg + Hahn, who in favor for their own necks would be reluctant to go out

a bomb + gave only lukewarm endorsement. All that Z told me is not hearsay - he talked to the man + saw the gadget himself. He told me how absolutely amazed he was at the simplicity of the basic theory + how much more he was amazed when the Germans told him of them + why they didn't actually use them. Z says they tested one of these devices 35 times + shot down 35 planes, 100% success on experimental basis. Z wrote the business up in an RAF paper which I will get on my return home. - We talked a lot - for two or three hours. About Henschel + his shells.

treatment by the British & how  
as a result of his wife & six  
children almost died & what  
Z did to get them strangled  
out. - Of how Z conducted  
the interrogations & "homework"  
of the 400 German scientists  
who had been crissled at Garm-  
isch-Partenkirchen, how the  
authorities let them practically  
starve until Z raised hell to  
get food from the Army for them  
& how Z got in bad by being  
a rather severe taskmaster  
in getting work out of these  
Germans. The British tried to  
get an official reprimand for  
Z - but it wound up in the  
end that the Germans all

wanted to work for Z in America + didn't want to do anything for the British. I imagine that Z is a severe, hard taskmaster but a most fair + just man without an ounce of insincerity or hypocrisy in his makeup. - When I changed shirts he made some comment that I seemed to carry everything with me. I offered to let him have one too, but doubted that my size would fit him - he's an enormous man. He laughed + told me a story about <sup>his diff. sizes in</sup> getting some shirts, size 17, + how the lady who had volunteered to obtain them brought him size 16, saying that

Oct 26-

Fr Francs 3183.00

Scrap \$ 50.60

US \$ \$ 10.00

Travel Checks \$200.00

Came home with :

\$ 34.15

Travel Cks 160.00

\$194.15

Fr Francs 139.

at the shop she visited, when she asked for 17's she was asked for whom they were. She said, for a professor. The salesman then assured her it just couldn't be so as only prizefighters and wrestlers wore 17 - it was impossible that a college prof could have a size 17 neck!

Whereupon I told him of Max's story about the man with the ringing in his ears, headaches, & pain in the neck. I laughed & laughed, thinking it a swell story. - We talked about Van-nessen, Bush & Conant & Crompton & others. of Shapley and Norris Russell, et al. - I enjoy him immensely & find so many things

in common with him, I wish he lived in Washington. I have long yearned for a male companion whom I could count as a real friend. There have been very few in my life and I've missed them consciously. Z's stock of technical information + knowledge is enormous + I could learn + learn just talking with him. Well, we went in for dinner at 1830 + lo! There was a very nice bar + dining room. So I ordered cocktails (two rounds) for us, excellent drinks at only 3¢ each. Then a very nice dinner with copious food + well cooked, everything nice + hot. - After dinner, more talk



+ then a walk in the crisp snow - not cold out, it seemed because the atmosphere is so dry. A fine  $\frac{1}{4}$  moon with an enormous halo - a lovely quiet night. - About seven or eight ATC planes all lined up & grounded because of bad weather elsewhere. - We turned in at 2200 but I didn't sleep too well. Forgot to say I took a nice shower - the first one since leaving home - & enjoyed that immensely. When I came back into our room with my bathing cap on, Z exclaimed "Why the man has everything!"

4 November - Monday - Up at about 0630, much noise during

The night of people coming  
 and going so I didn't sleep  
 too well. Shaved, dressed,  
 breakfast of ham + eggs. The  
 news of departure not good -  
 it seems we won't get off  
 until mid-afternoon. - 2 + I  
 walked a good deal, I sent a  
 Telegram to E + cashed a trav-  
 eler's check. - Fine, crisp,  
 sunny + clear day out. -  
 (Aboard the plane now) - We had  
 a leisurely lunch after vague  
 rumors we'd be leaving sometime  
 this afternoon. We'd just about  
 finished eating when all of a sudden  
 we got word we were taking  
 off in few minutes! - Got our  
 things together, paid our bill  
 for the billet (25¢) which seemed

quite out of line with the \$15<sup>00</sup>  
dinner last night) + went to the  
passenger terminal. There I talk-  
ed with the officer in charge +  
requested he wire Westover field  
to hold the shuttle plane to  
Washington if necessary. He agreed  
to do so after I received support  
from the Persian colonel + one  
other passenger. We took off  
at 1410 local time = 1310 EST +  
are scheduled to arrive after 4 1/2  
hours. Weather calm but we  
are flying in cloudy haze all  
the time. Hope the field is clear.  
One of the things Z + I talked  
about yesterday I failed to  
record: the way in which Swiss  
technicians working inside  
Germany on some of the most

secret German projects got their information into American + Swiss hands. It was all done by individual Swiss working alone, without cognizance of Swiss Govt. One of the important items of information they got out was notice of impending invasion of Switzerland, twice in 1940 and once in 1943. The Swiss Govt mobilized 1,000,000 men + the Germans had to cancel their plans. Z says this is recorded in last official report of Swiss Army's Chief of Staff. - Z said that he + good many associates of the Swiss scientists in U.S. got continuously the latest info re German scientific progress for the Swiss in Germany - at the risk of their lives.

- Arrived at Westover at 1835, the ride quite calm except for a few minutes now & then. We rode just over very heavy banks of very dark clouds a good part of the way. - On arrival we cleared through customs ZIP! just like that, as I think some notice of VIP arrivals (maybe me?) must have been given because the OD came aboard & pretty soon I and the Persian Colonel were escorted to a nice shiny car & taken to the terminal. This enabled me to clear customs & immigration.

the first. - Then I sought information re a plane to Washington but things are quite SNAFU in that respect, the OD told me. The regular 1800 shuttle plane was cancelled + a special C-54 is now on the runway - but it developed a leak in the gas line + that must be fixed before it can take off. It is estimated now to be ready at 2100 but I'd go with my fingers crossed. May have to go by train. - Now 2145 + I'm aboard a C-54 Cargo plane bound for Bermuda, one stop in Wash-

ington, due there about  
2330. It's rough + a couple  
of the passengers are sick. I  
feel OK so far. - I phoned  
E from Westover + awfully  
glad to hear her voice. Told  
her the situation + not to  
come to airport. - Soon we are  
over New York City - a wonderful  
sight. In 20 minutes more, over  
Philadelphia. We are going about  
3 miles a minute apparently. -  
Now over Baltimore, the going  
is much smoother. - We are  
due at Washington at 2330. -  
Now I can see Washington, a  
very lovely sight below. Sky  
perfectly clear. - Down we  
go now. We have our harness

on - we had to put that on  
when taking off also. -

Arrived - 23~~25~~<sup>25</sup>, a few minutes  
ahead of time. - It's good to  
be back + will phone to at  
once.



Office of the Chief of the Air Corps,  
 Washington

Memorandum for:

Mr. Friedman: →

Series #  
 300,212 deals  
 with M-138 and  
 in view of recent  
 happenings it seems  
 desirable to reclassify  
 this patent —

70,412 and <sup>134C</sup>  
 443,320 <sup>228</sup>

Small 382,561  
 W33 682,096  
 W33 107,244

Declassified  
 and approved  
 for release  
 by NSA on  
 08-06-2014  
 pursuant to  
 E.O. 13526

Hall is returning Rosen's  
 application - *BR*

CHAS. A. ROWE  
 Patents Section S. C.  
 Room 3143 Branch 1313

Goes to checks

Drawings go to Commercial  
Company for reproduction

Drawings go to Richmond on truck  
unattended (daily trips)

REPORT TO COLONEL LIPPINCOTT

Mr. Polton, Mr. Hall and the writer went to the Patent Office in Richmond on December 9, 1942. The purpose of the trip was to learn, first-hand, the manner in which secret applications were handled by the Patent Office and to determine both the procedures and the facilities for observing secrecy.

In Divisions 21, 16, 40, 53 and 55, it was found that secret applications were kept in the drawer of a steel desk belonging to the Chief of the Division in each case, and locked therein, the Chief of Division usually keeping the key. In Divisions 16 and 53 are kept some of the highly secret cryptograph applications of the Signal Corps. We were informed that in Division 16 these cases were given to the messengers for the purpose of carrying to other parts of the building to obtain photostats and to be delivered to other examiners. It is further understood that these messengers have not been cleared for secrecy. The status of examiners and others in this regard is not known. In Division 56, the cases are kept in a locked standard file. In Division 36, they are kept in an old standard file, which is provided with a lock. In Division 61, there is a key-locked file which most nearly approaches our combination file cabinets. The key for this cabinet was kept in the desk of the Assistant Chief Examiner of that Division.

Mr. Polton, under direction of Mr. Hall and with an order signed by Mr. Hall, proceeded to the photostat room and introduced himself as an employee of the Signal Corps, with no other identification, and personally being unknown to the members of the photostat room. He handed the order to the Chief of the Division, said order calling for a photostatic copy of each sheet of the drawing of an application filed by the Signal Corps, and asked if the photostat could be furnished that afternoon. The answer being in the affirmative, Mr. Polton returned at the appointed hour and was handed the photostats. No further identification

~~SECRET~~

was requested.

Each Division has a docket-book, which includes the Serial Number, filing date, name of the inventor, title of the application, the status thereof, and name of the examiner to whom it is charged. These books are kept on the desk of the clerk of the Division and are not in the safe. While these books are watched during the day, it would be readily possible for a foreign agent to examine these books and ascertain the Serial Number and filing date of several Signal Corps applications, provided they knew the name of the inventor or some other information, and thereby get the data with which to place an order similar to that given to the photostat room by Mr. Pelton.

When an application is filed, it is not put in a locked cabinet of any type, even though the case may be secret, until the examiner receives information that the case is secret. Before that time, the cases are kept in racks along the side of the wall and the drawings are kept in <sup>UN-</sup>locked file cabinets, accessible to any person who might break in after hours. WST

The security of the portion of the Patent Office in Washington has been under constant observation for some time by Mr. Hall and Mr. Pelton. This investigation has revealed the locked file cabinets in the War Division are not of approved construction, they being key-locked file cabinets. Mr. Welsh keeps the keys in the drawer of his steel desk. It may be added that Mr. Welsh's desk appears to be habitually locked, even throughout the day except when actual use requires it be temporarily unlocked.

Applications filed in the Patent Office include drawings. These drawings are sent to a commercial photostatic company in Washington for photostating. The applications are processed through the Patent Office in regular course of business similar to unclassified or perhaps "restricted" papers of the War Department.

Trucks transport the cases from Richmond to Washington and back. These trucks

~~SECRET~~


~~SECRET~~

Report to Col. Lippincott (cont'd)

are not provided with an armed guard and generally have a negro truck driver. The present conditions of the trucks raise the possibility of serious breakdown which might endanger the security of the documents contained. The two trucks meet at Fredricksberg, where the drivers exchange trucks. It is suspected, on the basis of remarks made, that the drivers in exchanging pleasantries, possibly stop in for sandwiches, etc., leaving the trucks unguarded.

---

N. N. Moore  
Captain, Signal Corps

  
William D. Hall  
Patent Advisor

---

R. G. Pelton  
Patent Advisor

~~SECRET~~

PAPERS

1. A means of providing an irregular wheel movement in cipher machine using cipher wheels
  1. Carbon copy of final
  2. Original of draft
  3. Carbon copy of draft with hand written corrections
  4. Early draft with photostat
  5. Hand written draft
2. Instruction sheet and blank for patent application
3. Report on M-228 (to Col. Corderman) carbon copy
4. Draft "Replacement of the Present Combined Cipher Machine"  
Carbon copy of staff study
5. Report to Col. Lippincott on visit to Patent Office in Richmond
6. Contribution of the Signal Corps. Carbon copy of pertinent passage from Naval history.
7. Excerpt from Drew Pearson on the Yalta Agreement
8. Informal memorandum on faults of cryptographic machine

CORRESPONDENCE

1. Letter dated May 16, 1935, subject: Blank forms for code accounting
2. Letter dated August 31, 1935 on principles of Converter Type M-134-T2.
3. Photostat of document dated June 26, 1935 on device to be attached to the electrical counting sorter, signed by Friedman and Rowlett
4. Photostat of memorandum dated July 6, 1935, forwarding draft of specifications upon which application for patent on Cipher Device Type M-138 may be based.
5. Photostat of Routing and Work sheet regarding evaluation of patent.
6. Copy of letter from Friedman and Rowlett setting forth the principles of M-134-T2, dated February 15, 1936.
7. Copy of letter dated 27 September 1945, subject: Release of Patent Application Serial No. 443,320.
8. Copy of memorandum dated 15 January 1946, subject: Release of cryptological inventions and developments.

9. Memorandum from AC of S, G-2, dated 29 April 1946, subject: Release of Cryptographic principles
10. Letter dated 20 May 1946, subject: Release of Patent Application Serial No. 443,320.
11. Memorandum dated 10 April 1947 on Procedure for release of information concerning secrecy patents.
12. Draft of indorsement on patent release of 443,320.
13. Comments on Patent Application No. 443,320, dated 29 December 1947.
14. Memorandum for record dated 25 September 1947 on Meeting with Captain Safford and engineers of Teletype Corporation.
15. Memo dated 20 September 1949, subject: Replacement of the CCM.

PAPERS

1. A means of providing an irregular wheel movement in cipher machine using cipher wheels
  1. Carbon copy of final
  2. Original of draft
  3. Carbon copy of draft with hand written corrections
  4. Early draft with photostat
  5. Hand written draft
2. Instruction sheet and blank for patent application
3. Report on M-228 (to Col. Corderman) carbon copy
4. Draft "Replacement of the Present Combined Cipher Machine"  
Carbon copy of staff study
5. Report to Col. Lippincott on visit to Patent Office in Richmond
6. Contribution of the Signal Corps. Carbon copy of pertinent passage from Naval history.
7. Excerpt from Drew Pearson on the Yalta Agreement
8. Informal memorandum on faults of cryptographic machine

CORRESPONDENCE

1. Letter dated May 16, 1935, subject: Blank forms for code accounting
2. Letter dated August 31, 1935 on principles of Converter Type M-134-T2.
3. Photostat of document dated June 26, 1935 on device to be attached to the electrical counting sorter, signed by Friedman and Rowlett
4. Photostat of memorandum dated July 6, 1935, forwarding draft of specifications upon which application for patent on Cipher Device Type M-138 may be based.
5. Photostat of Routing and Work sheet regarding evaluation of patent.
6. Copy of letter from Friedman and Rowlett setting forth the principles of M-134-T2, dated February 15, 1936.
7. Copy of letter dated 27 September 1945, subject: Release of Patent Application Serial No. 443,320.
8. Copy of memorandum dated 15 January 1946, subject: Release of cryptological inventions and developments.



9. Memorandum from AC of S, G-2, dated 29 April 1946, subject: Release of Cryptographic principles
10. Letter dated 20 May 1946, subject: Release of Patent Application Serial No. 443,320.
11. Memorandum dated 10 April 1947 on Procedure for release of information concerning secrecy patents.
12. Draft of indorsement on patent release of 443,320.
13. Comments on Patent Application No. 443,320, dated 29 December 1947.
14. Memorandum for record dated 25 September 1947 on Meeting with Captain Safford and engineers of Teletype Corporation.
15. Memo dated 20 September 1949, subject: Replacement of the CCM.

*Safford*  
✓

The Contribution of the Signal Corps

15. Mr. Friedman and interested officers at Signal Corps Headquarters were familiar with the various models of the HCM, but not with the prospective changes which the Navy had concealed from Hebern. In fact, the Signal Corps purchased two of Hebern's nonprinting models in 1924. At the request of the Navy Department, Friedman undertook solutions of the HCM in 1923 and again in 1932, being furnished the machine, code wheels, instructions, and test cryptograms in both instances. Friedman was successful both times, and developed a method of solution whereby, under certain conditions of meter action, solution could be achieved without possession of the code wheels. As the Navy Department did not intend to use a meter action in the stepping of its service models, these solutions did not worry us particularly. However, the techniques and experience gained in these solutions paid big dividends later on, as they were instrumental in the solution of certain systems which cannot be named. These solutions were published in SECRET status by the Signal Corps in 1935, as

Analysis of a Mechanico-Electrical Cryptograph - Part I  
Analysis of a Mechanico-Electrical Cryptograph - Part II

The Navy Department was not consulted in the matter, although furnished copies of these pamphlets after printing. This caused bad feeling on both sides which lasted for several months and led to an order from the D.N.C. that the Signal Corps was not to be shown the ECM (Mark I) or to learn any of its details. This order was not revoked until January 1940, when Signal Corps representatives were invited by Admiral Noyes to inspect the Mark II ECM.

16. Late in 1935, or early in 1936, Friedman disclosed to Commander Wenger, of Naval Communications, his invention of an electric stepping control for the electric cipher machine, and three different methods for accomplishing this electric control. These are all covered in Secret Patent Application #70412, dated 23 March 1936, in the name of W.F. Friedman and F.B. Rowlett. An experimental model of an electric cipher machine using one of the Friedman-Rowlett electric control methods was built by the Signal Corps at Fort Monmouth, New Jersey, about this time and shown to me after its completion. About 25 or 30 of these machines were made in small lots up to 1939 or 1940 and used for special types of communication, such as Military Attaches and Commanding Generals. These Army machines indicated the reliability of electric control but the undesirability of the particular method used in the Signal Corps machine.

17. Friedman and Rowlett assigned the entire rights to their three inventions to the U.S. Government (Secretary of War). The Navy took another of the Friedman-Rowlett control methods (the "Stepping Maze"), experimented with it, and further developed it.

This was done without their knowledge until the day that the Mark I and Mark II ECMs were disclosed to the Signal Corps. On that occasion (3 February 1940), I acknowledged to Mr. Friedman, in the presence of General Mauborgne and Admiral Noyes, our use of his invention. The Navy also considered the third Friedman-Rowlett control method (the stepping circuits through the "Alphabet Maze") with the idea of conserving space, but abandoned it as unreliable and impracticable on the recommendation of the Teletype Corporation. At the suggestion of the Signal Corps, a last-minute change was made in the stepping of the code wheels in the "Stepping Maze".

18. Electric control of the ECM by means of the Friedman-Rowlett "Stepping Maze" is the essential feature that places the Mark II ECM in a class by itself as regards security. Those who have participated in the development of the Mark II ECM have always acknowledged these contributions of the Signal Corps. The "Index Maze" adds to the security afforded by the "Stepping Maze," but it is worthless without it. The importance of electric control can best be estimated by a consideration of what the Mark II ECM would have been if Friedman had not disclosed his invention to the Navy. Although the "Stepping Maze" appears obvious, now that it is in use, no one in the Navy thought of it in a period of 15 years, and no foreign machine employs it. Therefore, the Navy would have continued the development of the older methods and the new ECM would have used the mechanical stepping control found in CSP 903 or CSP 1700. We would have had a secure machine, superior to anything in use by foreign nations, but definitely inferior to our present ECM. This hypothetical machine (as well as CSP 1700) would defy attempts at solution until such time as machine and code wheels were captured. After this, each day's keys would resist solution for a long time. "Short-cut" solutions would be impossible, due to the erratic stepping of the code wheels, but a trial and error solution would be within the range of possibility. We could not make the flat statement, as we do for the Mark II ECM, that solution would be utterly impossible. In other words, the machine would be adequate to take us through World War II but, because we had stopped short of perfection, there would always be the desire to develop a new machine with electrical control. Friedman and Rowlett are entitled to full credit for their invention of electric control and the "Stepping Maze," which add so much to the excellence of the Mark II ECM.

19. The Signal Corps' willingness to accept the Navy ECM for their own use as well as joint Army-Navy use, and to drop the development of their own machine, reflects credit on all who made that decision. The joint Army-Navy ECM Cipher became effective

~~CONFIDENTIAL~~

in July 1941, and the two services had a common high-security cipher system in effect and in use prior to the attack on Pearl Harbor. This use by the two services of an identical machine with interchangeable code wheels has been of great military value, particularly in the early stages of the war when the distribution of machines and code wheels was incomplete. In the Philippines, Java, Australia, and even in North Africa, Navy wheels have been used in Army ECMs, Army wheels in Navy ECMs, machines borrowed back and forth between the two services, Army messages sent in Navy ECM ciphers and Navy messages sent in Army ECM ciphers. One other contribution from the Signal Corps came in 1943, after the ECM was in service; namely, the "Plugboard Code Wheel." This was developed by the Army for field use, where the danger of capture was greater than in the Navy. The "Plugboard Code Wheel" was adopted for joint Army-Navy use, at the request of the Army, and later distributed to all Navy holders of the ECM. The chief value of the "Plugboard Code Wheel" is possibly psychological, but we do have it in case of need.

~~CONFIDENTIAL~~

~~SECRET~~

Exhibit 4. This is the final version that Capt. Safford put in the record and which he sent me without comment. F.

### The Contribution of the Signal Corps

23. Mr. William F. Friedman, Principal Cryptanalyst of the Signal Intelligence Service, and interested officers at Signal Corps Headquarters were familiar with the various models of the HCM, but not with the prospective changes which the Navy had concealed from Hebern. In fact, on Mr. Friedman's recommendation, the Signal Corps purchased two of Hebern's early 5-wheel nonprinting models late in 1923. At the request of the Navy Department, Friedman undertook a cryptanalytic test of the HCM in the spring of 1924, being furnished a set of 10 test cryptograms prepared by the Code and Signal Section. Friedman was successful, and developed cryptanalytic techniques whereby, under certain conditions of meter action, solution could be achieved even without possession of the code wheels. Again at the request of the Navy Department, in April 1932 Friedman undertook a second test on the much improved 1930 model of the HCM. This time he was furnished the machine, a description of the general system employed in setting up the message indicators, and a series of test messages. Again he was successful, with the aid of three or four of his assistants. As the test messages were enciphered with Hebern's stepping action and not with the irregular code-wheel stepping produced by the HCM adapter (CSP 535), the solution did not worry us particularly. These solutions were very important, in three ways, namely:-

- I. They showed the weakness of the meter action of the 1923 HCM and of 6 of the 30 optional stepping actions of the 1930 HCM.
- II. The 1924 solution was the basis of further analysis by the Navy which disclosed stepping actions that would block analytical solutions or short-cut solutions based on possession of the code wheels. Friedman arrived at similar conclusions, independently. Otherwise, we would have had to abandon the Electric Cipher Machine as being deficient in inherent security.
- III. In recent years, the principles and techniques of these solutions were instrumental in the solution of certain systems which are still using a meter action.

24. The first solution (that of 1924) was written up by Friedman in secret, typewritten, technical paper completed early in 1924, which was not printed, however, until 1934, under the title "Analysis of a Mechanico-Electrical Cryptograph--Part I." The second solution (that of 1932) was also written up by him in a second secret paper completed in 1933 but not printed until 1935, under the title "Analysis of a Mechanico-Electrical Cryptograph--Part II." Both papers were very carefully safeguarded at all times and were employed only in the SIS for the advanced training

~~SECRET~~

~~SECRET~~

of a very limited number of students. The documents were given no dissemination except that the Navy Department was furnished copies. But, because it was not consulted with regard to the advisability of printing these papers, combined with a serious mistrust of the Government Printing Office, The Navy Department entertained some apprehensions as to security and this led to an order from the D.N.C. that the Signal Corps was not to be shown the Mark I ECM or to learn any of its details. This order, which was not revoked until January 1940, was responsible for later misunderstandings. Certain Signal Corps representatives, including Friedman and Mr. Frank B. Rowlett, had been shown the pilot model of the Mark I ECM sometime in the winter of 1934-35, before the order was issued, so they were not entirely ignorant of what the Navy was doing along these lines.

25. From 1924 to 1932 the Signal Corps appeared more interested in the Teletype Scrambler than in the ECM as a practical cipher machine which would meet Army requirements. However, under date of 25 July 1933, the Chief Signal Officer filed on behalf of Friedman a patent application (Serial No. 682,096) covering a cryptographic system and machine in which the stepping of the code wheels was very irregular and under the control of a keying tape. Electric control thus made its first appearance! Friedman made a complete assignment of his invention to the War Department and one or two preliminary models were built in 1935-36. These were successful and an order was placed with a relatively small and inadequately equipped manufacturer for a few machines, which were designated as Converter M-134A. It took a comparatively long time to build these few machines but by 1938 some of them were delivered and placed in service for communication between the War Department and the Commanding Generals of Overseas Departments. Later, additional ones were delivered and placed in service for intercommunication among the War Department and Corps Areas and between the War Department and the U.S. Military Attache in London. The first model of this machine was shown to me by the Signal Corps sometime in 1937. This machine indicated the reliability of electric control but the undesirability of the particular method (perforated tape) used in the Signal Corps machine.

26. Shortly before 15 June 1935, during the interval when preliminary models of the foregoing machine were being built, Mr. Frank B. Rowlett, principal assistant to Friedman, conceived the idea which constitutes the basis of the "stepping maze" in the present ECM. His concept was based upon the principle of sending an electrical impulse through the circuits of a code-wheel maze to generate a long, irregular sequence of events which could then be used for various purposes, such as keying. Rowlett and Friedman then jointly developed Rowlett's novel idea of a key generator as applicable to the Signal Corps machine and reduced it to more practical form in drawings. No model incorporating their ideas was built by the Signal Corps, however, because the Chief Signal Officer was committed to the type embodied in the Converter M-134A.

~~SECRET~~

~~SECRET~~

pre-production models of which were then under manufacture, and he was reluctant to make any change in design, despite Friedman's urgent recommendations that this be done. The inventors proceeded to incorporate the results of their theoretical studies and their drawings, reducing the new principles to practice in a patent application filed in the Patent Office on 23 March 1936 by the Chief Signal Officer on their behalf as joint inventors (Serial No. 70,412). The inventors made a complete assignment of their invention to the Secretary of War on 2 April 1936 and the application was processed through the Patent Office, though, of course, it is held in the secret status. Nearly all of the claims (39) have been allowed in the case.

27. In October 1935, Friedman and Lieutenant Wenger (of the Code and Signal Section) held a general discussion on cipher machines. Wenger expressed considerable dissatisfaction with the Mark I ECM and asked Friedman whether the Signal Corps had any "good" ideas along these lines. Friedman indicated that there were several ideas which the Signal Corps was not exploiting but which he was not at liberty to disclose, since they had been placed in the secret category. Friedman further indicated that if Wenger so desired, permission to disclose them to the Navy would be requested. Wenger asked that this be done. Accordingly, Friedman requested and was granted permission by his superiors to disclose the details of the Friedman-Rowlett patent application to representatives of the Navy Department. Therefore, on 21 October 1935, at a conference in Friedman's office, the details were disclosed to Commander McClaran and Lieutenant Wenger, who were shown the drawings that form the basis of the patent application Serial No. 70,412. On 31 October 1935, a second and similar disclosure was made to Commander McClaran, Lieutenant Wenger, and Lieutenant Harper. A third disclosure was made on 1 November 1935 to Lieutenants Wood and Dugan, also of the Code and Signal Section. Friedman and Rowlett were told very little as to the Navy Department's reaction to the disclosures; in fact, they were told that the principles disclosed were of no interest to the Navy at that time - which was the truth of the matter.

28. My first-hand knowledge of the Friedman-Rowlett invention began in the winter of 1936-37 when we were preparing initial specifications for the Mark II ECM. Wenger stated that Friedman had an idea for an electric control which had very interesting possibilities and produced from his safe a single sheet of cross-section paper containing three elementary wiring-diagrams by means of which electric control of an ECM could be achieved through an ECM maze. This paper was dated and signed (as I remember) by Harper, Wenger, and Wood, and by Friedman and Rowlett. (We have been unable to locate this paper since 1940.) I immediately realized that electric control gave us the answer to many of our unsolved problems and therefore had to be incorporated in the new machine. I was under orders not to discuss or show either the Mark I ECM or the Mark II ECM to the Signal Corps and, therefore,

~~SECRET~~

~~SECRET~~

adopted electric control and further developed the basic idea without the knowledge of the original inventors. In January 1940 the Mark II ECM was offered to the War Department for Joint Army-Navy use and also for purely Army use. It was explained that the mechanical features were well developed and "frozen" in design, and that we believed the Army would be well satisfied with the cryptographic principles involved, but that we were willing to discuss any security features in order to get a machine that would be satisfactory to both services. We wanted the Army to join us on the first order for the machine in order to further the idea of using identical cryptographic systems in the two services, as had already been done with the Strip Cipher Device. Another reason was to share the overhead for tooling-up and thereby give us a better price. It had been previously suggested that the Army and Navy get together on the Signal Corps machine or the Mark I ECM. We advised that neither machine was acceptable because of mechanical deficiencies but that we were developing a new machine and as soon as we had a working model we would endeavor to get permission to make it available as a common Army-Navy machine.

29. On 3 February 1940, Admiral Noyes (D.N.C.) invited General Mauborgne (Chief Signal Officer), Captain Cook, Mr. Friedman, and other Signal Corps representatives to inspect a pilot model of the Mark II ECM. On that occasion I acknowledged to Mr. Friedman, in the presence of General Mauborgne and Admiral Noyes, our use of his invention. Later there was a special conference attended by Mr. Reiber and Mr. Zenner of the Teletype Corporation, Mr. Friedman of the Signal Corps, Commander Safford and Lieutenant Zern of Naval Communications, and possibly others. The blue prints were carefully examined and a general discussion of cryptographic features followed. Friedman pointed out that the underlying principles of the control circuits of the Mark II ECM were those which had been disclosed by Rowlett and himself to the Navy Department in 1935, and this was confirmed by me. The four experimental changes to the Friedman-Rowlett circuit which had been made by Seiler and myself were discussed and the following decisions made:

- I. "Index Maze," which replaced the plugboard in the Friedman-Rowlett invention - Retained. The "Index Maze" accomplished the same cryptographic result as the plugboard but was much more convenient to the operator.
- II. Grouping of end contacts in the "Stepping Maze" and in the "Index Maze," which replaced the arrangements of the Friedman-Rowlett circuit - Retained. These groupings together with the ten circuits through the "Index Maze" gave 49 times as many stepping combinations as was possible with the Friedman-Rowlett invention (5,855 against 120).

~~SECRET~~



~~SECRET~~

- III. Subdivision of "Stepping Maze" into two parts - Unanimous decision to return to the original Friedman-Rowlett "Stepping Maze." Friedman protested the subdivision as an unnecessary complication. Reiber and Zenner did not like from the viewpoint of design and construction.
- IV. Stepping order for the "Stepping Maze" proposed by the Navy was 3-1-5, the other two wheels being dead to simplify construction. The stepping order was changed to 3-4-2 upon Friedman's recommendation.

With these exceptions the Mark II ECM, as developed by the Navy and Teletype using the Friedman-Rowlett "Stepping Maze," was satisfactory to and accepted by the Army. Washington Navy Yard sketch RW68F201, dated 24 April 1940, used as a basis for specifications of the production model, is the earliest-dated drawing showing the "Stepping Maze" and associated circuits exactly in their present form.

30. One other contribution, Major Leo Rosen's "Plugboard Code Wheel," came in 1943 after the ECM was in service. This was developed by the Signal Corps for field use, where the danger of capture was greater than in the Navy. The "Plugboard Code Wheel" was adopted for joint Army-Navy use at the request of the Army, but is being distributed to all Navy holders of the ECM. The chief value of the "Plugboard Code Wheel" to the Navy is possibly psychological, but we do have it in case of need.

31. Electric control of the ECM by means of the Friedman-Rowlett "Stepping Maze" is the essential feature that places the Mark II ECM in a class by itself as regards security. Those who have participated in the development of the Mark II ECM have always acknowledged the contributions of the Signal Corps. The "Index Maze" and grouping of end contacts add to the security afforded by the "Stepping Maze," but would be worthless without it. The importance of electric control can best be estimated by a consideration of what the Mark II ECM would have been if Friedman and Rowlett had not been permitted to disclose their invention to the Navy. Although the "Stepping Maze" appears obvious, now that it is in use, no one in the Navy thought of it in a period of 15 years, and no foreign machine employs it. Therefore, the Navy would have continued the development of the older methods and the new ECM would have used the mechanical stepping control found in CSP 903 or CSP 1700. We would have had a secure machine, superior to anything in use by foreign nations, but definitely inferior to our present ECM. This hypothetical machine (as well as CSP 1700) would defy attempts at solution until such time as machine and code wheels were captured. After this, each day's keys would resist solution for a long time. "Short-cut" solutions would be impossible, due to the erratic stepping of the code wheels, but a trial-and-error solution would be within the range of possibility.

~~SECRET~~

~~SECRET~~

We could not make the flat statement, as we do for the Mark II ECM, that solution would be utterly impossible. In other words, the machine would be adequate to take us through World War II but, because we had stopped short of the ultimate step, there would always be the desire to develop a new machine and scrap the old one. Rowlett is entitled to full credit for his discovery of the principle of the key generator as embodied in the "Stepping Maze," which adds so much to the excellence of the Mark II ECM, and Friedman and Rowlett jointly are entitled to full credit for their joint invention of methods of applying and reducing the principle to practical form.

32. The Signal Corps' acceptance of the Mark II ECM for Army as well as Joint Army-Navy use reflects credit on all who made that decision. The joint Army-Navy ECM Cipher System became effective on 1 August 1941, and the two services had a common high-security cipher system in effect and in use prior to the attack on Pearl Harbor. This use of an identical machine with interchangeable code wheels has been of great military value, particularly in the early stages of the war when the distribution of machines and code wheels was incomplete. In the Philippines, Java, Australia, and even in North Africa, Navy wheels have been used in Army ECMs, Army wheels in Navy ECMs; machines have been borrowed back and forth between the two services; Army messages have been sent in Navy ECM ciphers and the Navy messages sent in Army ECM ciphers.

~~SECRET~~

~~TOP SECRET~~

## Informal Memorandum

The two primary faults of the cryptographic machine under discussion, and faults which alone permitted the solution described, are, as described:

1. Non-pluggable cipher maze output endplate.
2. Provision for cipher rotors to move singly on occasions.

In section XIX, recommendations, P. 190, paragraph 48 (b) 1, a pluggable endplate is recommended. This takes care of "fault #1."

But paragraph 48 (b) 2 does not recommend, as we believe it should, a change in the cipher maze stepping provisions. It suggests instead that the stepping of the stepping rotors be changed by insertion of an additional fast moving wheel there, which is a good idea and certainly should be adopted. The cipher maze stepping rotors however should never be allowed to move singly, or they will "give themselves away" as this paper so aptly demonstrates.

Experience in B-III-Research tells us that in a Hebern-type of machine (which the SIGABA is except for motion) that there should always be THREE NON-ADJACENT WHEELS MOVING AT ALL TIMES. In an Engima type of machine, there should always be TWO NON-ADJACENT WHEELS MOVING AT ALL TIMES. We believe a recommendation should be made to the effect that two more fast moving wheels be provided for the cipher maze in addition to the one which might be moving at any one time, or else that one more fast moving

be provided the cipher maze and the cipher maze converted to Enigma type.

It has long been the contention of B-III-Research that wheels in cryptographs of Enigma type should never move singly, nor in Heber types ever in less than threes, and that endplates should be protected by plugging. We therefore read the attached paper with greatest interest.

March 28, 1944

OCSigO 461 Codes  
(Gen.)

WAR DEPARTMENT  
OFFICE OF THE CHIEF SIGNAL OFFICER  
WASHINGTON

8

SUBJECT: Blank forms for code accounting.

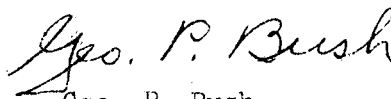
MAY 16 1935

TO:

1. Par. 11, AR 105-25, dated September 1, 1934, requires that certain reports be accomplished whenever any registered War Department cryptographic publication is transferred from one holder to another, and that a semiannual report of possession be made on all such items. For purposes of facilitating the making of these reports a standard form has been established, designated as WDSC Form No. 84, "Semiannual or Transfer Report of Registered Secret and Confidential War Department Publications and Devices."

2. Attention is invited to the fact that the above-mentioned form (Stock No. 6D84) is now stocked at the Signal Section, New York General Depot, and issued on approved requisitions in the same way that other authorized Signal Corps forms are issued.

For the Acting Chief Signal Officer:



Geo. P. Bush,  
Major, Signal Corps.

July 1935

~~CONFIDENTIAL~~

8

June 26, 1935

MEMORANDUM FOR: Research and Development Division  
(Military War Plans & Training Division)

1. In connection with the tabulating machinery now employed by the Signal Intelligence Section, the undersigned have invented a new and useful device which may be attached to the electrical counting sorter and which will be of importance in future employment of this machine in code compilation and in other work not related thereto, of a purely commercial character.
2. The principal object of the invention is to transform the electrical sorter into a device of exactly opposite function, viz., to "unsort", "scramble", or disarrange in a wholly random sequence a set of punched cards originally arranged in a definite or regular sequence. Another object is to provide a means and device for obtaining a wholly random, small sample from a large set of punched cards.
3. In view of the fact that such a device will be very useful in code production, it is desirable that patent application be made in order to protect the government's interests.
4. At the same time, in view of the usefulness of the device for certain commercial tabulating installations in which random selections of punched cards must occasionally be made, permission is requested to enter into negotiations with the International Business Machines Corporation or other companies, with a view to possible sale of commercial rights to this invention.
5. Attached hereto is a sketch and description of the invention, in the form of a preliminary draft of specifications.

William F. Friedman  
Frank B. Rowlett

Attached:  
Sketch  
Description.

OCsigo-413.52-Gen. (6-26-35)

1st. Ind.

10.

War Department, OCsigo, Washington, August 21, 1935. To: Mr. W. F. Friedman and Mr. F. B. Rowlett, War Plans and Training Division.

1. In compliance with request made in paragraph 4, of your memorandum, dated June 26, 1935, relative to an invention covering an attachment to an electrical counting sorter, there is no objection to your entering into negotiations with any industrial organization with a view to possible sale of commercial rights to your invention, described in the memorandum herein referred to.

By Order of the Chief Signal Officer:



Dawson Olmstead,  
Colonel, Signal Corps,  
Executive.

WAR DEPARTMENT  
OFFICE OF THE CHIEF SIGNAL OFFICER  
WASHINGTON

8

August 31, 1935

1. This is to record certain facts in connection with the invention of several alternative means of providing an aperiodic displacement of the substitution cipher wheels of a cipher machine as granted in claim 17 of the patent specifications having reference to Converter Type M-134-T2.

2. It is desired to record here that the fundamental principle of using one or more commutators in conjunction with a set of selector magnets as a means for effecting the aperiodic displacements discussed in par. 1 is the contribution of Frank B. Rowlett.

3. The subsidiary principle (subsidiary to that set forth in par. 2) of producing aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of an independent set of commutators containing contacts equal in number to the number of substitution cipher wheels to be displaced, is the contribution of Frank B. Rowlett.

4. The subsidiary principle (subsidiary to that set forth in par. 2) of producing aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of an independent set of cipher wheels, hereinafter called the control cipher wheels, and having the latter cipher wheels identical in number of contacts and construction with the former so that all cipher wheels are interchangeable, is the contribution of William F. Friedman.

5. The subsidiary principle (subsidiary to that set forth in par. 2) of producing the aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of a second set of control contacts on each face of each of the substitution cipher wheels themselves, and providing appropriate electrical circuits for the control contacts to govern the operation of the displacement mechanism, is the contribution of Frank B. Rowlett.

6. The subsidiary principle (subsidiary to that set forth in par. 2) of producing the aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of the same set of substitution contacts operating in connection with a gang switch which makes these contacts serve for substitution and control in alternate sequence, is the contribution of Frank B. Rowlett.



7. The application of the principle of aperiodic displacement of substitution cipher wheels to cryptographs of the original Enigma type (in which the electrical circuit through the cipher wheels is reversed by means of a reversing cipher wheel and again conducted through the other cipher wheels before reaching the signaling element) is the contribution of William F. Friedman.

8. The foregoing facts will be used as a basis for evaluation and division of interest in all financial benefits which may accrue from the prosecution of the invention and its reduction to practice.

William F. Friedman  
William F. Friedman.

Witnesses:

Chas. A. Howe

Frank B. Rowlett  
Frank B. Rowlett

Louise N. Nelson

---

File M-138  
Patent Application

6

July 6, 1935

MEMORANDUM FOR: Research and Development Division (Navy W.P. &amp; T. Div.)

1. In accordance with provisions of Par. 4c, AR 850-50, there is attached a draft of specifications upon which application for patent on Cipher Device Type M-138 may be based.
2. It is understood that the Navy Department has pending an application for patent on their first type of strip cipher device, and are filing an application covering their second type. They are apparently satisfied to standardize, for the Naval Service, our Type M-138, and are planning to purchase 100 or 200 devices identical with ours, except as to name plate.
3. It is recommended that the attached draft be forwarded to the Signal Corps Patents Section for use in the preparation of detailed specifications and drawings. In view of the existence of similarities between our Type M-138 and the Navy types, it is probable that patent of only limited scope can be obtained. Nevertheless, the improvements devised by me, consisting in the use of metal channel ways, a slidable guide rule, and a construction which permits of setting up the text alternately at the left side and right side of the assembly, make our type of device a very much more practical instrument than any of those heretofore devised.
4. Since these improvements arose from my own studies, it is requested that application be made in my name as inventor.

William F. Friedman,  
Signal Intelligence Section.

COPY FOR: Mr. Friedman.

85

Recd. 7/18/55  
Chas. A. Rowe  
Patent Section

~~Confidential~~

ROUTING and WORK SHEET

(To be used under provisions of Par. 41.6 b, Office Regulations, OCSigO, 1934)

From: WP+T

To: R+D.

Forwarded  
K

From R+D to WPT

Request following information

1 Has Mr. Friedman been designated or employed for the purpose of making this invention?

2 Is the invention important to National Defense?

WPT to R+D.

RPR

1. Mr. Friedman was not ~~was~~ designated or employed for the purpose of making this invention
2. The improvements are not considered to be of such character as to warrant being classified as "important to National Defense" K

(WPT)

To NRS for patent action

RPR

(Check one)

REF ID: A4126886

SECRET

CONFIDENTIAL

RESTRICTED

DATE 29 July 49

TO	FROM	TO	FROM
CHIEF, ASA	(10)	Tech Staff	(96)
Spec Asst to the Ch	(14)	Spec Proc Br	(97)
Ch, Hist Unit	(13)	CH, SECURITY DIV	(80)
Asst to the Chief	(11)	Tech Staff	(81)
Joint Secretariat	(12)	Ch, Materiel Br	(82)
DEPUTY CHIEF, ASA	(20)	Ch, Methods Br	(83)
Asst Deputy Chief	(20)	Ch, Protective Br	(84)
Executive	(20)	Ch, Maint Br	(85)
Secretariat	(20)	CH, RES & DEV DIV	(70)
Ch, Pres Sec	(21)	Tech Staff	(71)
Ch, Org & Tng Sec	(22)	Ch, C & C Br	(72)
Ch, Plans & Oper Sec	(23)	Ch, Equip Br	(73)
Ch, Logistics Sec	(24)	Ch, Electromech Br	(74)
Ch, Fiscal Sec	(25)	Ch, Lab Serv Br	(75)
Adjutant General	(26)	Ch, Cryptologic Br	(76)
Ch, Sec Cont Sec	(27)	Ch, Electronics Br	(77)
CH, OPERATIONS DIV	(90)	Ch, Pers & Tng Br	(61)
Directives Br	(90x)	Ch, Supply Br	(62)
Ch, Lab Br	(91)	SIGRP-5	(62)
Ch, Machine Br	(92)	CO, Arlington Hall Sta	(40)
Ch, Gen Processing Br	(93)		
Ch, Facilities Br	(94)		
Ch, I & D Br	(95)		

- Approval & Return
- As Requested
- Concurrence or Comment
- Information & Forwarding
- Information & Return

- Information & File
- Recommendation
- Signature if Approved
- Your Action (by \_\_\_\_\_)
- For recommended reply

Copy for you & one for the person writing up history of SIGASA.

one copy forwarded to J  
AS - 80 8/1 Aug 49  
AS

C O P Y

WAR DEPARTMENT  
Office of the Chief Signal Officer  
Washington

February 15, 1936

1. In connection with a memorandum dated August 31, 1935, (copy attached) setting forth "certain facts in connection with the invention of several alternative means of providing an aperiodic displacement of the substitution cipher wheels of a cipher machine as granted in claim 17 of the patent specifications having reference to Converter Type M-134-T2," the following additional facts are made of record:

2. The principle of employing a set of juxtaposed rotating commutators as a means of selecting in an irregular, aperiodic manner, the successive alphabets (for encipherment or decipherment) from among a plurality of cipher alphabets is the contribution of Frank B. Rowlett.

3. The associated principle of controlling the stopping positions of a single substitution cipher wheel by a set of juxtaposed control cipher wheels is the contribution of William F. Friedman. Note: Thus, for example, in Friedman and Graham U. S. Patent No. 2,028,772 the cipher key transmitter and its associated mechanism would be replaced by a set of control cipher wheels, the 26 final contacts of which would be connected to pins which would stop the substitution commutator in the enciphering (or deciphering) position.

4. The idea as to the possibility of directly applying the foregoing principles to the stopping of a rotating printing wheel at cipher positions, the latter being superimposed upon the stopping position determined by the key depressed on the keyboard, is the equal and joint contribution of both William F. Friedman and Frank B. Rowlett. In this case, in order to prevent cumulative errors it is necessary to return the printing wheel to an initial position after each operation. The cipher stopping position of the printing wheel is determined after it has been stopped by the depression of a key of the keyboard.

/s/ WILLIAM F. FRIEDMAN

Witnesses:

/s/ Louise N. Nelson

/s/ Chas. A. Rowe

/s/ FRANK B. ROWLETT

C O P Y

WAR DEPARTMENT  
Office of the Chief Signal Officer  
Washington

August 31, 1935

1. This is to record certain facts in connection with the invention of several alternative means of providing an aperiodic displacement of the substitution cipher wheels of a cipher machine as granted in claim 17 of the patent specifications having reference to Converter Type M-134-T2. [Application Serial No. 682,096]

2. It is desired to record here that the fundamental principles of using one or more commutators in conjunction with a set of selector magnets as a means for effecting the aperiodic displacements discussed in par. 1 is the contribution of Frank B. Rowlett.

3. The subsidiary principle (subsidiary to that set forth in par. 2) of producing aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of an independent set of commutators containing contacts equal in number to the number of substitution cipher wheels to be displaced, is the contribution of Frank B. Rowlett.

4. The subsidiary principle (subsidiary to that set forth in par. 2) of producing aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of an independent set of cipher wheels, hereinafter called the control cipher wheels, and having the latter cipher wheels identical in number of contacts and construction with the former so that all cipher wheels are interchangeable, is the contribution of William F. Friedman.

5. The subsidiary principle (subsidiary to that set forth in par. 2) of producing the aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of a second set of control contacts on each face of each of the substitution cipher wheels themselves, and providing appropriate electrical circuits for the control contacts to govern the operation of the displacement mechanism, is the contribution of Frank B. Rowlett.

6. The subsidiary principle (subsidiary to that set forth in par. 2) of producing the aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of the same set of substitution contacts operating in connection with a gang switch which makes these contacts serve for substitution and control in alternate sequence, is the contribution of Frank B. Rowlett.

7. The application of the principle of aperiodic displacement of substitution cipher wheels to cryptographs of the original Enigma type (in which the electrical circuit through the cipher wheels is reversed by means of a reversing cipher wheel and again conducted through the other cipher wheels before reaching the signaling element) is the contribution of William F. Friedman.

8. The foregoing facts will be used as a basis for evaluation and division of interest in all financial benefits which may accrue from the prosecution of the invention and its reduction to practice.

/s/ WILLIAM F. FRIEDMAN

/s/ FRANK B. ROWLETT

Witnesses:

/s/ Louise N. Nelson

DRAFT

WDGSS-14

15 January 1946

MEMORANDUM FOR ASSISTANT CHIEF OF STAFF, G-2

SUBJECT: Release of Cryptological Inventions and Developments

## DISCUSSION

1. In the years preceding the outbreak of the present war and during the war itself, numerous cryptological inventions were made by <sup>ASA</sup> military and civilian personnel. Applications for patent were filed on some but not on all of such inventions. In either case, information regarding such inventions has for the most part been denied the public. Since the most recent War Department policy is to release as much technical information as possible, it is necessary to reexamine inventions in the cryptologic field.

2. The inventions concerned fall into five categories. Army Regulation 850-50, <sup>17 July 1942,</sup> paragraphs 7 and 9, (Tab A), refers to three of these categories and indicates the nature of the Government's rights. Additionally, there are inventions made by persons or companies under contract to the Government and in these cases normally the Government's rights depend upon the terms of the contract but usually amount to a royalty-free license to practice any inventions made, with ownership of the inventions remaining in the contractor. The last category involves the independent agent, one who, working entirely on his own, produces an invention of merit. In



such a case, the Government has no rights except through purchase or the taking of a license.

3. Further discussion in this memorandum will be limited to the second category of Army Regulation 850-50 wherein the Government takes a nonexclusive royalty-free license and the inventor has a theoretical right to exploit commercially for his own benefit. Where cryptologic inventions are involved, classification of the equipment and security restrictions placed upon information pertaining thereto have been used to prevent commercial promotion. Cash awards to civilian inventors in Government service are in some circumstances possible, but the Army Security Agency has held that where the invention is within the purview of the employment an award is improper. Virtually the only other possibility of compensation to an inventor is by Congressional action.

4. ~~With the cessation of hostilities,~~ cryptologic invention and development by independent inventors and by contractors <sup>has</sup> ~~can~~ <sup>in the past produced very little</sup> ~~be expected to fall off to nearly nothing,~~ and reliance, therefore, ~~will have~~ to be placed on Government employees. It is believed that some incentive must be furnished if <sup>and invention in this field</sup> research is to continue to be highly productive; the possibility of financial returns from commercial promotion <sup>of cryptologic inventions that can be released</sup> may be sufficient.

5. The latest War Department policy bearing on the matter appears in a memorandum, subject: Classification,

Reclassification, and Declassification of Scientific and Technical Information, for the Assistant Chief of Staff, G-2, Director, New Developments Division, Director, Bureau of Public Relations, Commanding Generals of the Army Air Force, Army Ground Force and Army Service Force (Tab B), which states in paragraph 3 that "as liberal a policy with respect to review and declassification of classified projects and material as is consistent with continuing only those items of information, the publication of which would cause exceptionally grave danger to the nation or endanger the national security or cause serious injury to the interest or prestige of the nation or any Governmental activity thereof or which would be of great advantage to a foreign nation or cause administrative embarrassment, etc., will be retained in a security classification." According to General Borden, New Developments Division, the policy of the said memorandum is such that very good reasons must be presented in order to prevent the release of information. Further of interest in this regard is the policy of the United States Patent Office with respect to applications on file, which policy is indicated in a letter from Colonel Donald K. Lippincott, Patents and Inventions Counsel, Legal Division, Office of the Chief Signal Officer, to Intelligence Branch (Tab C). Patent Office policy is based upon a memorandum from the Joint Chiefs of Staff (Tab D).

6. Since fundamental cryptographic systems are well known, the greatest danger involved in the release of information in the form of patents or otherwise appears to be that of acquainting foreign powers or unfriendly forces with effective adaptations and arrangements of these systems. Patent applications need not and rarely do contain key generating means, rotor wiring, and other specific features upon which the security of cryptographic text really depends. The main difficulty is that, by disclosing basic features of successful machines used by this country, the development of other adaptations is made possible, and our own cryptanalysts will be faced with text very difficult to decipher. On the other hand, many American machines already are known in principle to thousands of persons who either maintained or operated the same, and it is most unlikely that the principles can be now successfully suppressed. Added to this is the probability that independent inventors, and particularly contractors who have acquired techniques and know-how in the performance of war contracts, will produce machines similar to those at present in use. Such machines would not be classified nor is there any means of restraining their promotion.

7. It is the well-established policy and practice of the War Department to declassify material when the information can no longer be considered as secret, confidential, or

restricted. To maintain classification on information the control of dissemination of which is ineffectual only results in the degradation of the classification system itself.

8. To declassify any specific item does not establish a general policy applicable to other items in the same general category. If this were not true the declassification of any item, whether it be a document or a piece of equipment, would be impossible, except in the rare case in which the entire category consisted of but a single item. Hence, to declare that declassifying a specific item of cryptographic equipment would lead to the declassification of all other classified items of cryptographic equipment is not warranted by considerations of policy or practicability. *In declassification, each item must be considered and evaluated on its own merits.*

9. It should be stressed that the declassification of a patent application and thus the issue of a patent covering certain principles or features of a cryptographic apparatus does not usually have as a consequence the declassification of a machine as a whole or the traffic handled by it since, as indicated in paragraph 6, the working apparatus will depend for its security upon specific wiring and so forth not disclosed in the patent.

#### RECOMMENDATIONS

10. That no exception from the announced War Department policy of liberality with respect to the release of technical information be made in the case of cryptologic inventions.

11. That the Chief, Army Security Agency, determine specifically which cryptologic patent applications or developments may be released.

~~TOP SECRET~~

*Jean*  
*in my Personal file*

29 April 1946

MEMORANDUM FOR THE CHIEF, ARMY SECURITY AGENCY:

SUBJECT: Release of Cryptographic Principles.

1. The following policy is announced to be effective immediately:

a. Cryptographic principles or devices developed by officers, enlisted men, or civilians employed in any War Department Agency, or patents or patent applications on such principles or devices which are owned by, assigned to, or licensed for use of the War Department will not be released for use of foreign governments or for foreign or domestic commercial or private use until such time as necessary information is available and a procedure established in the Army Security Agency whereby information which is cryptographed by means of such principles or devices can be cryptanalyzed and read under any and all circumstances.

b. Where it is in the interest of the Government of the United States that an employee have no patent rights in cryptographic principles or devices to dispose of, and for the Government to own the entire interest for security reasons throughout any foreseeable future; and where discovery or invention of cryptographic principles or devices has been made by a civilian employee and does not relate to a matter as to which the employee was specifically directed to experiment with a view to suggesting improvements nor was produced as a result of any specific employment or contract to invent a specific device or article; and where an application for patent on such principles or devices has been filed with an assignment-in-trust to the Government for the purpose of maintaining such application in secrecy; the Military Intelligence Division will support, subject to the availability of appropriations, any reasonable request for purchase of all commercially exploitable reversionary rights of the inventor in the patent application.

CARTER W. CLARKE  
Colonel, GSC  
Acting Deputy, A.C. of S., G-2

~~TOP SECRET~~

*Copy for Col Row*~~CONFIDENTIAL~~

27 September 1945

SUBJECT: Release of Patent Application Serial No. 443,320

TO: Commanding General  
Army Security Agency

1. The subject patent application covers a cryptographic means and device for automatic encipherment and decipherment of teletypewriter signals and was filed in the U. S. Patent Office on 16 May 1942 in the name of the undersigned and Frank B. Rowlett, as co-inventors.

2. The principles involved in the subject application have been utilized in Converter M-228 and Converter M-294.

3. It is requested that the subject application be officially declassified in order that it may be allowed to go to issue, whereupon the right and title will revert to the undersigned and Frank B. Rowlett, subject to an irrevocable, non-exclusive, and royalty-free right and license remaining vested in the United States of America.

4. This action is desired because of the commercial applications of the invention, interest in which is believed to exist on the part of the U. S. communication companies.

5. Declassification of the patent application does not necessarily involve the declassification of the specific embodiments thereof represented in the apparatuses mentioned in paragraph 2.

WILLIAM F. FRIEDMAN

~~CONFIDENTIAL~~

AS-70 AS-23 10 Apr 47  
AS-80  
AS-90

Procedure for Release of Information  
Concerning Cryptography Patents

Lt. Chapman, Ext 462

1. All previous instructions pertaining to the above subject are rescinded.

2. Research Laboratories Division is charged with the primary responsibility for making recommendations related to the control and evaluation of all patents and patent applications affecting cryptologic equipment and processes. In view of the above, the following procedure will be adopted for the handling of requests relating to the release of patents held in secrecy:

a. If the request is received by Research Laboratories Division, comments and recommendation will be forwarded by AS-70 to AS-20 after coordination with AS-80 and AS-90.

b. If the request is received by the Deputy Chief, it will be forwarded to AS-70 who will coordinate with AS-80 and AS-90 and return comments and recommendation to AS-20.

3. Comments should include sufficient background material to determine that recommendation is in accord with current policy on release of cryptographic principles, a copy of which is attached. The last sentence of paragraph 1a of attached policy will be interpreted on the basis that the Army Security Agency could expect to solve communications which may be passed therein, assuming the device were to be used in a practical manner by adequately trained personnel and resulting in a normal military or commercial traffic expectancy.

1 Incl  
Memo for Ch, ASA fr  
ACofS, G-2 dtd 29 Apr 46  
subj: Release of Cryptographic Principles

/s/ Harold G. Hayes  
HAROLD G. HAYES  
Colonel, Signal Corps  
Chief, ASA

CYS FURNISHED

AS-14  
23  
24



WASHINGTON 25 D.C.  
~~SECRET~~  
HEVDONVBLETS

COPY



Encl. 9



**COPY**

~~SECRET~~ ID: A4126886

HEADQUARTERS  
ARMY SECURITY AGENCY  
WASHINGTON 25, D. C.

*File key personal  
file*  
*BS*

WDGSS-23

20 May 1946

SUBJECT: Release of Patent Application Serial No. 443,320

TO: Mr. William F. Friedman, WDGSS-14

1. Reference your letter dated 27 September 1945, subject as above, the attached memorandum from the Acting Deputy Assistant Chief of Staff, G-2, outlines the War Department policy on the release of cryptographic principles.

2. Analysis of the policy would indicate that:

a. Patent application No. 443,320 will not be released unless it can be shown that the employment of the principles involved are susceptible to cryptanalysis under all circumstances; and

b. If not released, a request for purchase of all commercially exploitable reversionary rights may be entertained provided it can be shown that Frank B. Rowlett and yourself were not directed or employed to experiment on or to invent the principles or improvements embodied in Converter M-228 or Converter M-294.

3. If it is felt that subject Patent Application should be released under (a) above; or if and when it is felt a case should be presented for purchase of rights in conformity with stipulations contained in (b) above, an application for release or purchase, containing pertinent facts and necessary proofs, may be prepared and submitted to the Director of Intelligence through the Chief, Army Security Agency.

1 Incl  
Cy ltr dtd 29 Apr 46  
subj: "Release of Cryptographic Principles"

/s/ HAROLD G. HAYES  
Colonel, Signal Corps  
Chief, Army Security Agency

~~SECRET~~

COPY

29 April 1946

MEMORANDUM FOR THE CHIEF, ARMY SECURITY AGENCY:

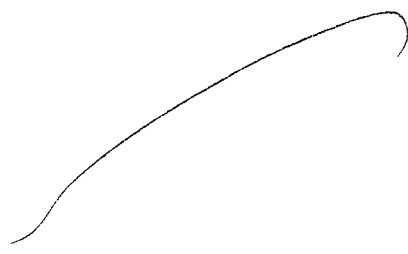
SUBJECT: Release of Cryptographic Principles.

1. The following policy is announced to be effective immediately:

a. Cryptographic principles or devices developed by officers, enlisted men, or civilians employed in any War Department Agency, or patents or patent applications on such principles or devices which are owned by, assigned to, or licensed for use of the War Department will not be released for use of foreign governments or for foreign or domestic commercial or private use until such time as necessary information is available and a procedure established in the Army Security Agency whereby information which is cryptographed by means of such principles or devices can be cryptanalyzed and read under any and all circumstances.

b. Where it is in the interest of the Government of the United States that an employee have no patent rights in cryptographic principles or devices to dispose of, and for the Government to own the entire interest for security reasons throughout any foreseeable future; and where discovery or invention of cryptographic principles or devices has been made by a civilian employee and does not relate to a matter as to which the employee was specifically directed to experiment with a view to suggesting improvements nor was produced as a result of any specific employment or contract to invent a specific device or article; and where an application for patent on such principles or devices has been filed with an assignment-in-trust to the Government for the purpose of maintaining such application in secrecy, the Military Intelligence Division will support, subject to the availability of appropriations, any reasonable request for purchase of all commercially exploitable reversionary rights of the inventor in the patent application.

/s/ CARTER W. CLARKE  
Colonel, GSC  
Acting Deputy, A.C. of S., G-2



REF ID:A4126886

These are my original work  
sheets of Hebern Solution

W.S.F.

REF ID: A4126886

---

1936

FRIDAY, NOV.

**27**

EFGHIJKLMNOPQRSTUVWXYZ

REF ID: A4126886

MONTE #9

HDRYYZ YTO  
LCRYZYV BBE  
ZEPPLIN C

NEW VEG  
000

MONTE

UJJSLSWCRNULSAEXTGWPZYV GIV  
 HNOWBYWCGBRIFNUYTSIVTZKY  
 MCOMPANYACCEPTALLGENERALCOMP  
 CBXYRKRHNZZWJAYYNRYVFZJSKG  
 VSLHCUEBAIJBYNSTIPWHFUIQN  
 FSSIONREQUIREMENTSANDAREAN  
 OVDUQZTHHSYGEGKOAQFZHXRPMH  
 FPMKREJBCCOMSODUGEDSOEUZ  
 XIOUSTOPROCEEDASSOONASPOSSO  
 YZTJLIUNXXUJAIIVSSTFXTZLJVU  
 EAFRBBNZRSRXMJCIJUDCXUTJMG  
 IBLLETIMETOEXECUTEONEXEYEA  
 VEYYGODZLNMLVKUOFRXHVKIHPF  
 OHGHFKGGFBSIACVUBPBNINSRAN  
 TTHEYPROPOSESESEVERALMODIFI  
 LNCELFFQESQZSWHLEHDTGSBUHET  
 XTJJBQTSBWJECHLVKBVUNMDRE  
 ATIONSWHICHDEPARTMENTSHOUL  
 UZACAMHVPDJZKIFAJGVORHXODJ  
 HACYENAVKTWKBJZPCSGYSPFCIL  
 DCONSIDERANDWHICHAREINMAIOL  
 SJBUSKBBHFNIBYXYXDIHLKEHQJ  
 TNTKXUXBCVCHDRXTZBONRKCRLL  
 STOPMEANWHILETHEPRESENTGER  
 ELCHUKFNCOZDYCKTYPQPDCCHOM  
 GYXXLURZDOJVGIDSUTEVPERRDH  
 MANLAWMUSTBEAMENDEDDBYGERMA  
 ULZPOATXITVKTCKWNTQJEVODGG  
 HYBFJFJQEMYAPIDFIVEFAJBHZA  
 NLEGISLATUREBEFOREZEPPLIN  
 CUZQWDVWQXZENEQESHCECLUHPS  
 VIBQUPUXYSJRETBVJLNZPSDRAS  
 OMPANYCANPROCEEDFURTHERINT  
 HEXGEKOE  
 UHLEKULN  
 EMATTER

EMATTER

HAGUE #8

S Y Y G S T X V P

L X D W P A H N C  
H A V E A B S O L E

MAG V Q J H A R Q R M F L A H W T Z L B H T V D R  
J C F S S S B I H X J U Y L P K H V S R N Q A M J Y  
11 13 20 5 4 3 21 5 22 12 1 5 20 22 10 26 14 3 16 12 13 22 14 10 13 7

O H H B H P D Q N T K Q Q H S F J M C F O J A A M K  
W X V Z I R V B N A Z T L J B D A O F A I X Y H  
25 12 19 17 24 7 25 13 19 10 26 17 24 25 24 12 7 19 11 25 16 17 25 9 6 25

W Y S X V B I W O A J Z G Z E J A D C K W Z K R I  
R G W N T X D Y O K X L O N V C R C O L L V M W V W  
5 24 11 16 23 16 17 25 21 6 11 24 17 6 6 25 15 23 11 18 15 25 11 16 22 14

T I N O V U O Z P Y L H T Y S R P W G L R V Y F G B  
E Y V J T N M H L O I G Q S I O T I U R T K B J A R  
22 5 18 8 22 14 1 23 1 20 2 14 5 21 24 11 10 21 24 12 6 20 5 14 12 6

A I H P U C B R K O Z U G C C H W Z D I X G R B A P  
B Y X G M B Y G Y P K T O J K K H R D G E X V P I C  
1 5 19 22 3 22 26 18 24 15 5 15 17 24 1 26 14 14 5 24 2 26 24 1 4 15

Z G C U N V K U A T D Y X V E K N W Y X R V P D W K  
A D Y L X U W P J N V Q W C V F J I X D T K Z I P P  
10 22 4 6 17 11 7 17 3 10 10 6 1 1 6 3 21 21 3 4 6 20 6 15 26 25

G U X J B X E O D S P Q S A X A O Z M B V K F G M G  
C J M Q W P N N T D N Z G O Y Q W R B L J L I Z H O  
14 10 5 14 9 19 13 12 18 14 9 17 13 16 18 2 23 14 9 16 17 14 16 5 6 2

Z I F O D O F Z I F T E L V M U D C B V P O P T N O  
A Y O J P L S H F V O S K C X X B N K I X D Z B R F  
10 5 1 3 20 4 2 23 10 11 19 23 3 1 7 6 11 2 23 19 1 6 6 4 2 19

A G I N K L B W V X J V C V Z Y K A W O P T E C P Y  
B D T W U D Y Y X T X A I C O U G S J Z X Z D T B E  
1 22 26 10 12 18 26 25 13 17 11 25 26 1 15 1 4 17 19 9 1 7 1 3 3 23

C U W I I J K B Q P W O T H S G L S Y D F Q U Q N J  
W J T A B S W I W M B R O I L R O I X E G J E L R M  
13 10 24 7 23 3 7 24 5 24 17 20 5 25 24 16 13 18 3 3 5 16 26 12 7 3

V R Q G B S N J H B S P X Q V S U M H K W Y I B C Y  
P A G F W Z Z U D B E O W B D J Y A N J L A T P U E  
24 9 15 15 9 23 22 9 15 18 12 18 1 14 9 22 16 19 1 18 15 15 4 1 18 23

H O W F Y F J N N A U J F L S C O  
V H T P T R T A B K S Y Y L L W  
20 3 24 21 22 26 20 3 19 6 24 21 20 22 24 20 23

N: M E R M A N G O V E N N M E N T

Underlined portion represents arrow in decipherment

AG (AGANA #4) but should really be AGANB

ESRUXMMFY EPA  
WFLVY YZDXAXWA  
YAVALCOUNCT

BH JIUKXJ SQSG ZIRK SRY LRLR DYCOVZ  
JUGPKOWRY HGEH ZEKRLMOBWOZ JAV  
NOWINSESSSIONTCKYOTODETERM I

BI O.EEKAPN.ZRQB POSSEPEQDXGDLTNA  
CEFPBEVDDTYKODESPBZZSCQXNW  
NEDEMANDS ATPACIFIC CONFERENCE

DJ O.PRRNF.OBZFLCKGMRCLMXLLJHV  
CAXYTNIVEREDYLTBILXZOPFOJK  
CEPRACTICALYALLAGREERATIO

EK O.HUDHVOGAKDICSCBEYXMPYTRDK  
CSGKVQIFFVREEDGDTSYTWWSF  
JETAPANESEVESSELSSTOUNITIEDS

FL KVJJDWDOALJZCQMMWTYUODVZCOE  
MMLKRMIECSGDWCTCQSWVBWSPAC  
TATESNAVALVESSELSMUSTBESEV

GM SNWCHZYG AJBF GOZGUFQRTC YMKV  
QQPVVBHFFSYTEPINUZCOUNXCKA  
ENTENTHSORTWOSHIPSSTOTHRES

HN YRMKZOMCLGPCS OZSC CAMPNXHVQ  
BWHPAHLZCHJDCPKFIJPITKCOJ  
TOPDECIDEDITOPUTIMRESERVEFO

HO RSKJHLLZFNZQYSBZOLITIXMRUJU  
MROMVZADQVGVNDCLSL SMAARBHD  
URPREDRADNAUGHTSSEVENARMO

JP ZAMPKQADBRBCORPUGJIHKAJKLLK  
WYHCQPDOWEYDOINTOALKGSFJSL  
REDLCRUTSERSEFIVEICRUISERSALL

KQ MGSPEGRESIFAIXZQFIWMADUCFM  
FZSCHDBKYCSTFTKZYKFYRCAPGE  
OLDSTOPNAVALDELEGATESWILLB

LR IVDAESILFUZTGKPEWDPZHKLKTE  
TMJAHVZAQNGLKZNSDYRPLHQJYC  
EVIDEADMIRALKATOCAPTAINSYA

MS BGRUBHCVIQUAUNGW IC  
OZXHSWYSBTOIQCMC  
MAYASHIANDNAGANO

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25



GENOA Effective key GENPA

REF ID: A4126886

D Y P F M L W Q Y S D Z U  
DRQAYOIGYOGWF  
G E R M A N C O N T H R A C

HNCO fZ

W X Q G M G X N K T R V K V T T B Y T P V D Z T N N  
P J O D L F O Y W L H Y A A Q R G U U V H E U Z P Q  
26 12 3 22 7 15 25 1 2 22 23 26 25 5 18 11 26 23 12 3 22 7 20  
T S F O R Y E A R C O N T E M P L A T E S F O R C O

LNCO gN

N R O T L D H S W W G M I P B Z Z C G P G P R V T B  
R Y G F A O Z Z X Y K S H O E N O L S U U W T K A P  
7 1 25 17 8 26 22 23 15 2 25 20 18 10 6 15 20 18 22 24 20 6 20 14 10  
T T F A G U P O R I T I S H W A R S H I P S A S F O

JNCO hT

B M B Y B U Q Q O U R Q D M D B N E Q D S B H Y C Z J  
H R E T K R S L O G W U T W E G V D B L K O Z R W K  
6 6 18 25 13 2 4 4 23 18 5 7 16 2 10 12 6 8 11 18 23 10 8 10 17 18  
L L O W S A P P R O X I M A T E L Y F O R T Y T H O

KNCO iZ

X S J R L I G G D J D V A T H Y W R U W X L B Y Y I  
I T N A A A G H R U T Y L P H S F O Y I C R N A O J  
14 1 19 9 8 7 21 25 25 9 18 23 26 13 18 24 4 14 16 21 22 13 15 5 19  
D I C E S E A M B F S Q M S A Z D Y A O

LNCO jY

L J Y V T N D B Q T Z W H X D Q C C G M O U R Y X W  
W M F G G W P X U L I A F V X B S L S A Y 3 T A G J  
15 8 18 16 23 10 26 16 10 2 4 1 8 9 9 1 16 18 14 2 6 15 3 6  
L U B I N G R I G H T S U P P O S E D F O U R L A R

MNCO kX

W C T B J P N R M F F O V L Z Q D V B Z Q A T O C Q Z  
G O U D S O F W D O S T O Y I L A Y D H Q F T X A R K X  
12 12 21 2 2 16 10 2 22 19 24 23 21 23 24 19 9 13 8 22 16 10 19 22  
C R U I S F R S T H R E E S M A L L C R U I S E

NNCO lQ

Z E W D K L W H H P V W A U T U N K A E I S J T B Z P  
X X O L R A U T A J W Y K S P U G E O X O M G X N W A  
12 18 9 4 13 24 5 5 6 20 6 14 13 4 2 8 2 5 12 15 6 12 14 13  
R S U R T E E N I N I T R O D U C E E D A N D T H R

PNCO mZ

P I L L V M K Q B O Y X J M H U K F H B G X S A H Z O  
W A Y X Y Q L T S X M M S W T G U D A K I T C N V G W D  
22 22 6 16 7 23 4 16 1 26 26 4 16 14 4 18 22 26 22 9 22 26 26 22 17 26  
F E M O N I T O R S S T O P T H E S E V E S S E L S

QNCO nZ

O I Q N M G M O G Y B W U H Y F K O T S P L I B O F  
W J E W O U L F N L I M A A S G R Z E V U L V R R N C J  
22 14 3 15 7 15 15 4 6 26 2 24 14 19 15 9 26 18 2 17 18 14  
H A V E E E N P O R C H A S E D O U T R I G H T A

ROCO oF

F E W K D Y A D X Z S N X L J Q W O S K U R L E O G L  
C F Q Q M H E P P G H R T I Y A E U J G Z R R B B Y V  
20 18 17 6 2 19 20 19 19 20 19 17 2 4 4 9 22 9 13 22 7 6 18 13  
C P B L T Z R Z C Z B T X U D T K D V A R E L O R

SPCO pG

L S V Z W W G O Y Q C W J S A D P S O Q U Y H D S U R  
Y Y S O A S T F K K U D Z W E M X Q I V E Z X O F E W  
10 4 10 7 15 11 10 10 16 20 4 5 12 22 9 4 24 5 6 11 3 10 4 3 26 16  
T S W O B A T T L E S H I P S O F D A N T O N C L

TDCO qR

R S E N X T M F T Q Y L O S W U M J L P V A Q K T  
S G T L G M Q J U N G P E C U W B N T G T H K Z  
10 26 26 8 13 4 13 26 17 15 17 5 4 26 13 4 10 9 8 11 2 26 16  
A S P U R C X A S E D F O R S C R A P P I N G Z M 9

62 out

DOVER

effective - key DOVFS

DOVFS &

L P I O U E Z K S J D X C A F E U K S D W H  
Z F A K N N H Y D X D W J P B X Z I N F M R  
W U S F O R C E O F T W F N T Y F I V E T H

EPVBO

R Y S N W A N I P U J M Z A H O U Y V U V O E C N B  
W D T T S D W W I O U R J L G S V T E Y G Y A Q O  
O U S A N O M E N E X F C U T I N G N O R T H

FQVBO

B S M P N L Q A P T A G G V H R M Z V B N Z I X P G  
R H C T Z Q E H J H J K Y F K V N D H J R P Q E Y O  
E N C I R E L I N G M O V E M E N T C H A N G S P O

GRVBO

B O L Y X B S S M B W L H V X V S P Z I K O G O O C C  
D W E K T W X N X X F D Y U A G Q O M G X U Z A R S  
S I T I O N V F C F N T Y O F R I V E R B E C A

HSVBO

C F E K X M R A L N V R S K A E S D S M T G R X S Y P  
J F P K V E C Y V G C Z L S G Y I Y U T R D O A N  
E U N T E N A B L E C H A Z G S A R M Y I S W I T H

ITVBO

P S M G S G Z B V D E N W Z S I V J E S V W Y J R G X  
R H B U D C V T Q N A Z J E I B A V J F I X G T X G  
D R A W I N G I N T O A Z C H U R I A F O R R E F

JUVBO

X E P I X V E J E B H I G S V P X X G A Z C Q C Z S  
E B W K Q J Q L X B E U L E A P X Y R R R O H Q V  
R G A N I N A T I O N W H E R E W U I N A L L P R

KVVBO

S F R I V W W D G V A H G H Q L V L M V B U S W X Y Z  
J X W P S T O G U H C K E Y J B L X E I Z M K E A  
A B I L I T Y W I L L N O T T F O L L O W F O R

LWVBO

Z H N W W T N K V B Z U Y R T P M R W P I C V Q Z P D  
S R O R E V T T X G P N I O O V M F S N N H H Y  
A R S C O M P L I C A T I O N S W I T H A P A N

MXVBO

D N X C E W Y R M H D W N P Z L W C C N X W T L V K G  
Q I V H S H C N A R Y B N K J D J K I A I W R J L Y  
D U R I N G W H O L E C O A M P A I G N W U W A R K

NYVBO

G K F E N T M E G L C U M E V K H Z Y N A H D S T J L  
V K G T F L K G D C P R Q Z B H N T I R M D X Y I U  
D A L L A M E R I C A N C I T I Z E N S T O L D E A V

PZVBO

L D H J B N I Q W N W A T I T L S J F U A R Y N W L E  
L T M S U I R Y X I M G O J G A A X R Q X M L T D  
E I M M E D I A T E L Y A N D S H O W E D G R E L T H

QAVBO

F K O S P S C F A Z W S N T Q Y B X Q M G G V A N  
J O F U E W Z Q G G Y C C O Z R F Y D T U I V  
P E R S O N A L B R A V E R Y R E M A R K A B L E

Handwritten notes and symbols on the right margin, including circled 'X' marks and other markings.

CUNEO #5 UE

REF ID: A4126886

HKWZARRPBQBI VY SMPDMQMYUDC  
 WSUEGFGGLBYDJCTJZUDCIELFO  
 SMITHSTATESCASESCONTAININ  
 EMZXDPIDLIAWWUBQMEZPIXISNH  
 HKNPIDSSGLCDVGDZYSWRFTRR  
 CONTRABANDWEREPOLINTE  
 RIQOWYINRCXYMXHJZCRHATHSBZ  
 ZYQJYKDAHFUQVXJCONROVZRR  
 ONM BYMAJORRSSNIVELYWHOST  
 PMLKVOUZRS AUGOHLTKOUZJECXL  
 DKATTLOHHDLYTOTJNUHYBUIDT  
 TETHATTHEYCONTAINEDHOUSES  
 SKDHWBILES KSWGZGPRUIQLHJJ  
 URNYVXD F D A F D P O R T Q A Q I T R K L  
 OLDG O O O O F H I S S T O P N E R F R U E  
 MKDQEUDKMIGEOJLRZDKNNPNYXY  
 JRNRLNRXRGMS S A M O C C I M N Y P C I  
 F D S M I T T L O K O U T F O R T H E M S T  
 HNMS SYWQDWDKVOBBGLUEBWMZXD  
 VULXYKXVTAVBHTCHSPAAMMFX  
 PSMITHSAIDNESAWSIMILARBOX  
 WKS AVUEASULCOGRQLZWUKIKTJZ  
 RRWETNNICRINS PNDORJBKSMBL  
 SINCOURSE OF CONS TRUCT ION I N  
 POWIXHLJBHFKBWVGGLAGGYICY  
 DHTABPBFVBFXCFEESTOUWXBUVE  
 ACKYARD OF SNIVELY SQUARTERS  
 VCJABXNDIWCCEMHGKQQDCB I G R I  
 PXPEWPZSFAGHTWJRGFGI QNTZ X W  
 NDSAWASIMILARBOXWITHHONECOR  
 AZEHOFORZFFJONFIVSMOQWTZIS  
 BBJYKRMGLVWYSGAMFLBZIMAXYT  
 NEROPENATPOLICIA BARRACKS I  
 WZLIEUEYZPBQEZIQG O P L Y W B T I X  
 BAALNNMIMCZTNLDSXVRJMOBV  
 THISBOXHERECOGNIZEDACASSEM  
 HQBXRZSIVZMCSPZ  
 VPUNDEAEXJTHGO  
 KEIDHAI GAN D H A I G

Underlined portions were incorrectly deciphered.

AGANA

Key: AGANA. REF ID: A4126886

4

~~(AGANA)~~ FSRUXMMFYEP  
WFLVYYZDXAXW  
NAVALCOUNCIL

J I U K X J S Q S G Z I R K S R Y L L R D Y C O V Z  
J U G P K O W R Y H G E H Z E K R L M O B W O Z J V  
N O W I N S E S S I O N T O K Y O T O D E T E R M I

O E E K A P N Z R Q B P O S S E P Q D X G D L T N A  
C E F P B E V D D T Y K O D E S P B Z Z S C Q X N W  
N E D E M A N D S A T P A C I F I C C O N F E R E N

O P R R N F O B Z I F L C K G M K C L M X L L J H V V  
C A X Y T N I V E R E D I L T B I L X Z O P F O J K  
C E P R A C T I C A L L Y A L L A G R E E R A T I O

O H U D H V O G A K D I C S C B E Y X M P Y I R D K  
C S G K Y Q I F F V R E E D G D T S Y Y T W W S F L M  
O F J A P A N E S E V E S S E L S T O U N I T E D S

K V J D W D O A L J Z C Q N M W T Y U O D Y Z C O E  
M M L K R M I E C S G D W C T C A S W V B W S P A C  
T A T E S N A V A L V E S S E L S M U S T B E S E V

S N W T S F Y C G P X V R V J C E Y F Y V L G W P K P Y  
Q Q P D V X M B H Z E G X S Y V T E X P X A X U X Z C O D T N X V C K X A  
E N T E N T H S O R T W O S H I P S T O T H R E E S

Y R M K Z O M C L G P C S O Z S C C A N P N X Y W Y Q  
B W H P A H L Z C H J D C P K F I J P I T K C X O X A O  
T O P D E C I D E D T O P U T I N R E S E R V E F O

K S K J H L L Z F N Z Q Y S B Z O L T I X M R U J U  
M R O M Y Z A D Q Y G V N D C L S L S M A A R D H D  
U R P R E D R E A D N A U G H T S S E V E N A R M O

Z A M P K Q A D B R B C O R P U G J I H K A J K L K  
W Y H C Q P D O W E Y D O I N T O A L K G S F J S L  
R E D C R U I S E R S F I V E C R U I S E R S A L L

M G S P E G R E S I F A I X Z Q F I W M A D U C E M  
F Z S C H D B K Y C S I F T K Z Y K F Y R C A P G E  
O L D S T O P N A V A L D E L E G A T E S W I L L B

V D A E S I E V O Z S O B H M Q N W N D U R G O L E  
T M J A H Y Z X M N G B O E F N K A D G F R I P T E X Y X Y C  
E Y I E A D M I R A L K A T O C A P T A I N S Y A

B G R U B H C V I Q U A U N G W  
O Z X H S W Y S B T O I Q C M C  
M A N A S H I A N D N A G A N O

The key as given was in error, it should have read AGANB instead of AGANA

NES  
BLOIS

E F G H I J K L M N O P Q R S T U V W X Y Z A B C D

REF ID: A4126886

BLOED l

P Z X X O Z W T S R S F F B X K H Y X B Y  
7 19 24 26 15 5 3 5 17 5 22 24 6 23 4 21 22 5 7 19 23  
C O M P L E T E G E R M A N F I R E C O N

CMOED m

J N I R N L I F K V O R A R B V Z U G V A C C N B T  
19 15 26 11 17 18 17 19 24 23 7 4 7 20 11 7 1 11 24 19 26 10 12 20 19 24  
T R O L S Y S T E M A V A I L A B L E T O U N I T E

DN OED w

Y L P C W T O L Q D V H A Z Z G Z P G J P F E R M Q  
18 1 16 25 16 6 1 11 5 7 18 14 7 6 5 16 1 25 24 6 1 9 1 16 6 20  
D S T A T E S F O R D I R E C T S A L E S Y S T E M

ED OED o

U D P K F K Q E M D S O D L M O K R T D U V C A N L  
12 6 16 23 13 15 10 22 23 7 12 20 9 22 7 5 9 26 21 3 20 20 12 9 7 22  
E M P L O Y S A L T E R N A T I N G C U R R E N T A

FPOED p

Z Q B O R W I U P F H Q O O G X M T M I J M V U B Z  
10 23 14 8 19 8 17 17 11 8 17 22 13 3 13 12 3 9 24 10 1 13 21 19 3  
N D H A S A C C U R A C Y T O T W O M I N U T E S O

GR OED g

G A H P N G Q R J F T L S I P N L W C K I E T H I K  
14 13 19 22 17 25 10 18 12 11 9 26 13 2 17 23 13 21 11 18 11 19 14 11 22 25  
F A R C S T O P G E R M A N S H A V E P E R F E C T

HR OED v

O S E R O I B J O P H X S V X G L Y U F Y A E L G K  
25 19 9 11 11 9 26 9 21 24 8 9 13 1 18 16 13 22 18 25 8 18 1 23 12 25  
E D A P P A R A T U S A L O N G L I N E S N O W B E

ISOED a

O L A L F V E F H R N Z D X I X Z K V B G I Q P M L  
25 1 21 24 13 11 13 19 15 3 13 24 9 8 21 13 11 13 12 16 19 13 19 13 6 22  
I N G D E V E L O P E D B Y G E N E R A L E L E C T

JTOED t

R Y H A Q H Q U G Q X O U K C M P A Q U R N Z E A C  
2 24 19 19 4 5 10 17 7 12 6 20 4 10 1 17 10 17 7 8 6 8 17 25 4 21  
R I C C O M P A N Y S T O P J A P A N E S E A B O U

KU OED w

X N T X I C L R S Z O A A P H B I K S D C H R Y R S  
15 15 23 16 23 22 16 18 6 2 7 22 7 4 23 15 3 13 15 3 23 22 24 17 23 1  
T T O C O N C L U D E N E G O T I A T I O N S F O R

LV OED w

W W D Y C Q S K K U B J I Q W Q F J H N U K Z U S D  
5 7 17 9 6 21 4 14 24 22 4 21 25 14 9 8 24 5 1 14 20 14 17 21 10 16  
P U R C H A S E O F S A M E S T O P G E N E R A L D

MWOED w

R I B N W M S C S F M N H Q D U P P U Q L U U R A H  
2 5 14 10 16 24 4 16 6 11 16 11 18 14 14 6 10 25 18 11 14 2 26 16 4 17  
E S C R I P T I O N I N A C C O R D A N C E W I T H

NX OED x

X I N G Q E D J M R W X X K R Y S V  
15  
M Y R E P O R T N U M B E R O N E

E F G H I J K L M N O P Q R S T U V W X Y Z A B C

NUTXHVZSLUMLZXHXHOHYDRCLMS  
 NHELXSEZEPRHKOHXJVLWKSOFTFR  
 RESSENEFHEUNITSDSAES  
 UFCDSUFMOVKCNKYNGAUWYL IQZ  
 LWMWLQOMWYFDBRGHRZJYS SX  
 UTLWBWDGOWKHXTCJCSVGJJFYV  
 DYSSVHMYFEJVOJBLKEUGH  
 CLEANPOLICIESCOMESLIKEABOMB  
 JSRCEZUQKDOYTVTCASNOQPGEC  
 TZXJUNWSDOOVKDLVHXIT  
 TOJAPANWHOWASPREPARED TOCONY  
 ARUCWLDDCUQDXFLCBKDBECHXDG  
 YIXTBPCUWUXLGHJPHN  
 SIDERREDUCTIONARMAMENTSOUTY  
 VAYEEUZHWRWVVPVDVMGENJWVUU  
 NAFJLEAXGZYZOEYDYSYLGLKEF  
 RESENTSDISCUSSIONASTATTEPR  
 ENMOQJPUMVKGWQCZWKRIIXMJAC  
 FSJHQHNPWYLBZINEEPDDIXT  
 OBLEMSASUNWARRANTEDINTERFE  
 LNSWEAMIAUVVWVBLEMBOSPXFRR  
 WSUSJENCHPGYBAELVYIXNWEHVW  
 RENEGREATESTBLOWTOPRIDEAN  
 SGOWCJLVMHYAJEZGFYBUDAZLOQ  
 SBGSYQCUPCNKXSMPAUIZDUITCI  
 DPREJUDICEIS INVITATIONTOCH  
 UMTZTOVTBDKWHACHYNYOBNPIHR  
 GLEBGJTJYSYAFMLITJYXMXSRW  
 INATOPARTICIPATEFOLLOWINGJ  
 TKSXFGWMNLNGOHYMKHPGWWEBEL  
 CPULOFOYZFBLQGRWEKTTJQBNIV  
 APANSFAILURETORENEWBRITESH  
 ABLZCJUC LJXSOU DLWUTAFIARTU  
 ZRYBYQMBEUSQTXLFXUSEQVUAE  
 ALLIANCEBRINGSHREALTZATTNO  
 SNGXAZBOHGWPGZRV  
 SSCLDDWLBZMPNMDX  
 FNATTONSISOLATION

A B C  
Z N  
X R  
A R

D E F G H I J K L M N O P Q R S T U V W X Y Z  
 S I I B X A R U N D E G X D Z M M Q X Y A Y T F G B  
 T X Y U N E E O A T O M V X N X Y E B X U Z Z I Z O  
 M Y G E N E R A L S T A F F C I R C U L A R I N G  
 E U Z W C L G R B M Q K T C C G H V P T F A B X D H  
 G I B T Z C H E Z R X A P I J O K F U W F V N G I T  
 A P A N E S E P R O P A G A N D A H E R E A N D C H  
 H U D X Z S P N O L Y V C T R E C G J S E A J L W T  
 U I M M D Y I Z N G O Z H Q M V L S E M A V I U O C  
 I N A S T O P U N I T E D S T A T E S M I L I T A R  
 P M L J B R Y O M C V T N P Q P Y D M N T S C P U F  
 C J Z P V D K M G E Y O E P B R U B A L X O R Z F I  
 Y A N D E C O N O M I C A L M E N A C E S T O P H E  
 E X V M N P X Q Y I I R F X Z Z G K G Z T C Y D V W  
 G K G L W H P U M F G J X W N O R G T S X Q A H M P  
 R I N T E R F E R E N C E E P T A A N D S I B E R  
 Q I A F M V D U F C L Q J A G C Z A B B D K T I U E  
 N X C O M I Q O T E H Y Y N P K P R J K E K Z T E F  
 J A C O M P E S J A P A N T O B U I L D A N M A  
 J Y W P O T P F G W L B X M M B D J V L F Q F Q W T  
 M F S F J I I S J Z H C V V W G A D G Q F I H K O C  
 N T A I N N A V Y B E Y O N D M E A N S S T O P N I  
 P X D J K B X C N I F S C M G S T G B T O R E M T E  
 C K M P T W P C A F V E M V P I T S J W Z T C F B X  
 E L I N G T O M A K E S O M E R E D U C T I O N B U  
 K L H C C U P D Q X C P T F O B L M V Y Z R I R M V  
 P Y W Y Z M I R V S E N P Y T G N Z G X T T S V G N  
 T M U S T R E T A I N N A V A L S U P R E M A C Y  
 H D G G H V T F W Q R Q F H K H N L X Q J I T N C S  
 U L D E Y T I S Y W I Y X H D J I O B G G R Z P T  
 F W E S T E R N H E M I S P H E R E P R E V E N T A  
 G S N S E J Q W R B I U K V G T O V E T B W P L C U  
 B U W K R T X G A G S O B P S V Y Y W L L Y U T  
 M E R T C A F E K O M E V E R T N T E R F E R I N G  
 Y C X Q T B P J D M U S I R O K Y M A D O B V U P Z  
 E W L Q H W I T S R R F I L T E U Z S D Z M K E A Y  
 N T H E T R D O T N G S T N T H I S P A R T O F T H  
 M B K H V B  
 I S R X S W  
 E W A R L D

BL015#3

P Z X X O Z W T S R S F F B X K H Y X B Y  
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17

J N I R N L I F K V O R A R B V Z U G V A C C N B T  
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Y L P C W T O L Q D V H A Z Z G Z P G J P F E R M Q  
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

U D P K F K Q E M D S O D L M O K R T D U V C A N L  
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Z Q B O R W I U P F H Q O O G X M T M I J M V U B Z  
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

G A H P N G Q R J F T L S I P N L W C K I E T H K  
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

O S E R O I B J O P H X S V X G L Y U F Y A E L G K  
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

O L A L F V E F H R N Z D X I X Z K V B G I Q P M I  
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

R Y H A Q H Q U G Q X O U K Z X P A Q U R N Z E A C  
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

X N T X I C L R S Z O A A P H B I K S D C H R Y R S  
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

W W D Y C Q S K K U B J I Q W Q F J H N U K Z U S D  
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

R I B N W M S C S F M N H Q D P U E D Z R K U R A H  
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

X N G Q E D J M R W X X K R Y S V  
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

K I E R L Q T Q H A U V C M T J F  
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

BL015-#3

AF

CH



B J E N F C A D D A Y G K N S T R B H W L U K J P Q  
 P L G T N Y E P Q H M K Z D F Y M G K H P A J H Y K  
 Z E P P L I N C O M P A N Y A C C E P T A T I O N  
 U Q I S A H S V I H S W D T I D Y A B J G T K K M Y  
 F M W U C X X T C B B Z U O I X S P H D T W J K E B  
 E R A L C O M P R E S S I O N R E Q U I R E M E N T  
 X O L D Y N V H C B Q T J O N I Y X J M J D O D T B  
 H E X L G V S Z B Y V M W Q E J S Y C Z E D Z F Z O  
 S A N D A R E A N X I O U S T O P P R O C E E D A S S  
 L R K S N Z K M K P X U S U D S O C R J I Y A T X J  
 V X P U U C T N Y J R Q D S W G T K O D O X U Y F J  
 D O N A S P O S S I B I L I T Y H E Y P R O P O S  
 X M R W F Z H E B B Z E B X F F W H P F V Y H F V  
 H H Y F S O D Z M Y Z I C V Y Z F K T D H Y P H L  
 E S E V E R A L M O D I F I C A T I O N S W H I C H  
 B S A G B T A L Z U G G E X A X A K X Y I H H N E T  
 P S A C T G E C F O J K G U M W O F Z V O N O N H A  
 D E P A R T M E N T S H O U L D C O N S I D E R X A  
 D T L L O W U O A I N H N J W Y B P T A Y I D G J B  
 I C X Y H T L K G D A D C X C R F R T R W P E W I  
 N D W H I C H A R E I N M A T E M A N W H I C H  
 N U V J L Y T G F C D N F Q J P L X T J C J R P H K  
 G O N Z H H G R C S B V Y P L Y D N F S X Q M  
 W E P R E S E N T G E R M A N L A W M U S T B E A M  
 Z G G V J M X F M C Z T Q K Z S T F H S W O U D T R  
 X A B P O L N Q U C H M X A L G R A K K I Y B F Z V  
 E N D E D O Y G E R M A N L E G I S L A T U R E B E  
 Z L U P J T Y B G J C P O N X Y A Q Y H H M C W M W  
 R W H D O G I W H T I L P D V R O C U L M B P L E N  
 F O R E Z E P P L I N C O M P A N Y C A N P R O C  
 Y B H I W I V O Z H H J K E O W Y I C E A C Y Y O Q  
 C Q U X S Z S K F B C V Z R R D S L L X S O Y Z B K  
 E D S T O P T A M T O L D T H A T T H I S A M E N D  
 V G W C S F S Z U E N J Q I O P D J F U C U B T O Y  
 M A Q W Y O X E N N A V X H S P Y B B Y N A L Y B  
 M E N T C A N N O T A R E E F F E C T E D U N D E R  
 W P Z A Q S T M K G I H G Z  
 O B Z B P W H N Y I E D L K  
 W O R T H R E E W E E K S

50  
 70  
 80  
 90  
 100  
 110  
 120  
 130  
 140  
 150  
 160  
 170  
 180  
 190  
 200  
 210  
 220  
 230  
 240  
 250  
 260  
 270  
 280  
 290  
 300  
 310  
 320  
 330  
 340  
 350  
 360  
 370  
 380  
 390  
 400  
 410  
 420  
 430  
 440  
 450  
 460  
 470  
 480  
 490  
 500  
 510  
 520  
 530  
 540  
 550  
 560  
 570  
 580  
 590  
 600  
 610  
 620  
 630  
 640  
 650  
 660  
 670  
 680  
 690  
 700  
 710  
 720  
 730  
 740  
 750  
 760  
 770  
 780  
 790  
 800  
 810  
 820  
 830  
 840  
 850  
 860  
 870  
 880  
 890  
 900  
 910  
 920  
 930  
 940  
 950  
 960  
 970  
 980  
 990

H-R  
 J E  
 W K  
 #2



SECRET

CONFIDENTIAL

REF ID: A4126886

DATE 11 April 47

TO	FROM	TO	FROM
Chief, ASA.....(10)		Ch, Security Div.....(80)	
Executive O.....(11)		Tech Staff.....(81)	
Co'r Joint Oper....(12)		Ch, Materiel Br....(82)	
Deputy Chief, ASA... (20)		Ch, Methods Br....(83)	
Dir, Comm Res....(14) ✓		Ch, Protective Br... (84)	
Ch, Pers Sec.....(21)		Ch, Maint Br.....(85)	
Ch, Org & Tng Sec..(22)		Ch, Res & Dev Div..(70)	
Ch, Plans & Oper... (23)		Tech Staff.....(71)	
Ch, Materiel Sec....(24)		Ch, Ch. Ciph & Cif Br(72)	
Ch, Fiscal Sec.....(25)		Ch, Int Equip Br... (73)	
Adjutant, ASA.....(26)		Ch, Elec & Elec Br. (74)	
Ch, Sec Cont Sec... (27)		Ch, Lab Serv Br....(75)	
✓ Ch, Operations Div..(90)		Ch, C'logic Br.....(76)	
Ch, Lab Br.....(91)		Ch, Pers & Tng Br... (61)	
Ch, Machine Br....(92)		Ch, Supply Br.....(62)	
Ch, Crypt Br.....(93)		Co, Arlington Hall....(40)	
Ch, Int Cont Br....(94)			
Ch, I & D Br.....(95)			
Tech Staff.....(96)			

- Approval & Return
- As Requested
- Concurrence or Comments
- Information & Forwarding
- Information & Return
- Information & File
- Recommendation
- Signature if approved
- Your action by
- Info upon which to base reply

Pre look this over at your earliest convenience + then call me. I think this is a good way to go at the problem.

You might suggest rearrangement of the order of the enclosures - I am not sure its the best as I have it now.

7

~~SECRET~~

1st Ind

William F. Friedman, WDGAS-14 11 April 1947

TO: Chief, Army Security Agency

1. Reference is made to paragraph la of the inclosure to the basic letter. In view of the interpretation made of the meaning of that paragraph, as set forth in ASA Memorandum dated 10 April 1947, Subject: "Procedure for Release of Information Concerning Secrecy Patents", information is requested as to the bearing that interpretation has on the question dealt with in the basic letter in regard to the status of Patent Application No. 443320. It is also requested that clarification be made as to what rights, if any, the inventors may have in regard to Patent Application No. 443320 under paragraph lb of the policy directive forming Inclosure 1 to basic letter, in the light of the recent interpretation of the meaning of paragraph la thereof.

2. This indorsement is submitted on the premise that it would be to the advantage of the Army Security Agency, the War Department, and the Government as a whole, as well as to the inventors as individuals, to seek some clarification of the rights of inventors of equipment which must be safeguarded and held in a classified status for a relatively long period of time, since a clarification of this point might assist in formulating

~~SECRET~~

~~SECRET~~

a policy which would be most conducive to the stimulation of invention by Army Security Agency personnel.

3. In connection with the foregoing, there are submitted herewith, as information pertinent to the circumstances, <sup>nine</sup> in-closures listed below.

4. This matter has been discussed with Mr. F. B. Rowlett, co-inventor in the case of Patent Application No. 443320, and this indorsement is submitted on behalf of both inventors.

9 Incls

WILLIAM F. FRIEDMAN

1. Ltr dtd 27 Jan 47 to President  
frm Acting Secretary of War  
w/incls-3
2. Cy of Memo for Record, dtd 19  
December 46, Subj: Conference  
on Proposed Patent Policy
3. Cy of Brief <sup>by</sup> Chief of the *dtd 10 March 47*  
Patents and Inventions Br,  
Legal Div., OCSigO
4. Cy of Memo for Judge Advocate  
General, dtd 14 Apr 44
5. Cy of 2nd Ind from JAGO to  
Asst. Sec. of War, dtd 17 Jan 36
6. Cy of 2nd Ind from JAGO to Adj.  
General, dtd 19 Apr 35
7. Cy of Brief <sup>by</sup> Chief of Patents *dtd 15 Feb 47*  
and Inventions Br., Legal Div.,  
OCSigO
8. Cy of ltr from Patents & Inven-  
tions Council, Legal Div., OSCigO,  
dtd 10 June 46 to Mr. W.F.Friedman
9. Cy of ASA Memo dtd 10 Apr 47,  
Subj: Procedure for Release of  
Info. Concerning Secrecy Patents

~~SECRET~~



~~SECRET~~

REF ID: A4126886



HEADQUARTERS  
ARMY SECURITY AGENCY  
WASHINGTON 25, D. C.

WDGSS-23

20 May 1946

SUBJECT: Release of Patent Application Serial No. 443,320

TO: Mr. William F. Friedman, WDGSS-14

1. Reference your letter dated 27 September 1945, subject as above, the attached memorandum from the Acting Deputy Assistant Chief of Staff, G-2, outlines the War Department policy on the release of cryptographic principles.

2. Analysis of the policy would indicate that:

a. Patent application No. 443,320 will not be released unless it can be shown that the employment of the principles involved are susceptible to cryptanalysis under all circumstances; and

b. If not released, a request for purchase of all commercially exploitable reversionary rights may be entertained provided it can be shown that Frank B. Rowlett and yourself were not directed or employed to experiment on or to invent the principles or improvements embodied in Converter M-228 or Converter M-294.

3. If it is felt that subject Patent Application should be released under (a) above; or if and when it is felt a case should be presented for purchase of rights in conformity with stipulations contained in (b) above, an application for release or purchase, containing pertinent facts and necessary proofs, may be prepared and submitted to the Director of Intelligence through the Chief, Army Security Agency.

1 Incl  
Cy ltr dtd 29 Apr 46,  
subj: "Release of Cryptographic Principles"

*Harold G. Hayes*  
HAROLD G. HAYES  
Colonel, Signal Corps  
Chief, Army Security Agency

~~SECRET~~

~~SECRET~~

29 April 1946

MEMORANDUM FOR THE CHIEF, ARMY SECURITY AGENCY:

SUBJECT: Release of Cryptographic Principles.

1. The following policy is announced to be effective immediately:

a. Cryptographic principles or devices developed by officers, enlisted men, or civilians employed in any War Department Agency, or patents or patent applications on such principles or devices which are owned by, assigned to, or licensed for use of the War Department will not be released for use of foreign governments or for foreign or domestic commercial or private use until such time as necessary information is available and a procedure established in the Army Security Agency whereby information which is cryptographed by means of such principles or devices can be cryptanalyzed and read under any and all circumstances.

b. Where it is in the interest of the Government of the United States that an employee have no patent rights in cryptographic principles or devices to dispose of, and for the Government to own the entire interest for security reasons throughout any foreseeable future; and where discovery or invention of cryptographic principles or devices has been made by a civilian employee and does not relate to a matter as to which the employee was specifically directed to experiment with a view to suggesting improvements nor was produced as a result of any specific employment or contract to invent a specific device or article; and where an application for patent on such principles or devices has been filed with an assignment-in-trust to the Government for the purpose of maintaining such application in secrecy, the Military Intelligence Division will support, subject to the availability of appropriations, any reasonable request for purchase of all commercially exploitable reversionary rights of the inventor in the patent application.

/s/ CARTER W. CLARKE  
Colonel, GSC  
Acting Deputy A.C. of S., G-2

~~SECRET~~

OSGAS

SUBJECT: Patent Application Serial No. 443,320

TO: The Judge Advocate General  
Department of the Army  
ATTN: Chief, Patents Division

FROM: Director of  
Intelligence

DATE: 19 Feb 48 COMMENT No. 4  
Capt. Rambo/147 Ext 462

1. With reference to the request contained in Comment No. 2, a search of the files of the Army Security Agency fails to reveal the specific evidence upon which the Signal Corps Patent Board based its decision regarding subject patent application.

2. The following information from the files of the Army Security Agency is submitted as evidence which may have been considered by the Signal Corps Patent Board in reaching its decision.

3. Mr. Friedman has been a civilian employee of the Department of the Army since 31 December 1921. His duties as described in the original appointment were: the compilation and preparation of all methods for secret correspondence to be used in the Army; the supervision of instruction of commissioned personnel in the proper use of codes and ciphers; preparation of instructions and papers on such subjects; and compilation of special problems for instruction purposes (Inclosure 2). Formal job descriptions of the type currently in use for civilian employees were not initiated within the OCSig until 1942 and therefore no such formal job descriptions are available for periods before 1942. However, in the case of Mr. Friedman, written indications of his duties in a form somewhat equivalent to that followed in the currently used job descriptions were found for the years 1930 and 1942. In 1930, Mr. Friedman's job was designated as that of "Principal Cryptanalyst," P-6, and in the year 1942 this title was changed to read "Head Cryptanalyst," P-7, concomitant with a promotion to the next grade (Inclosure 2). Mr. Friedman has held a comparable position since his original appointment under Section 10, Rule II, on 30 December 1921. The responsibilities of the position have greatly increased with the growth of the Army Security Agency, but the basic duties of the position are essentially those for which he was originally appointed (Inclosure 2).

4. Mr. Rowlett was appointed "Junior Cryptanalyst," P-1 in the year 1930. His duties were largely of an independent nature, under the general supervision of "Principal Cryptanalyst," Mr. Friedman. As in the case of Mr. Friedman, his duties remained relatively the same through the years, although his title changed in accordance with his promotions. Descriptions of the duties performed by Mr. Rowlett for the years 1936 and 1941 are inclosed (Inclosure 3). No written descriptions of the work performed by Mr. Rowlett are available between these years for reasons cited in the case of Mr. Friedman, paragraph 3 above.

5. Relative to the rights of Mr. Rowlett in the subject invention, he has been contacted personally and states that he has full knowledge of his rights in the matter and that he concurs fully with the action being taken by Mr. Friedman.

FOR THE DIRECTOR OF INTELLIGENCE:

COPIES FURNISHED:

- AS-71F
- Mr. Friedman
- Mr. Rowlett

3 Incls

- 1. n/c
- Added 2 Incls

- 2. Job info on Mr. Friedman
- 3. Job info on Mr. Rowlett

HAROLD G. HAYES  
Colonel, Signal Corps  
Chief, Army Security Agency

FEB 20 1948  
SIGNED AND SENT OUT



SUBJECT: Patent Application Serial No. 443,320

TO: JAG

FROM: D/I, GSUSA

29 DEC 1947    COMMENT  
Colonel McGarr/6967/rsr

1. Mr. William F. Friedman, a civilian government employee of the Army Security Agency, Intelligence Division, has requested certain information on which to prepare a case looking towards disposition to the Government of all commercially exploitable reversionary rights as an inventor in the subject patent application.
2. The policy of the then War Department, A. C. of S., G-2, as announced 29 April 1946 (Tab B-1 of Incl " ), is that where it is in the interest of the Government an employee have no patent rights for security reasons in a device he has not specifically directed to invent, the ID will support any reasonable request for purchase of commercially exploitable reversionary rights of the inventor.
3. The Signal Corps Patent Board has rendered a decision that the subject invention was not the result of " - - - specific designation to invent - - - ", Tab B-1 to Incl 5.
4. It is considered that the secrecy order now standing against the subject application must be continued (Incl 4).
5. From a legal viewpoint, information is requested on the actions to recover outlined in paragraph 2 a and b of subject letter 8 December 1947 by Mr. Friedman, and the manner in which final action should be accomplished.

FOR THE DIRECTOR OF INTELLIGENCE:

1 Incl  
Ltr dtd 8 Dec 47  
w/incls (5)

/s/ Bruce W. Bidwell  
BRUCE W. BIDWELL, Col, GSC  
Assistant Executive

---

FILE No. JAGP 1948/103-S (5 Jan 48)	SUBJECT As above		
TO	FROM	DATE	COMMENT NO. 2
Chief Signal Officer	Patents Division,	7 JAN 1948	Col. G. W. Gardes/6822
ATTN: Mr. Pernice, Chief, JAGC Legal Division.			

Reference is made to paragraph 3, Comment No. 1, which states that the Signal Corps Patent Board has rendered a decision that the subject invention was not the result of "specific designation to invent". It is requested that this office be advised of the underlying facts determined by the Board in connection with the employee's status and assignment, including his job designation, which resulted in above decision.

FOR THE JUDGE ADVOCATE GENERAL:

ncl: n/c

/s/ George W. Gardes  
GEORGE W. GARDES, Col, JAGD  
Chief, Patents Division

SIGLG-3HMS (29 Dec 47) Patent Application Serial No. 443,320

TO: Chief, Army Security Agency From: Legal Div., OSCigO Date: 15 Jan 48 COMMENT NO. 3  
Washington 25, D. C. Saragovitz/73720  
Att: Mr. Stauffer

1. In accordance with telephone conversation 14 January 1948 with Colonel Gardes, JAG Patents Division, the inclosed correspondence is forwarded for your direct reply for the reason that subject patent application is now being prosecuted and is under the general jurisdiction of the Army Security Agency, and also because the joint inventors are now employees of the Army Security Agency.

2. A search of the files in this Office failed to reveal any written or documentary evidence upon which the Signal Corps Patent Board based its decision that the subject invention was not the result of specific designation to invent.

3. It is noted that the other joint inventor, Mr. Rowlett, has not entered into the question being raised by Mr. Friedman. It is believed that the rights of Mr. Rowlett in the subject invention must also be taken into account in this matter.

FOR THE CHIEF SIGNAL OFFICER:

Incl. n/c

/s/ J. E. Pernice  
JOHN E. PERNICE  
Chief, Legal Division

~~SECRET~~

CSGAS-14

25 September 1947

## MEMORANDUM FOR RECORD

1. Pursuant to an invitation from Captain Safford to participate in a meeting with engineers from Teletype Corporation, the undersigned, accompanied by Dr. Kullback and Dr. Sinkov went to Captain Safford's office at 1000 hours on 9 September 1947.

2. Captain Safford explained that the Teletype engineers were delayed and that he really did not know why they were coming or whether they were bringing any model or models.

3. While waiting for the Teletype engineers to appear, Captain Safford demonstrated two recently completed developments of his own laboratory:

a. A modification of Converter M-228 (SIGCUM) to be known as CSP-3300. This equipment is designed to give improved security for SIGCUM usage especially in connection with the transmission of intercept traffic for OP-20-2. The modified machine eliminates the 131 mixing cabinet and uses relays mounted underneath the frame of the SIGCUM for this purpose. These relays also are used in connection with a baud transposition feature so that the plain text bauds undergo transposition before Vernam-rule substitution. The motion of the rotors has also been modified, with the introduction of reversed stepping in the case of two of the five rotors as an added feature. Off-line (tape) operation was demonstrated but it was my understanding that provision has been or will be made for on-line operation also. This machine is worth ASA's study; however, it will only operate from tape and hence its application is limited.

b. A modification of SIGABA for the production of one-time key tapes. The output of the cryptographic rotors is reduced to 5-unit code symbols. The control and cryptographic rotors are subjected to a different motion control than in SIGABA. The purpose of this equipment is to permit local stations to produce "one-time tapes" from machine settings, so as to have the equivalent of "one-time" intercommunication among a large number of stations when conditions permit.

~~SECRET~~

~~SECRET~~

Otherwise, the one-time tapes can be produced by a central station and distributed to users by courier, as is normally the case. Captain Safford claims that the output is perfectly random. This machine also should be investigated by ASA.

4. Since the noon hour was approaching and the Teletype engineers had not yet arrived, the ASA representatives left, with the statement that other representatives would replace them for a meeting at 1400.

5. The other ASA representatives, Messrs. Rosen and Barlow from AS-70 and Messrs. Kuhn and Brann from AS-80 attended the conference in the afternoon. Mr. Rosen reported to me that the Teletype engineers brought nothing with them, stating that the model of the HOCM would not be completed until sometime in November. The project is apparently not going forward as had been anticipated.

6. The ASA representatives were then shown the model of CSP-3300 discussed under Paragraph 3a above. Mr. Rosen reports that he regards the equipment as too complex, that it uses relays which will not stand up under ordinary usage, and will not perform the functions required of the Converter MK-519()/TG. Mr. Brann, having read the foregoing, makes the following comments:

"It might be noted that Navy is placing the greater emphasis upon modification of existing equipments instead of development of new ideas. It is believed the CSP 3300 will cause very awkward operational practices in that transmission and encryption will have to be on-line with reception on-line and consequent decryption off-line. This method of operation would not be acceptable to any of the Army using services."

Mr. Kuhn adds the following:

"In addition to the remarks made by Mr. Brann in connection with the CSP 3300 I believe it might be more economical in the end to build a complete new unit rather than attempt to convert the M-228 unit. The work involved would exceed that now being done to convert a SIGABA to a SIGROD."

WILLIAM F. FRIEDMAN  
Chief, Communications Research  
Ext 215

~~SECRET~~

A means of providing an irregular wheel movement  
in Cipher Machine using cipher wheels.

The basic principle of this invention utilizes the cipher wheels of the cipher machine to provide an irregular selection of the particular wheel which is to be moved. A method of effecting this selection is to provide, in addition to the present ring of 26 contacts on each face of the wheel, a second ring of 26 contacts, which contacts are independent of the first mentioned set of contacts, but are connected to each other in an irregular manner, analogous to the manner in which the first mentioned set of contacts are connected. Also the end plates will bear a double ring of contacts which coincide exactly with the two rings of contacts on the face of each cipher wheel. These two rings of contacts on each end plate are connected as indicated in Figs. 1 and 2 of the attached drawing.

The action of the machine is as follows: when a key is depressed, two contacts are closed, namely, (1) the key contact which allows a current to pass through one of the above-mentioned rings of contacts to operate an indicating device giving the encipherment of the letter corresponding to said key and (2) a universal contact which permits current to enter at a single contact of the other of the aforementioned rings of contacts on one of the end plates, pass through one of the contacts of the corresponding rings of contacts of all the cipher wheels, and pass out at one of the contacts on the corresponding ring of contacts of the other end plate, and thence to a selecting magnet which permits the cipher wheel corresponding

thereto to move forward.

Figure 1 is a schematic diagram of the invention. 1, 2, 3, 4, and 5 are the hereinbefore described cipher wheels; 19 and 20 are the end plates, 6, 7, 8, 9, 10 are the wheel selector magnets which allow a mechanism to step one of the wheels forward at each depression of a key; 11 and 13 are the rings of contacts through which the current passes to the wheel selector magnets; 12 and 14 are the rings of contacts through which the "key to lamp" current passes; 15 is the key contact; 16 is the above-mentioned universal bar contact; 17 is the source of power; 18 the reversing switch; 21 is the indicating device; and 22 is the connection to the universal contact which may be connected to any contact of the rings of contacts 11 on end plate 19.

Fig. 2 shows one manner in which the ring of contacts on end plate 20, through which the current passes to the selector magnets, are connected to the wheel selector magnets.

A means of providing an irregular wheel movement in  
Cipher Machine of the Hebern and *using cipher wheels.*  
Enigma type.

The basic principle of this invention utilizes the cipher wheels of the cipher machine to provide an irregular selection of the particular wheel which is to be moved. A method of effecting this selection is to provide, in addition to the present ring of 26 contacts on each face of the wheel, a second ring of 26 contacts, which contacts are independent of the first mentioned set of contacts, but are connected to each other in an irregular manner, analogous to the manner in which the first mentioned set of contacts are connected. Also the end plates will bear a double ring of contacts which coincide exactly with the two rings of contacts on the face of each cipher wheel. These two rings of contacts on each end plate are connected as indicated in Figs. 1 and 2 of the attached drawing.

The action of the machine is as follows: When a key is depressed, two contacts are closed, namely, (1) the key contact which allows a current to pass through one of the above-mentioned rings of contacts to operate an indicating device giving the encipherment of the letter corresponding to said key and (2) a universal ~~key~~ contact which permits current to enter at a single contact of the other of the aforementioned rings of contacts on one of the end plates, pass through one of the contacts of the corresponding rings of contacts of all the cipher wheels, and pass out at one of the contacts on the corresponding ring of contacts of the other end plate, and thence to a selecting magnet which permits the cipher wheel corresponding

thereto to move forward.

Figure 1 is a schematic diagram of the invention. 1, 2, 3, 4, and 5 are the hereinbefore described cipher wheels; 19 and 20 are the end plates, 6, 7, 8, 9, 10 are the wheel selector magnets which allow a mechanism to step one of the wheels forward at each depression of a key; 11 and 13 are the rings of contacts through which the current passes to the wheel selector magnets; 12 and 14 are the rings of contacts through which the "key to lamp" current passes; 15 is the key contact; 16 is the above-mentioned universal bar contact; 17 is the source of power; 18 the reversing switch; 21 is the indicating device; and 22 is the connection to the universal <sup>contact</sup> ~~bar~~ which may be connected to any <sup>contact</sup> ~~one~~ of the rings of contacts 11 on end plate 19.

Fig. 2 shows <sup>one</sup> ~~the~~ manner in which the ring of contacts on end plate 20, through which the current passes to the selector magnets, are connected to the wheel selector magnets.



A means of providing an irregular wheel movement in ~~Cipher Machine of the Hebern and~~ *using a cipher wheel*  
~~Enigma type~~ *of the type employed in the*  
~~Hebern cipher machine~~

The basic principle of this invention utilizes the cipher wheels of the cipher machine to provide an irregular selection of the particular wheel which is to be moved. A method of effecting this selection is to provide, in addition to the present ring of 26 contacts on each face of the wheel, a second ring of 26 contacts, which contacts are independent of the first mentioned set of contacts, but are connected to each other in an irregular manner, analogous to the manner in which the first mentioned set of contacts are connected. Also the end plates will bear a double ring of contacts which coincide exactly with the two rings of contacts on the face of each cipher wheel. These two rings of contacts on each end plate are connected as indicated in Figs. 1 and 2 of the attached drawing.

The action of the machine is as follows: When a key is depressed, two contacts are closed, namely, (1) the key contact which allows a current to pass through one of the above-mentioned rings of contacts to operate an indicating device giving the encipherment of the letter corresponding to said key and (2) a universal ~~is~~ contact which permits current to enter at a single contact of the other of the aforementioned rings of contacts on one of the end plates, pass through one of the contacts of the corresponding rings of contacts of all the cipher wheels, and pass out at one of the contacts on the corresponding ring of contacts of the other end plate, and thence to a selecting magnet which permits the cipher wheel corresponding

thereto to move forward.

*as applied to a Helium  
type machine.*

Figure 1 is a schematic diagram of the invention, 1, 2, 3, 4, and 5 are the hereinbefore described cipher wheels; 19 and 20 are the end plates, 6, 7, 8, 9, 10 are the wheel selector magnets which allow a mechanism to step one of the wheels forward at each depression of a key; 11 and 13 are the rings of contacts through which the current passes to the wheel selector magnets; 12 and 14 are the rings of contacts through which the "key to lamp" current passes; 15 is the key contact; 16 is the above-mentioned universal bar contact; 17 is the source of power; 18 the reversing switch; 21 is the indicating device; and 22 is the connection to the universal bar <sup>contact</sup> which may be connected to any one of the rings of contacts 11 on end plate 19.

Fig. 2 shows <sup>one</sup> the manner in which the ring of contacts on end plate 20 through which the current passes to the selector magnets are connected to the wheel selector magnets. ~~These of course are~~ *These*

*connections may be made at random and the*  
*keys may be composed of any number of*  
*each contact.*

*A random selection of these contacts may be made for connection to the contacts wheel selector magnets. Also current may enter at one or more <sup>contacts</sup> points on the opposite end plate, effecting a movement of one or more wheels per cycle.*

A means of providing an irregular wheel movement in Cipher Machine of the Hebern and Enigma type.

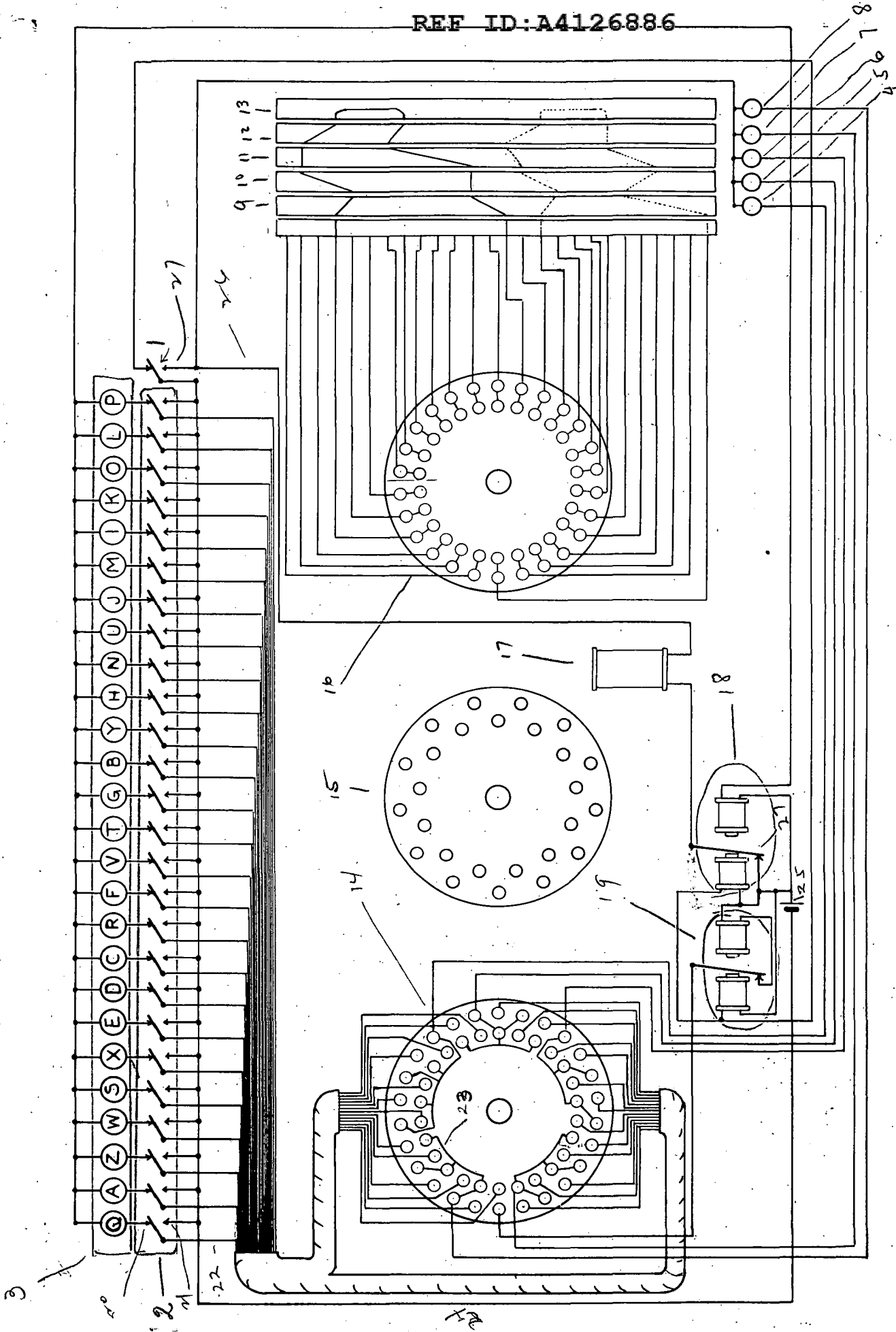
The basic principle of this invention utilizes the cipher wheels of the cipher machine to provide an irregular selection of the particular wheel which is to be moved. A method of effecting this selection is to provide, in addition to the present ring of 26 contacts on each face of the wheel, a second ring of 26 contacts, which contacts are independent of the first mentioned set of contacts, but are connected to each other in an irregular manner, analogous to the manner in which the first mentioned set of contacts are connected. Also the end plates will bear a double ring of contacts which coincide exactly with the two rings of contacts on the face of each cipher wheel. These two rings of contacts on each end plate are connected as indicated in Figs. 1 and 2 of the attached drawing.

The action of the machine is as follows: When a key is depressed, two contacts are closed, namely, (1) the key contact which allows a current to pass through one of the above-mentioned rings of contacts to operate an indicating device giving the encipherment of the letter corresponding to said key and (2) a universal bar contact which permits current to enter at a single contact of the other of the aforementioned rings of contacts on one of the end plates, pass through one of the contacts of the corresponding rings of contacts of all the cipher wheels, and pass out at one of the contacts on the corresponding ring of contacts of the other end plate, and thence to a selecting magnet which permits the cipher wheel corresponding

thereto to move forward.

Figure 1 is a schematic diagram of the invention. 1, 2, 3, 4, and 5 are the hereinbefore described cipher wheels; 19 and 20 are the end plates, 6, 7, 8, 9, 10 are the wheel selector magnets which allow a mechanism to step one of the wheels forward at each depression of a key; 11 and 13 are the rings of contacts through which the current passes to the wheel selector magnets; 12 and 14 are the rings of contacts through which the "key to lamp" current passes; 15 is the key contact; 16 is the above-mentioned universal bar contact; 17 is the source of power; 18 the reversing switch; 21 is the indicating device; and 22 is the connection to the universal bar which may be connected to any one of the rings of contacts 11 on end plate 19.

Fig. 2 shows the manner in which the ring of contacts on end plate 20 through which the current passes to the selector magnets are connected to the wheel selector magnets.



A means of providing an irregular wheel movement in cipher machines of the Hebrun ~~type~~ and Enigma type.

The <sup>basic</sup> principle of this invention is ~~to~~ utilizes the cipher wheels of the Hebrun cipher machine to provide an irregular selection of the particular wheel which is to be moved. A method of effecting this selection is to provide, in addition to the present ring of 26 contacts on ~~the~~ face of the wheel, a second ring of 26 contacts, which contacts are independent of the first ~~set of~~ ~~or~~ first mentioned set of contacts, but are connected to each other in an irregular manner, analogous to the manner in which the first mentioned <sup>set of</sup> contacts are connected. Also the end plates, ~~providing a means of~~ will bear a double ring of contacts.

which coincide exactly with the two rings of contacts on the face of each cipher wheel. These two rings of contacts on each end plate are connected as indicated <sup>total fig 1 of 2 of the</sup> ~~in the description thereof which follows.~~ <sup>the attached drawing</sup>

¶ The action of the machine will be as follows: When a key is depressed, two contacts are closed, namely (1) the key contact which ~~will~~ allows a current to pass through <sup>one of the</sup> ~~one of the~~ <sup>above mentioned</sup> rings of contacts to operate an indicating device giving the encipherment of the letter corresponding to said key and <sup>has</sup> a universal contact which permits current to enter at a single contact <sup>of the other of the aforementioned rings of contacts</sup> on one of the end plates, pass through <sup>each of the contacts of the</sup> the corresponding rings of contacts of all the cipher wheels, and <sup>pass out</sup> ~~exit~~ at <sup>the corresponding</sup> contacts on the other end plate, and thence to a selecting magnet which permits the cipher wheel corresponding thereto ~~to~~ to move ~~over~~ forward.

Figure 1 as a schematic diagram of the invention. 1, 2, 3, 4, and 5 are the herebefore described cypher wheels; 19 and 20 are the end plates, 6, 7, 8, 9, 10 are the wheel selector magnets which allow a mechanism to step one of the wheels forward at each depression of a key; 11 and 13 are the rings of contacts through which the wheel stepping selector magnets; 12 and 14 are the rings of contacts through which the "key test lamp" current passes; 15 is the key contact; 16 is the above-mentioned universal bar contact; 17 is the source of power; 18 the reversing switch; and 21 is the interesting device; and 22 is the connection to the universal bar which may be connected to any one of the paper contacts ring of contacts on end plate 19.

Fig 2 shows the manner in which the ring of contacts on end plates 20 are connected to the wheel selector magnets.

current passes to the selector magnets



WAR DEPARTMENT  
 Office of the Chief of Air Service  
 Patents Section  
 Munitions Building, Washington, D. C.

(Use separate sheet for each invention)

FOLLOW INSTRUCTIONS ON BACK

(a) Inventor: W. F. Friedman F B Rowlett  
 (1) Name: W. F. Friedman F B Rowlett  
 (2) Rank, position or employment: Cryptanalyst Jr Cryptanalyst  
 (3) Permanent address: Wash DC Etchells Church, Va  
 (b) Title of Invention: System for Randomizing the Relations of Electrical Circuits  
 (c) Description of Invention: See Description and drawings attached

(d) Dates and places of Invention:  
 (1) Conception by inventors: June 15, 1935 at Wash, DC  
 (2) Disclosure to others: no at \_\_\_\_\_  
 (3) First sketch or drawing: June 24, 1935 at Wash  
 (4) First written description: June 24, 1935 at Wash  
 (5) Completion of model or full sized device: none at \_\_\_\_\_  
 (6) First test or operation of invention: none at \_\_\_\_\_

(e) Results of tests, and extent of use of invention: none

(f) Names of persons having knowledge of facts stated under (d) and (e): none

(g) Prior Reports: none

(h) Patents and Patent applications: none other than present application

(i) Rights of U.S. Government: None known

(j) Licenses or Assignment: none

(k) Contracts involved: none

Contractors	Address
Contract No. and date	
Subject matter	Type of Contract
Location of Plant	
Official title or status of employment of inventor:	

(l) Signature of witness and date: \_\_\_\_\_ Signature of inventor and date: WF F & F B R

(m) Remarks of Forwarding Officer: \_\_\_\_\_ Signature of Forwarding Officer and date: \_\_\_\_\_

## INSTRUCTIONS

The following information will be given under the headings indicated:

- (a) The inventor should give his permanent address. He should also give his rank, corps, position or status of employment at the time invention was made.
- (b) The title of the invention should start with words indicating the class to which the invention belongs, such as "Method of" or "Process of" in case the invention relates to a method or process; or the name of the article, device or type of machine in case the invention relates to an article, device or machine, or the name of the material or composition in case the invention is an improvement in material or composition.
- (c) The description of the invention may be brief, provided reference is made to detailed specifications and drawings, which should be identified by date and file number, if official, or should be attached to the report if not part of the official records of the War Department. In either case, all drawings and descriptive pamphlets relating to the invention should be listed.
- (d) Care should be taken to give the earliest date on which the invention suggested itself to you, even though it was not completely in mind. If the invention comprises different inventive ideas, give the dates with reference to each part of the invention separately, taking care to identify each part clearly in the description of the invention.
- (e) State whether or not the invention was found to be operative, and the degree of success attained at each test of the model or full sized device. In stating the extent of use of the invention, separate "use by the Government" from "commercial use".
- (f) State the names of persons who had knowledge of the invention and facts concerning it on or about the dates mentioned.
- (g) Has description of invention or report of test, if any, been submitted to officers of the War Department? If so, when and to whom? Give references to all prior reports, including all information needed to locate same in files.
- (h) List all applications for patents by filing dates, serial number and title. List all patents by patent number, date of grant, and title.
- (i) Has tender to the United States been made? If so, when and to whom? If not, tender the use of the invention to the United States or explain why not.
- (j) State what, if any, rights in the inventions have been granted to others; including extent of interest granted and date of recording assignment or license in Patent Office.
- (k) If contracts have been placed for the invention, or if the invention was made in connection with the performance of a contract in which the United States is interested, the facts should be given briefly, including contractor's name and address; Contract No. and Date of Contract; Subject Matter; Location of Contractor's Plant where work was done; and Official Title or Status of Employment of Inventor.
- (l) It is desirable that the witness be familiar with the facts stated concerning the invention and have a sufficient understanding of the invention to describe its construction and operation.
- (m) The forwarding officer should give his opinion of the value of the invention to the U.S. and whether or not the prospective development or the art to which the invention relates would make it advisable to protect the invention and the Government's right to use the same by an application for patent.

Report of M-228

1 Col. Corderman

1. There is appended herewith a report on the security of the M-228. The material on which this study was based was taken from War Department channels and is a true indication of the type of security which may be expected from usage of this equipment.

2. The recommendations given below were arrived at in a conference among Major Rosen, Major Hiser, Captain Douglas and myself:

a. It is recommended that a study be undertaken immediately by the ablest cryptanalysts in SSS to determine if it is possible to reconstruct the cryptographic elements used in the M-228 under the conditions stated in the appended discussion.

b. It is further recommended that the M-228 be used for confidential and lower classification on radio, and then only under special conditions where complete supervision and control can be exercised by personnel properly trained in handling the M-228 both from operational and security standpoints; that for such use special keys will be arranged; that typing reperforators or equivalent equipment be used; and that under no circumstances will conference calls be permitted.

c. It is further recommended that no change be made in the present use of the M-228 on circuits such as land lines which are reasonably secure from interception.

d. It is further recommended that a study be undertaken to determine the most expeditious method of handling traffic over channels similar to the

Report on M-228

1  
(cont'd)

Washington-London, Washington-Brisbane,  
or Washington-Algiers channels. This  
study should be directed towards  
evaluating the relative merits of  
fully automatic versus systems using  
the 134-C and usual transmission  
agencies.

*Att: Report w/13 Incls.*

Frank B. Rowlett  
Major, Sig.C.  
SPSIS-4  
8 June 1943

~~SECRET~~

Report To: Colonel Corderman

Subject: Report on the M-228

1. The M-228 is the mechanism for generating a key which is used for the encipherment of plain-text signals generated by a teletypewriter mechanism. The invention of the cryptographic principle was made at SSS and reduced to practice at the SCGDL. The electrical application of the cryptographic key generated by the M-228 is almost identical with that proposed by Gilbert S. Vernam in 1918 and later. (See Vernam patents attached.) The M-228 was proposed initially for encipherment of messages to be transmitted on land lines. It was not contemplated that it should be used for enciphering signals to be transmitted by radio.

2. The relationship between the teletype, the M-228 (key generator) and the device (applique unit) which "scrambles" the plain-text signals is shown in the schematic diagram of Fig. 1. The teletype generating the plain-text signals is standard equipment which feeds the signals into a group of relays inside the applique unit. The M-228 consists of a set of 5 cipher wheels which, in conjunction with a teletype distributor head, generate an extremely long sequence of impulses similar to the plain-text signals. The impulses of the M-228 are fed into the relays of the applique unit where the combination of the plain-text and key impulses are effected as described below, to produce cipher text. On the receiving end the conditions are reversed. The signals of the enciphered text are fed into the relays of the applique unit where the key generated by the M-228 is removed and the remaining plain-text signal is fed into a standard teletype printer to produce the plain text version of the message.

3. a. Cryptanalytically, the encipherment effected by the applique unit can be expressed as a mathematical equation with elements of a limited binary system of 32 combinations. The Baudot Code used by the teletype is nothing more than the expression of 32 conditions by means of combinations of elements referred to hereinafter as + and -. The equation stating the conditions of encipherment is simply  $P + K = C$ .

b. In the case of the encipherment of a single letter, say the first letter of a message, the specific equation will become  $P_1 + K_1 = C_1$ . Likewise, the second, third, and fourth

~~SECRET~~

~~SECRET~~

encipherment, etc., may be expressed by the same type of equation using the appropriate subscripts,  $P_2 + K_2 = C_2$  etc. Given the conditions that two messages are enciphered by the same key, if the second message is represented by primes, these equations may be written as  $P_1' + K_1 = C_1'$  etc.

g. Given the first letters of two messages enciphered by the same key the equations pertaining to these two letters are:

$$P_1 + K_1 = C_1$$

$$P_1' + K_1 = C_1'$$

Since  $C_1$  and  $C_1'$  are the cipher texts of the messages which will be available to the cryptanalyst,  $C_1$  and  $C_1'$  may be considered as known, giving 2 equations with 3 unknowns. By subtracting one equation from the other, the  $K_1$ 's can be eliminated giving  $P_1 - P_1' = C_1 - C_1'$ , a single equation with 2 unknowns. This equation can be solved since the condition that  $P_1$  and  $P_1'$  must be plain-text letters can be applied. Practically, this would be effected by considering several equations at one time and examining a probable word for either the  $P$  or the  $P'$ , as indicated in the following paragraphs.

4. a. <sup>(inclosure #2)</sup> There is attached a chart which gives the Baudot equivalents of the 26 letters of the alphabet plus the 6 functions of the teletype giving a total of 32 distinct combinations. As stated above in Par. 3b these combinations may be considered as elements of a system of binary notation and the customary processes of addition, subtraction, multiplication, and division may be applied. The cryptographic function of the relays of the applique units is to perform addition of the 5 impulses of the plain text letters generated by the teletypewriter with the 5 impulses generated by the M-228. Since all 32 possible combinations are generated by the M-228, a total of 32 x 32 conditions will arise from the addition of a plain-text signal and a key signal. This can be best demonstrated by performing an example in addition which simulates the action of the relays. Suppose the plain text to be enciphered is the plain-text word THE. The Baudot equivalents for the 3 letters are shown below:

T	=	-	-	-	-	+
H	=	-	-	+	-	+
E	=	+	-	-	-	-

~~SECRET~~

Let it be assumed that the key generated by the M-228 at the instant is:

- 1st Key combination: + - + + +
- 2nd Key combination: - + + - +
- 3rd Key combination: + - + - +

In reference is made to the accompanying chart (Incl. No. 2), it will be noted that the first key combination corresponds to the letter X, the second to the letter V, and the third to the letter Y. The addition performed by the relays of the applique unit can be effected by the application of the following rule: If two like elements are added a + is obtained; if two unlike elements are added, a - is obtained. The addition in this case will be non-carrying, and since only two elements are used in the system it will be noted that addition and subtraction produce identical results. Based on this rule, the addition of T and the first key combination produces a combination which corresponds to the letter L; H and V give Y; and E and Y give J, as shown herewith:

First key combination (X)	T - - - - +	$\begin{array}{r} + - + + + \\ \hline - + - - + \\ \hline \end{array}$	1st Letter = L
2nd Key combination (V)	H - - + - +	$\begin{array}{r} - + + + + \\ \hline + - + - + \\ \hline \end{array}$	2nd Letter = Y
3rd Key combination (Y)	E + - - - -	$\begin{array}{r} + - + - + \\ \hline + + - + - \\ \hline \end{array}$	3rd Letter = J

b. As stated above, the addition of each of the 32 elements with itself and all the other elements gives  $(32)^2$  combinations. These combinations are represented in table attached (Incl. No. 3). Reference to this table permits rapid addition of plain text and key to give cipher, or an addition of cipher and key to produce plain text. The table is reciprocal in nature and may be used as follows: The plain-text letter is sought in the sequence at the left hand side of the table; the key letter is sought in the sequence at the top of the table; at the intersection of the row and column so defined, the cipher-text letter is found.

~~SECRET~~

text message with an assumed  
 cipher and a second message prepared  
 Given a text and a second message prepared  
 in the same Key,

c. The solution of the equation referred to in Par. 3,  $P_1 - P_1' = C$  can be effected empirically for two texts enciphered by the same key as follows. If the assumption is correct the exact key used for its encipherment can be obtained by use of the chart. This key can then be applied to the other of the two ~~superimposed~~ messages to produce the plain text corresponding thereto, as demonstrated in the following paragraph.

~~SECRET~~



**Page Denied**

~~SECRET~~EG 3.3(h)(2)  
PL 86-36/50 USC 3605

There ~~is~~<sup>are</sup> attached as Tables 5, 6, 7, 8 etc., examples of messages appearing on War Department radio circuits using the M-228 for which identical setting of cipher wheels were used. The solution of these messages is fairly simple. It can be greatly speeded up by application of machine methods and detailed worksheets are appended. A description of the method used, while fairly simple, is not within the scope of this paper.

5. The M-228 is misleading in appearance. The fact that it uses the same type of cipher wheels as the SIGABA immediately suggests to the observer that it effects the same type cryptographic treatment as the SIGABA. The SIGABA uses an entirely different cryptographic principle, and consequently its security is much greater than that of the M-228. The fallacy in assuming that the M-228 affords equal or comparative security with the SIGABA is dangerous since it produces a false feeling of security in the minds of those who do not appreciate the cryptographic principles about which the two machines are constructed.

~~SECRET~~

~~SECRET~~

6. Insofar as the security of the M-228 itself is concerned, considering the machine as it is now being used, the writer is aware of no method for reconstructing the wheels in case a large portion of the pure key is available. However, this appears to be a difficult problem, but in view of the fact that the principle is new in the art and that no extensive study of it has been made, there is some doubt in the writer's mind as to the validity of the assumption that the wheels can not be reconstructed under the circumstances of its present usage. For example, in the solution of the messages of Table 5, 6, etc. considerable pure key was recovered, which might be sufficient to permit a complete solution of the system.

7. A primary weakness of the M-228 lies in the fact that transmission can be made in the clear due to failure of contacts of the applique unit, or a simple failure on the part of the operator to throw a switch to cipher. In tape transmission on certain circuits the entire message could be transmitted without the operator's being aware that the message had gone out in the clear. It is therefore necessary to monitor all M-228 transmissions between the time of the encipherment and the time at which the impulses are fed into the transmission medium.

8. In view of the fact that the M-228 was designed for rapid handling of messages to be cryptographed, retransmissions of messages are made without paraphrasing. This happens most frequently with new operators and in general it is due to operational difficulties rather than functional or machine difficulties. No security study has been made to determine the effect of such transmissions on the fundamental security of the system.

9. The M-228 lends itself for use in conference calls. The nature of the language and text appearing in such a call cannot be readily controlled from the standpoint of security, and it is possibly more stereotypic in nature than any other type of communication other than "synoptics". This is because conferences usually consist of questions and answers and if a simultaneous recording is made of both channels, the assumption of plain text by the cryptanalyst is simplified considerably. Such things as OK, CAR RET, LINE FEED, GAPLS, and THAT IS ALL, will appear and can be readily recognized. If the system has any inherent weakness this type of usage will permit of its utmost exploitation.

~~SECRET~~

10. In the foregoing discussion the emphasis was placed on solution of two messages sent in the same key. No fair estimate of the security of a properly phrased, well-composed, and correctly cryptographed message can be given. However, for such communications the security of the M-228 can be estimated as lying somewhere between one tenth and one fourth that afforded by the SIGABA. In view of this statement, if the SIGABA is considered as the ultimate in security and the criterion of secret classification is based on the security afforded by it, it would appear that the M-228 on radio would afford only "confidential" security. When it is considered that the bulk of traffic will tend to move on M-228 channels this estimate makes it appear doubtful as to whether the M-228 should be used for messages of secret classification, when such channels are subject to interception.

D-R-A-F-T~~TOP SECRET - U.S. EYES ONLY~~REPLACEMENT OF THE PRESENT COMBINED CIPHER MACHINETHE PROBLEM

1. To determine the U.S. Position toward the United Kingdom's proposals in RDC 5/99 (attached as Appendix "A") that:

- (1) there be a full and complete interchange of cryptographic principles and policy on a reciprocal basis.
- (2) if the U.S. Chiefs of Staff cannot agree to (1) above, they authorize the disclosure of the principles of the ECM (SIGABA) so that these may be incorporated in a new British Cipher Machine.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

2. Of the two foregoing proposals, the first is unacceptable. The United States Government adheres to the following generally accepted basic principle of national sovereignty and security: the means and methods which a government employs for the protection of its own communications constitute a private matter not to be shared in toto with any other government. This principle is sound because it is impossible to be certain that a former ally will not be someday over-run by a common enemy or may even become a foe, in which case a well-forged weapon may be turned against its originator. As regards the effects of such a contingency, the primary danger in the cryptologic field is not that the security of communications may be destroyed or impaired but that the sources of communication intelligence may be dried up.

~~TOP SECRET~~  
~~TOP SECRET~~

3. With regard to the second or alternative proposal, it is felt that this solution should be accepted by the United States, for the following reasons:

a. In the spring of 1947 there were Combined discussions on this same subject. These resulted in a decision to withhold the ECM and to study possible improvements in the CCM. The results of this study have been largely negative, the only possibility being the BCM, a machine which represents some improvement in security over the CCM but not deemed sufficient in degree to meet with British acceptance. Moreover, the modifications which would be required in the British Typex machine to convert it into a BCM are such that there is grave doubt as to their accomplishment. Also, the British have decided that they must replace the Typex in any case and the introduction of a suitable replacement would be expensive in terms of time required for research, development and service testing. It would be to the advantage of the U.S. as well as to the British if such a delay could be avoided so that British equipment suitable also for Combined Communications would become available at an early date.

b. During the Combined discussions referred to above, the British indicated that they were aware of the principles of the ECM. They described them quite accurately and indicated that they considered their security to be of the highest order. They admitted, in fact, that they had incorporated those cryptographic principles in a radioteletype cipher machine for their own use. Furthermore, even as regards the engineering know-how which went into the construction of the ECM, this knowledge has been disclosed to the British, since they were provided with CSP 1700. This machine was simply an ECM chassis with certain of the ECM cryptographic features eliminated.

~~TOP SECRET~~  
~~TOP SECRET~~

c. Disclosure of the ECM to the British and its adoption by them would give the two governments a suitable piece of equipment ensuring the highest degree of security for vital combined U.S. - British communications.

d. Disclosure of the ECM will not leave the U.S. without equipment unique to the U.S. As a matter of fact, a modification of the ECM has already been developed (CSF 2900) and is available in quantity. This modification, which improves the security of the ECM, does so without in any way impairing its use as an ordinary ECM or as a CCM. By means of a simple switching arrangement it is possible to make the CSF 2900 serve as a device purely for U.S. communications, or as an ECM for U.S. - British combined communications, or as a CCM. However, the principles of the CSF 2900 would not be disclosed to the British.

e. Release of the ECM to the British would leave the way open to the adoption of the CCM for North Atlantic Pact communications if such a decision should be found to be necessary in the national interest. British - U.S. use of the ECM would be easily adaptable to North Atlantic Pact communications since the addition of a simple already available adapter to either the ECM or the CSF 2900 would permit communication with any North Atlantic Pact nation holding the CCM. In addition, disclosure of the CCM to the other signatories to the North Atlantic Pact would not impair the security of U.S. - British communications since the CCM system would then be reserved for that specific purpose.

f. At the time of the 1947 Combined discussions on this subject, one of the principal U.S. objections to disclosing the ECM to

the British was the increased danger of compromise arising from the wider distribution of the equipment if the British were permitted to have it. This increased danger is recognized but it is believed that the advantages cited above outweigh this objection.

g. Also at the time of the 1947 Combined discussions there were indications that the British did not provide and enforce physical security protective measures for their crypto-equipment equal to those required and enforced by the U.S. services. Because of this it was agreed on a Combined level that a prerequisite to further discussions regarding a replacement for the CCM would be a Combined agreement covering the measures both governments would apply in the handling and protection of combined cryptomaterial. Such an agreement has been concluded and concurred in by both Governments (CCB-285, 11 Oct 1948). A review of that document in order to insure identity in security regulations applicable to the ECM and an acceptance of such changes therein as may be deemed necessary by the U.S. should be a preliminary to entering upon discussions leading to a full disclosure of the ECM to the British.

#### CONCLUSIONS

4. It is concluded that:
  - a. The first proposal made by the United Kingdom in RDC 5/99 of 13 July 1949 should be rejected.
  - b. The details of construction of the ECM (SIGABA) should be disclosed to the U.K. in discussions which will include a review and acceptance by both Governments of identical security regulations to insure the physical protection and proper use of the equipment.



~~TOP SECRET~~

RECOMMENDATIONS

5. It is recommended that:

- a. A memorandum substantially as in Appendix "B" be forwarded to the British Joint Services Mission.

COORDINATION

6. Coordination with AFCIAC has been effected.

~~TOP SECRET~~

~~FOR AMERICAN EYES ONLY~~

~~TOP SECRET~~

~~TOP SECRET~~JOINT COMMUNICATIONS - ELECTRONICS COMMITTEESECURITY AND CRYPTOGRAPHIC PANELREPLACEMENT OF THE PRESENT COMBINED CIPHER MACHINE

(Proposed reply to the British Joint Services Mission)

1. The U.S. Joint Chiefs of Staff have carefully considered the proposals made in RDC 5/99 of 13 July 1949 concerning the replacement of the existing Combined Cipher Machine. The U.S. Joint Chiefs of Staff regret that they are unable to accept the proposal for a full and complete interchange of cryptographic principles and policy on a reciprocal basis. However, they are prepared to authorize discussions which can commence in Washington at any time, leading to the disclosure of the principles of the ECM (SIGABA) so that these may be incorporated in a new British Cipher Machine, these discussions to be preceded by a review and acceptance by both Governments of identical security regulations to provide for the physical protection and proper use of the equipment.

APPENDIX "B"

~~TOP SECRET~~

~~SECRET~~

CSGAS-14

20 September 1949

MEMORANDUM FOR: CHIEF, ARMY SECURITY AGENCY

SUBJECT: Replacement of the CCM

REFERENCE: (a) AFCIAC Document 13/4 of 14 Sept 49

1. a. In connection with reference (a), it is deemed advisable to note that the EGM-SIGABA is covered by a number of patents or patent applications.

b. Certain of these patents or patent applications are owned by the Teletype Corporation. The exact number of these cases, their serial numbers, and specific nature are unknown to this Agency, as they are being handled under Navy control.

c. There are certain other patents or patent applications, covering certain subsidiary features which were invented by Navy personnel. Details of ownership are not known to this Agency.

d. The basic cryptographic principles employed in the equipment are covered by the following patent applications, still in a secrecy status under the "Three-Year Rule" (Sec. 4894, R.S., as amended) and also under Public Law No. 700 (War-time secrecy for patent applications):

<u>App. Serial No.</u>	<u>Inventors</u>	<u>Date filed</u>
682,096	Friedman	25 July 1933
70,412	Friedman & Rowlett	23 Mar 1936

In each of these two cases the U. S. Government owns the entire right, title and interest in the invention, throughout the U.S. and territories and dependencies thereof, but not elsewhere; the inventors have an irrevocable, assignable, and exclusive license to make, use and/or sell and to license others to make use and/or sell the invention. Attached hereto is a copy of the assignment in each case. (Incl. 1 and 2).

~~SECRET~~

Legal size  
triple space  
carbon copy

For a half century following the close of the Civil War, cryptology in the United States enjoyed a period of hibernation from which it <sup>at long last in about 1914,</sup> awoke, not refreshed, as did Rip Van Winkle, but weaker. This is perhaps understandable if we take into account the fact that the United States was able to enjoy a long era of peace, broken only briefly by one short war, the Spanish American, of 1898. For over three decades there was no need for cryptologic operations except such as were required for the communications of the Department of State. The military and naval services apparently felt that ~~since in time of peace there is no need for~~ <sup>it looked as though the U.S. was going to enjoy</sup> ~~and since the duration of the peace appeared to~~ <sup>peace for as long, an indefinitely long time,</sup> those services did not think it necessary or desirable to engage in cryptologic studies. Of course, the War Department and the Army still had their route ciphers and cipher disks; the Navy Department and the Navy had their decks for producing monoalphabetic ciphers; and the Department of State had a ~~code~~ <sup>more or less</sup> code specifically designed for its ~~communications~~ <sup>communications</sup> ~~with the~~ <sup>with the</sup> ~~international scene,~~ <sup>international scene,</sup> ~~as far as concerns the U.S., was quiet.~~ <sup>as far as concerns the U.S., was quiet.</sup> Let Europe fight - it was none of our way of life or our affair.

The long hibernating period was briefly broken by one episode that may interest you. I had not planned to bring it to your attention in this brief history but certain events in the very recent past lead me to tell you about it. I refer here to the very small <sup>popular-vote</sup> ~~majority~~ by which Democratic candidate Kennedy won the presidency over Republican candidate Nixon, and the consequent talk about the possibility of an upset when the electoral college <sup>would vote</sup> came to do its work. The very same <sup>sort of</sup> situation occurred in the presidential election of 1876, in which Democratic candidate Samuel J. Tilden was pitted against Republican candidate Rutherford B. Hayes. <sup>On the basis of early returns Tilden seemed to be easily the winner.</sup> Going to bed on election night, 8 November 1876, Hayes conceded to Tilden and the newspapers next morning in fact reported <sup>a</sup> Tilden victory. But a couple of days after the election it began to appear that perhaps Tilden's victory was not sure, and his supporters began maneuvers to try to make it certain by taking advantage of our peculiar system of electing a president, peculiar because it is the electoral, not the popular vote which determines who is to be president. Two days

Telegrams also had to be exchanged among secret agents in the field.

after the people had voted it became clear that Tilden would have 184 electoral votes, just one vote short of insuring victory, whereas Hayes would have only 163, thus needing 22 more. The Tilden supporters began a frantic campaign to get that one additional vote and they didn't hesitate to try bribery, a rather serious piece of business obviously requiring <sup>a good deal of</sup> secrecy. Of course, many telegrams had to be exchanged between the Tilden headquarters in New York City and confidential agents sent to certain states where <sup>electoral</sup> votes could perhaps be purchased; About 400 telegrams were exchanged and about 200 of these were in cryptographic form. Because of communication difficulties two <sup>almost consummated</sup> ~~of three separate~~ deals fell through; a third deal failed because the electors were <sup>[insert over]</sup> honest Republicans not susceptible to bribery.

PP Those of you who are interested in the political aspects of this <sup>intriguing story</sup> campaign will find excellent reading material in various books dealing with it. Those of you who are interested <sup>only</sup> in its cryptologic aspects will find excellent material in the following three documents:

(1) "The Cipher Dispatches." <sup>The</sup> New York Tribune, Extra No. 44, New York, ~~1878~~ (14 January) 1879.

Insert

REF ID: A62844

existence of these  
The telegrams remained unknown for months. But the  
outcome of the election remained in doubt because  
four states, Florida, South Carolina, Louisiana and  
Oregon each sent two groups of electors, an event  
not foreseen and provided against in the Constitution. A  
crisis arose and the country seemed on the verge of  
<sup>another</sup> civil war. By an act of 29 January 1877, Congress  
created a special electoral commission to settle the  
<sup>electoral votes</sup> disputed in the four states. The commission voted in  
favor of the Hayes electors in each case and Hayes  
entered the White House. But it was only some months  
afterward that the telegrams to which I have referred  
were brought to light and a situation arose which  
Congress felt it had to look into. Somehow or other  
<sup>copies of</sup> the telegrams came into the possession of <sup>the</sup> Republican  
<sup>in the summer of 1878,</sup> the New York Tribune, and two  
members of its staff succeeded in solving those in  
cryptographic form.

Hassard, John R.G.

single  
space +  
indent

(2) "Cryptography in Politics." The North American Review, Vol. CXXVIII, No. 268, March 1879, pp. 315-25.

(3) "U.S. House Miscellaneous Documents, Vol. 5, 45th Congress, 3rd Session, 1878-79."

The Congressional House Committee designated to conduct the investigation was named "The select Committee on alleged frauds in the Presidential Election of 1876." In the course of the investigation the Committee called a Prof. Edward S. Holden, of the United States Naval Observatory in Washington. I think he was a captain in the Navy and specialized in mathematics. The Tribune had brought him into the picture and Prof. Holden solved the ciphers but only after Mr. John R.G. Hassard, the chief of The Tribune staff, and his colleague, Col. William M. Grosvenor, also of that staff, had reached a solution.

Prof. Holden's testimony is of considerable interest. He presented his solution of the nearly 200 cryptograms entered in evidence. His testimony is summarized in a letter dated 21 February 1879 and it sets forth all the cryptosystems used by both parties, together with their keys and full details of their solution. In that letter Prof. Holden makes the following statement: "By September 7, 1878, I was in possession



\* See pp 315-325 of U.S. House Miscellaneous Documents Vol. 5, 45th Congress, 3d Session 1878-79. See also article by John R.G. Hassard, "Cryptology in politics," in The North American Review, March 1879, pp. 315-325. (Vol. CXXVIII, No. 268) \*

~~Tails of the application Prof Holden in his letter makes this statement: "By September 1878, I was in possession~~

~~of a rule by which any key to the most difficult and ingenious of these (the transposition cipher of Democrats) could infallibly be found." Holden worked out the transposition keys ~~but in that he was of course anticipated by the Tribune cryptanalysts. There were the keys, although Holden independently discovered them~~ in all 10 different keys, two for messages of 10 words, two for messages of 15 words, <sup>up to and including</sup> two for messages of 30 words. Here is the complete table of keys:~~

leave 1/4 page space

[Pencil over]

I <sup>not</sup> ~~very~~ suspect that the <sup>base or "verse"</sup> sequences of numbers were drawn up at random but were derived from ~~the~~ words or phrases; <sup>and I suspect that the odd-numbered ones are the "verse."</sup> I have not had time to try to reconstruct them. Perhaps some of you may like to make the attempt. You will notice that in the odd-numbered keys the positions of sequent digits reflect an underlying <sup>word or phrase</sup>. In addition to transposition this system involved the use of code words to represent <sup>certain words and</sup> of certain persons, <sup>and</sup> places, and numerals. There were also a few nulls. Here is the entire vocabulary:

leave 1/4 page space

You may be wondering why there are two transposition keys for each length of message from

10 to 30 in multiples of 5. The two keys consisting

a pair are ~~correlatives of each other~~ related to ~~each other~~ <sup>that is, they bear a relationship -</sup> ~~something~~ which one of the Tribune cryptanalysts <sup>has</sup>

termed "correlatives," but which we now would call an "encipher-decipher" or "verse-inverse"

relationship. Either sequence may be used to encipher, ~~the other~~ ~~the other~~ ~~can be used~~

to decipher a message. For example, key III consists of the following: 8-4-1-7-13... etc, and the correlative,

key IV, is 3-7-12-2-6... etc. A <sup>cipher</sup> message of 15 words can be deciphered either by (1) numbering the words ~~con-~~ ~~secutively~~ and then ~~putting~~ assembling the words in the order 8-4-1-7-13 etc, or by (2) writing the sequence

3-7-12-2-6... above the words of the cipher message and then assembling the <sup>thus-rearranged</sup> words according to the sequence 1-2-3-4-5... Thus, there were, in reality,

not 10 different transposition keys but only five.

In <sup>the case of</sup> each pair of keys one of them must have been the basic sequence, the other the <sup>inverse</sup> ~~inverse~~ ~~sequence~~ of it.

Prof. Holden adds some comments <sup>about this system</sup> which are worth presenting:

The essence of this ingenious and novel system consists in taking apart a sentence written in plain English (dismembering it, so it were) and again writing all the words in a new order, in which they make no sense. The problem of deciphering it consists in determining the order according to which the words of the cipher should be written in order to produce the original message.

There is one way, and only one way, in which the general problem can be solved, and that is to take two messages, A and B, of the same number of words, and to number the words in each; then to arrange message A with its words in an order which will make sense, and to arrange the words of message B in the same order. There will be one order — and only one — in which the two messages will simultaneously make sense. This is the key.

It appears that Prof. Holden did not note the verse-inverse relation in each pair of sequences, or, if he did, he failed to mention it, as Hassard did in his article.

There were enough messages to permit of establishing the meanings of the code words used, so that the plain text of practically all the messages in this, the most complicated of the cryptosystems involved in this bizarre political episode, became quite clear.

[Insert over]

~~But~~ there were several other ~~systems~~ systems involved, <sup>but I am going to have to pass them by</sup> of which only one or two deserve attention in this brief history. I do, however, want to call your attention to the very close resemblance between <sup>the word-transposition ciphers</sup> what was characterized by Prof. Holden as "the most difficult and ingenious" of the ciphers he solved, and the USMTC route cipher ~~of the USMTC which I described in the preceding lecture.~~ <sup>and which, technically considered, were much simpler</sup> Yet, not only he but also the <sup>amateur</sup> Tribune cryptanalysts solved these ciphers without too much difficulty, <sup>even though they were technically more complex.</sup> I think their work confirms my own appraisal of the <sup>weakness and</sup> futility of the route ciphers <sup>used by the USMTC in the Civil War.</sup> as ciphers of merit.

Let us now go on with cryptologic history after this ~~political~~ digression into the realm of what may be called political cryptology. I do not know what the Department of State used

Insert

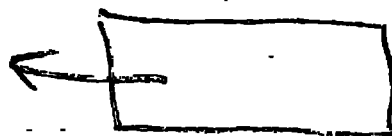
27/25

Another system used by the conspirators used a 2-letter for one <sup>letter</sup> substitution and was based upon a 10x10 checkboard. Apparently <sup>neither</sup> Prof. Holden nor the Tribune cryptanalysts recognized the latter principle, nor did they find that the coordinates of the checkerboard employed a key phrase, which, ~~appropriately enough, was "HIS PRIME"~~.

		H	I	S	P	R	I	M	E

nor did they realize that the same checkerboard, with numerical coordinates, was used for the 2-digit for one letter substitution. Here are two of the messages exchanged by the conspirators, one in the letter cipher, the other <sup>figures cipher</sup> in the <sup>figures cipher</sup>.

leave  
1/4 page space



They are long enough for solution, if you wish to try to solve them and find the key phrase, which <sup>should</sup> will amuse you by its appropriateness.

for cryptographic communications in the years following the Civil War. Probably it was a small code, even an adaptation of some commercial code. But in an article entitled "Secret Writing" which appeared in Century Magazine, Vol. LXXX<sup>Nov. 1912</sup>,<sub>112</sub>, a man named John

H. Newell, apparently a code clerk in the Department, referred to a new code<sup>of the department</sup> in the following terms:

The cipher of the Department of State is the most modern of all in the service of the Government. It embraces the valuable features of its predecessors and the merits of the latest inventions. Being used for every species of diplomatic correspondence, it is necessarily copious and unrestricted in its capabilities, but at the same time it is

Single  
space  
width

single  
space +  
indent

economic in its terms of expression. It is simple and speedy in its operation, but so ingenious as to secure absolute secrecy. The construction of this cipher, like many ingenious devices whose operations appear simple to the eye but are difficult to explain in writing, would actually require the key to be furnished for the purpose of an intelligible description of it.

Only four years later a <sup>certain</sup> telegraph operator and code clerk of the State Department proved how vulnerable the Department's system of enciphered code really was. His name was Herbert O. Yardley and many of you may know <sup>a bit</sup> about him because <sup>he was the author of a famous</sup> or infamous <sup>and</sup> book <sup>entitled</sup> The American Black Chamber, which <sup>was</sup> published by <sup>The</sup> Bobbs-Merrill <sup>Co.</sup> in 1931. So far as I know it is the only book which ~~cannot~~ <sup>is forbidden</sup> legally be reprinted in the United States because <sup>it</sup> a special law <sup>forbids</sup> <sup>makes it a criminal offense to do so.</sup> passed in 1934. That is quite a story in itself but I cannot ~~tell it now.~~ <sup>if you happen to own a copy of <sup>the first and only American edition</sup> it, protect it carefully. don't let it get away from you, because you can only obtain another copy of it by a more or less "under the table" deal or may only be <sup>able to</sup> purchase an English edition by a similar route</sup>

of deal. But to return to that State Department cryptosystem considered by Haswell "to assure absolute secrecy", here is the cover page of Yardley's 21-page typewritten analysis.

leave  
1/4 page space

Yardley was quite wrong in thinking that his was the first successful attempt to solve a problem in deciphered code, for in Europe successful attempts on more complicated cases were often the rule and I imagine that British cryptanalysts could have and perhaps did read ~~perhaps did read~~ cryptanalysts were quite successful in reading State Department messages on a more or less <sup>rather</sup> regular matter. For in Europe, cryptanalytic studies were going on apace during the years of American neglect of such studies.

In our Navy the monoalphabetic cipher continued in use until the middle of the eighties, when several naval officers were designated to prepare a more suitable system based upon a code particularly for naval communications. The system they worked out involved a <sup>very</sup> large codebook, which had the official title U.S. Navy Secret Code, <sup>has an accompanying</sup> ~~but separate~~ cipher book almost as large. In addition to these <sup>and</sup> ~~and~~ <sup>officially</sup> designated as the book of Key Words.



two books was a third book <sup>called</sup> "General Geographical Tables. The system was placed into effect on 1 December 1887. About 10 years later a new edition of the third book was placed into effect. Later I will show you a most historic message sent in that dummy system of secret communication.

In our Army <sup>in the middle eighties, too</sup> a code was also prepared, and its composition and format hardly shed laurels upon those responsible for its production because it was merely a counterfeit of a commercially available and ~~popular~~ <sup>first published in 1870</sup> small code, for use by the general public under the title: Telegraphic code to ensure secrecy in the transmission of telegrams, by

Robert Slater, Secretary of the French Atlantic Telegraph

Insert over Co. <sup>Slater's</sup> the code must have met with popular acclaim because by 1906 it was in its fifth edition. You may like to see the title page of the second edition, a copy of which is in my collection. I wish I had a copy of the very first edition but not even the Library of Congress has one, that's how scarce it is.

To get on with the story, in 1885 the War Department published a code for its use and the use of the Army. Here is a picture of its title page. The only difference between it and the title page of the 2nd edition of Slater's Code is in the spelling of the word secrecy, as you can easily see in the picture I show you next. It would appear that Col. Gregory was just a bit deficient

As to the nature of the code, I will quote from Slater's own "Short explanation of the mode of using this work":

It is a numbered Telegraphic Dictionary of the English language, of which each word bears a distinctive No. <sup>[from 6001 to 2000, with exactly 100 words per page.]</sup> and the method of using it is by an interchange of Nos., in accordance with a private understanding between correspondents that a further No. is to be added to or deducted from the No. in the code, of the word telegraphed or written, to indicate the real word intended, thus a "Symbolic" or "Dummy Word" is telegraphed, the meaning of which can only be read by those who have the key to the secret of how many should be added to or deducted from the No. in the Code, of the "Dummy Word" to find the word meant.

Single  
Square  
indent

Here we have a sentence of 116 words with a meaning which is quite murky but I think you will gather its import. The system, <sup>as thus far described.</sup> is what we now call an additive or subtractive code method. But in the detailed instructions Slater goes one step further and suggests that instead of telegraphing the code numbers resulting from addition or subtraction, the code words standing alongside the sum (or difference) of the mathematical operation be sent.

in imagination because, <sup>not only did he simply borrow the basic idea of Slater's code but also</sup> when it came to preparing the rules <sup>for</sup> and examples of enciphering the code groups the colonel used the identical rules and <sup>and even the same type of transformations</sup> wording of them that are found in Slater's original. <sup>In the latter, for. let me show, Example I of Slater's code</sup> side by side with the same example from Gregory's:

Leave 1/2 page space

All the other methods and examples in the two codes are practically identical. Colonel Gregory gives credit to a civilian aide, in the following terms: "The labor of compiling the new vocabulary has been performed by Mr. W. G. Spottswode. And Mr. Spottswode's work consisted in casting out such words as ABALLENATE and ABANDONEE from Slater's list and <sup>replacing them with</sup> adding such words as ABATEMENT and ABATIS. <sup>indeed</sup> This sort of work must have been arduous. I'm sorry to appear to be so critical of my predecessors in the construction of <sup>codes and code systems for</sup> War Department and Army usage, but I feel sure you will agree that more imagination and ingenuity could have been employed than were <sup>used</sup> by Messrs. Gregory and Spottswode.

Col. Gregory prepared a confidential letter

to Lieut. General Sheridan", Commanding Army of the U.S.", to explain the beauties of the new code. Again because I'm afraid you won't place too much credence in what I'm telling you, the confidential letter <sup>from Col. Gregory to Lieut. General Sheridan</sup> is printed in <sup>photo</sup> in Appendix I, to <sup>the letter</sup> <sup>to</sup> which I have added <sup>Col. Gregory's</sup> "Introduction" ~~that Col. Gregory prepared~~ to the instructions for using the code.

Believe it or not, this was the code that the War Department and the Army used during the Spanish-American war. It was apparently used with simple additive, <sup>because</sup> in a copy in my collection the additive <sup>is</sup> written on the inside of the front cover. <sup>page 41-42 of</sup> It was 777. In The American Black Chamber the author <sup>throws an interesting sidelight on this code system:</sup>

The compilation of codes and ciphers was, by General Orders [he meant Army Regulations], a Signal Corps function, but the war [1917] revealed the unpreparedness of this department in the United States. How much so is indicated by a talk I had with a higher officer of the Signal Corps who had just been appointed a military attache to an Allied country. It was not intended that attaches should actually

single  
space &  
indent

encode and decode their own telegrams, but as a part of an intelligence course they were required to have a superficial knowledge of both processes in order that they might appreciate the importance of certain precautions enforced in safeguarding our communications.

When the new attache, a veteran of the old Army, appeared, I handed him a brochure and rapidly went over some of our methods of secret communication. To appreciate his attitude, the reader should understand that the so-called additive or subtractive method for garbling a code telegram (used during the Spanish-American War) is about as effective for maintaining secrecy as the simple substitution cipher which as children we read in Poe's The Gold Bug.

He listened impatiently, then growled: "That's a lot of nonsense. Whoever heard of going to all that trouble? During the Spanish-American War we didn't do all those things. We just added the figure 1898 to all our figure code words, and the Spaniards never did find out about it."

single  
space  
&  
indent

Although The American Black Chamber abounds with exaggerations and distortions, what the author tells about the inadequacies of United States codes and ciphers in the years just before our entry into World War I are true enough and Jardley's impatience and satires in this regard are ~~fully and~~ unfortunately fully warranted.

We have noted how inadequately the Army and the War Department were equipped for cryptocommunications in the decades 1890-1910. Let us see how well equipped ~~the~~ Navy and the Navy Department were. For this purpose I have <sup>excellent</sup> an example and one of great historical significance and interest. You will recall my mention of the appointment of a board of Navy officers to prepare a suitable cryptosystem for the Navy and I told you about the <sup>large</sup> basic codebook and its <sup>almost as large book for</sup> companions, enciphering the code groups. For the ~~the afternoon of 25 February 1898, or~~ <sup>On Saturday, the Secretary of the Navy,</sup> ~~John D. Long,~~ <sup>for home,</sup> had taken off ~~perhaps for a nap or a game of cards,~~ leaving Theodore Roosevelt, <sup>the</sup> Assistant Secretary in charge of the store. It was ~~today's opportunity~~ <sup>today's opportunity</sup> for a bold move ~~unhindered by his superior's~~

story we go back to the time of President McKinley, whose election brought Theodore Roosevelt, a former member of the Civil Service Commission, back to Washington as Assistant Secretary of the Navy. Tully was an ardent advocate of military and naval preparedness and frankly favored a strong foreign policy, looking forward, in fact, to the ultimate withdrawal of the European powers from the Western Hemisphere. With vigor, he set to work to make the Navy ready. When the Battleship Maine was blown up in Havana harbor on 15 February 1898, Roosevelt sharpened his efforts. During a temporary absence of his chief, John D. Long, he took it upon himself to instigate the preparations which he had in vain asked the Secretary to make. He ordered great quantities of coal and ammunition, directed the assembling of the Fleet, <sup>and</sup> stirred the arsenals and navy yards to activity. On a Saturday afternoon, ten days after the Maine was blown up, and still in the absence of Secretary Long, Tully sat down and wrote <sup>out</sup> a cablegram to go to Commodore George Dewey. Here it is, with his bold signature at the bottom:

cablegram leave  
 1/4 page space

That was the <sup>now historic</sup> message which alerted Dewey and which resulted in our taking the Philippines from the Spanish in the war which was declared ten days later on Spain.

I don't know when that classification "Secret and Confidential" was crossed out but it must have been years later, for those three words appear in the plain text of the deciphered and decoded cablegram. Here is a picture of the <sup>code</sup> cablegram as it was received in Hong Kong:

Leave 1/2 page space

And now I show you the deciphered and decoded text, which I produced myself by courtesy of the Chief of the Navy Security Group, who permitted me to ~~consult and make the necessary~~ <sup>Security</sup> borrow the ~~two~~ books from Navy archives.

To translate a message three steps are necessary.

First, the cable words (<sup>the</sup> peculiar, outlandish words <sup>on line 2 =</sup> WASSERREIF PAUSATURA BADANADOS, etc.) are sought in the cipher book, and their accompanying <sup>cable-word</sup> numbers set down. WASSERREIF yields 99055; PAUSATURA yields 62399; BADANADOS, 11005; CENTENNIAL, 16820.

The next step is to append <sup>the second</sup> the first digit of cable word <sup>to make the latter a six digit number.</sup> to the last digit of the first cable-word number. Thus 99055 becomes 990556. The six-digit <sup>code group</sup> number is then sought in the basic code book and its meaning is found to be "Secret and Confidential." The transfer of



demonstration of a straightforward, mathematical method of solving the Vigenere cipher was published in Berlin during the mid-period of the Civil War in America. Of the book created an odd impression in Europe it was altogether unspectacular; in America it remained unheard of until after the advent of the 20th Century. Although Kasiski's method is explained quite accurately in the first <sup>American</sup> text on cryptology, Capt. Parker Hitt's Manual for the solution of military ciphers (Fort Leavenworth, Kansas: Army Service Schools Press, 1916), the name Kasiski doesn't even appear in it. Other books on cryptologic subjects appeared <sup>in Europe</sup> during this period, among which the more important were the following:

leave 1/2 page space

Of the foregoing two deserve special mention. The first, by Commandant Bazeries, is a book notable not for its general contents, which are presented in a rather disorganized, illogical sequence, but for its presentation of a cipher device invented by the author, the so-called cylindrical cipher device, a picture of which I

I now show you. But our own Thomas Jefferson anticipated Bazières by a century, and here are two slides describing Jefferson's "Wheel Cypher," copied from the original manuscript among the Jefferson Papers in the Library of Congress. The second book <sup>in the foregoing list which is</sup> deserving of attention is the one by de Viaris, in which he presents methods for solving cryptograms prepared by the Bazières cipher cylinder or Jefferson's Wheel Cypher.

It was in the period during which books of the foregoing nature were written and published that the chanceries of European Governments operated the so-called Black Chambers, ~~for~~ organized for solving the secret communications of one another. Intercept was unnecessary because the governments owned and operated the telegraph systems and traffic could be obtained simply by making copies of messages arriving <sup>or</sup> departing <sup>from telegraph officials</sup> or in transit through them. This was true in the case of every country in Europe with <sup>very important</sup> one exception: Great Britain. The story is highly interesting but I must condense it to a few sentences.

In England from about the year 1540 onward a black chamber was in constant operation. It was one of two <sup>collaborating</sup> organizations called The Secret Post Office and the Office of Decipherer.

A famous mathematician, John Wallis, took part in the activities of the Office of Decipherer, <sup>in</sup> ~~But~~ 1644.

In the <sup>former, letters were opened,</sup> copies of them were made, the letters replaced, the envelopes resealed, and if there were wax seals, duplicates were made. Copies of letters in cipher were sent to the Office of Decipherer for solution and the results sent to the Foreign Office.

a scandal involving these two secret offices <sup>completely</sup> caused Parliament to close them down, so that from 1644 until 1914 there was no black chamber at all in Britain. As a <sup>consequence,</sup> when World War I broke out on the first of August 1914 ~~the~~ England's black chamber had to start from scratch, but British brains and ingenuity within a few months built a cryptologic organization, <sup>known as "Room 40 O.B."</sup> which contributed very greatly to <sup>the</sup> Allied victory in 1918.

Perhaps the greatest ~~and most important~~

achievement of Room 40 O.B. was the interception and <sup>known as the Zimmermann Telegram,</sup> solution of what is deservedly called the most important <sup>single</sup> cryptogram in <sup>all</sup> history. On 8 September 1918 I gave an account of this cryptogram, its interception, its solution,

an operation which just in the nick of time brought this country into World War I on the Allied side. The active, intelligent operation involved

and how the solution was handed over to the United States, bringing America into the war on the British side, without disclosing to the Germans just how the plain text was obtained, least of all that it had been obtained by <sup>interception and solution by</sup> cryptanalysis. My talk took two and a half hours and I didn't quite succeed in telling the whole story, which you will find in great detail (except for some <sup>important</sup> technical data not yet available to the public) in a book entitled The Zimmermann Telegram, by Barbara Tuchman, (Date ). Also, you should consult a book entitled Eyes of the Navy, by Admiral Sir William James, (Date ). Both books deal at length with the Zimmermann Telegram and tell how astutely Sir William Reginald Hall, Director of British Naval Intelligence in World War I, managed the affair so as to get the maximum possible advantage from the feat accomplished by the British Black Chamber. To summarize, as I must, this fascinating true tale of cryptanalytic conquest, let me first show you the telegram as it passed from Washington to Mexico City.

Leave 1/2 page space

the day that

French Ambassador Page sent his cablegram to President Wilson on (24 February 1917) quoting the English translation of the Zimmerman Telegram in the form in which it had been forwarded by German Ambassador von Bernstorff in Washington to German Minister von Eckhardt in Mexico City, the entrance of the United States into the war as a belligerent on the side of the Allies was assured.

Under big black headlines the English text appeared in our newspapers on 1 March, ~~and on 6 April 1917~~ that the United States <sup>Congress</sup> declared war on Germany and the Central Powers. The date was 6 April 1917.

In the War Department, <sup>and in the Navy Department</sup> the face set for preparing for active operations <sup>war</sup> quickened.

There was at the moment <sup>in neither of those departments nor in the Army or in the Navy</sup> no organization.

~~in the Navy Department~~ ~~any organization~~ ~~either for intercepting enemy communications or for studying them.~~ ~~for cryptanalytic operations on them.~~ ~~since the autumn of 1916 a very small group of self-trained cryptanalysts, supported by a private citizen named Colonel Fabyan who operated the Riverbank Laboratories at Elmhurst, Illinois, that organization maintained an unofficial~~

relationship with the authorities in Washington and ~~established a small school for training military cryptographic~~ ~~staff~~ ~~needed~~ ~~from time to time~~ ~~copies~~ ~~of~~ ~~messages~~ ~~obtained~~ ~~by~~ ~~interception~~ ~~means~~ ~~from~~ ~~telegraph~~ ~~and~~

\* Honorary title conferred by the Government of Illinois for Fabyan's participation as a member of the Board Commission that negotiated

The Treaty of Portsmouth, which followed the Russo-Japanese War in 1906.

Insert

8-column

For instance, here is the bold black headline in the New York Times of 1 March:

GERMANY SEEKS ALLIANCE AGAINST U.S.

ASKS JAPAN AND MEXICO TO JOIN HER;

FULL TEXT OF HER PROPOSAL MADE PUBLIC

The New York World had a series of headlines and subheads that extended halfway down the page, beginning with:

MEXICO AND JAPAN ASKED BY GERMANY

TO ATTACK U.S. IF IT ENTERED THE WAR;

BERNSTORFF A LEADING FIGURE IN PLOT

There followed nine full lines of subheads to what was a most amazing and dramatic story.

Still, notwithstanding all the furor that the disclosure of the Zimmermann Telegram created in America, President Wilson still hesitated and it was not until more than a month later, and after several American ships were sunk without warning on 18 March, that

There were plenty of senators and representatives who disbelieved the story. It was too fantastic; it was a British plot unproved; Wilson was being taken in, etc., etc. But when Zimmermann himself foolishly acknowledged that he had indeed sent such a telegram, disbelief changed quickly into vehement anger. Surely war would now be declared on Germany!

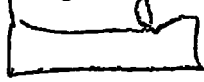
REF ID: A62844 ourselves for this unusual task, and later what we used later on for training the student officers sent to Riverbank for cryptologic instruction. As

Begin  
went

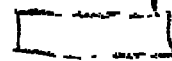
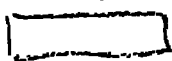
You may like to know what we regarded ourselves as instruction training material, well, there wasn't much but among the <sup>very</sup> sparse literature in English there was a small booklet entitled Manual for the Solution of Military Ciphers, which had been prepared by a Captain Parker Hitt and printed ~~at~~ by the ~~Seaworth~~ <sup>Army</sup> Press of the <sup>School</sup> Service Schools, Fort Leavenworth, in 1916. The Signal Corps, <sup>School</sup> was then a one of those ~~Service Schools~~ and there ~~at Leavenworth~~ a few lectures were given by two or three officers who, when World War I broke out in August 1914, took an interest in the subject of military ciphers. ~~Because they foresaw that sooner or~~ <sup>later there would</sup> be a need for <sup>immilitary</sup> knowledge and training. Capt. Hitt's Manual was then and still is a model of compactness and practicality. Here is its title page.

Fig. 00

It was the succinctness of the Manual that caused us ~~to sweat~~ <sup>work and</sup> much perspiration in our self-training. I later came to know and ~~very much~~ <sup>very much</sup> admire its author, whose photograph I show you.



There was one other item of training literature <sup>which we studied</sup> ~~avidly too,~~ a very small pamphlet entitled An Advanced Problem in Cryptography and its Solution, put out by the same Leavenworth Press in 1914. Here is its title page, and a photograph.



of its author, then 1st Lieut. J. O. Man Borgne, but later Chief Signal Officer of the Army. The advanced problem dealt with by that pamphlet was the Playfair cipher, about which I should say something later. If returning now to what be in NSA archives and a prediction prepared at Riverbank for this purpose. They are still of much interest historically.





principally between and among the headquarters of divisions and army corps.

In connection with the last-mentioned operations you will no doubt be interested to see what is perhaps one of the earliest, if not the very first chart <sup>in cryptologic history</sup> showing the results of traffic analysis, <sup>and its utility in deriving intelligence about</sup> enemy intentions from a mere study of the ebb and flow of enemy traffic.

Fig 00

This particular chart was drawn up from data based solely upon the ebb and flow of messages in what was called the ADFGVX cipher, <sup>\* a clever cryptosystem</sup> which was devised by German cryptographers and only used for German High Command communications. Theoretically it was <sup>extremely</sup> secure <sup>because it</sup> combined both <sup>a good</sup> substitution and <sup>an excellent</sup> transposition principle, <sup>in one and the same method without being too complicated for cipher clerks.</sup> Here is a diagram which, if ~~you~~ <sup>you</sup> study it ~~is no trick~~ <sup>carefully</sup>, you will give a clear understanding of its method of usage. If you should wish further details I suggest you consult documents available in <sup>the</sup> ~~the~~ Training Literature Department Division of the NSA Office of Training. In this lecture there is only time to tell you that although individual or isolated messages in that system appeared at that time to be absolutely unbreakable against solution, <sup>a great many</sup> ~~about 50%~~ <sup>messages</sup> ~~of all the~~

\* Initially this cipher employed only the letters A, D, F, G, and X, for a matrix 5x5; later, the letter V was added, for a matrix 6x6.

messages transmitted in the ADFGVX system were read by the Allies. You may be astonished by the foregoing statement and may desire some enlightenment here, and now on this point. Well, in brief, there were <sup>in those days three and only</sup> three different methods of attacking the traffic in that cipher. Under the first method two or more messages with identical beginnings/plain-text could be used to uncover the transposition as the first step. Once this had been done, the cryptanalyst had then to deal with a simple substitution in which two letter combinations of the letters A, D, F, G, V, X <sup>and</sup> represented single plain-text letters. The messages were usually of sufficient length for this purpose. Under the second method, two or more messages with identical plain-text endings could be used to uncover the transposition and this was even easier than in the case of <sup>messages with</sup> identical beginnings. You might think that cases of messages with identical beginnings or endings would be rather rare, but the stereotypic phraseology <sup>the</sup> in German military mentality was then - and perhaps still is - so conformal that cases were almost invariably found in each

day's traffic. This is astonishing considering that the keys changed daily. This system first came into use on 1 March 1918, three weeks before the last and greatest spring offensive by the German Army. Its appearance was almost coincident with that of other new codes and ciphers. The number of messages in the ADFGVX cipher varied from about 25 a day, when the system first went into use, to as many as about 150 at the end of two months. It took about a month to figure out a method of solution, and this was done by a very able French cryptanalyst named <sup>Capt<sup>George</sup></sup> <sup>Tauxem</sup> of the French Cipher Bureau.

The ADFGVX cipher was used quite extensively during May and June of 1918 but then the number of messages dropped very considerably. How many different keys were solved by the Allies? Not many — 10 in all, that is, the keys for only 10 different days were found. Yet, because the traffic on those days was heavy about 50% of all messages sent in that cipher were solved and a great deal of valuable intelligence <sup>was</sup> derived. On one occasion solution was so rapid that an important German operation dis-

closed by one message was completely frustrated.

Although the ADFGVX cipher came into use first on the Western Front, it later began to be employed on the Eastern Front, with keys that were first changed every two days but later every three days. On 2 November 1918 the key for that and the next day was solved within a period of an hour and a half because two messages with identical endings were found. A 13-part message in that key gave the complete plan of the German retreat from Roumania.

During the whole year of the life of the ADFGVX cipher, no general solution for it was devised by the Allies despite a great deal of study. However, members of the our own Signal Intelligence Service, in 1933, and while still students undergoing instruction in cryptanalysis, devised a general solution and proved its efficacy. ~~their~~ pride in their achievement was not diminished when, in the course of writing up and describing their method, a similar one was encountered in <sup>a book by French</sup> General Givierge (Cours de Cryptographie), published in 1925.

Solutions depended upon the three rather special cases mentioned.

an example of which is shown in Fig. 00. The process consists in applying the same transposition key twice.

The ADFGVX cipher was not the only one used by the German Army in World War I, and there will be time to mention only very briefly two others.

The first of these was a polyalphabetic substitution cipher, called "the Wilhelm," which used a cipher square with a set of 30 fairly lengthy keywords.

The cipher square is shown in Fig. 00 and the set of keys, as originally recovered, is shown in Fig. 00. Just why the square contains only 22 rows instead of 26 is unknown. Certainly

the rows within the square are not random sequences for the letters within them manifest permitted arrangements in sets of five; nor are the keys sequences of random letters. I leave it to you to try to reconstruct the real square and the real keys.

The latter problem should be relatively easy; as to the former, I really don't know — I have never tried it myself but I suspect some systematic disarrangement, something typical of German cryptography.

The other cipher to be mentioned is the double transposition, the true double transposition, usually depended upon finding two messages of identical length. No general solution was known to the Allies during World War I. Occasionally an operator would apply only the first transposition and when this happened solution was easy. Then the key thus recovered could be used to decipher other messages which had been correctly enciphered.

by the double transposition. Again, students of the Signal Intelligence Service devised a general solution for the double transposition cipher and during World War II were able to prove to our British Allies that such ciphers could be solved without having to find two messages of identical length. Having demonstrated <sup>the weakness of the system, even when</sup> ~~properly~~ <sup>probably</sup> employed, it was withdrawn from usage by the British, but we were not told directly that this was done. I should add that <sup>I think</sup> the devising of a general solution for the true double transposition cipher represents a real landmark of progress in cryptanalysis without the aid of high-speed, electronic equipment. I do not doubt that with such equipment this cipher could hardly be thought to be safe for modern <sup>military secrets</sup> communications.

We come now to the code systems used by the belligerents in World War I. And first, let us ~~review quickly what the Army~~ differentiate those used for diplomatic communications from those used for military communications. What parts did the German Foreign Office use? We have noted how the British Black Chamber, "Room 40 O. B." dealt

with stupendous success on the code used for the transmission of the Zimmermann Telegram. But that's only part of the story - the most important part remains to be told and unfortunately I cannot divulge that part yet. ~~But the version of that telegram as it passed from Washington to Mexico City was in one version of a basic code which had several other versions, all quite similar in basic construction and equally vulnerable to cryptanalytic attacks.~~ Excessive pride in German achievements, <sup>in a wholly unjustified confidence in their cryptosecurity,</sup> and a disdain for the cryptanalytic prowess of enemy cryptanalysts laid German diplomatic communications open to solution by the Allies to the point where <sup>there came a time when</sup> nothing the German Foreign Office was ~~thinking about~~ <sup>by telegraph, cable or otherwise</sup> ~~and telling~~ its representatives abroad <sup>remained</sup> ~~secret~~. For those of you who would like to learn some details, I refer you to the <sup>following</sup> fine monograph on the subject by <sup>my late colleague</sup> Charles J. Mandelsohn: Studies in German Diplomatic Codes Employed During the World War, Government Printing Office, 1937. This monograph is confidential; ~~and~~ copies are available in the Office of Training, NSA.

German codes were an unexplored field in the United States, says Dr. Mandelstam. "About a year later we received from the British a copy of a partial reconstruction of the German Code 13040 (about half of the vocabulary of 19,200 words and 800 of the possibly 7,600 proper names). This code and its variations or encipherments had been in use between the German Foreign Office and the German Embassy in Washington up to the time of the rupture in relations, and our files contained a considerable number of messages, some of them of historical interest, which were now read with the aid of this code book."

The vocabulary of the German diplomatic codes contained 189 pages containing exactly 100 words or expressions to the page,

arranged in two columns of 50 each accompanied by numbers from 00 to 99. In each column the groups were in blocks of 10, the pages in the basic code were numbered at the top, and derivative codes were made by the use of conversion tables. This enabled a single basic code to serve as a framework for several different communication nets.

Here is a copy of a typical page in Code 13040.

in the left-hand column, for instance, 00-09, 10-19, etc., to 40-49; then 50-59, etc.

from 10 to 339 and from this code several were made

by the use of conversion tables. This the original

upon the basic which enabled a single basic code to

serve as a framework for several different communication

nets. What the number of the basic code was is unknown, but we do know that from the derived code designated as 13040, a code designated as 5950, was derived

merely by means of tables for converting the page numbers in the basic code into different page numbers

in the derived code, and that these were tables for

converting the line numbers from 00 to 99 to

These conversions were systematic, in blocks of fours.

for example, Thus, pages 15-18 in 13040 became pages 65-68 in

code 5950; pages 19-22 in 13030 became pages 192-195 in

5950, etc. Then there were tables for converting line

numbers from one version to another version of the basic

and this was done in blocks of 10. For example, the fifth block (penultimate figure 4) became the first (penultimate figure 0), and the 1st, 2nd, 3rd, and 4th blocks were moved down one place.



The other five blocks (REF ID: A62844 and side of the page) were rearranged in the same manner.

It is obvious that codes derived in such a manner from a basic code <sup>can</sup> by no means <sup>be considered as</sup> ~~represent~~ ~~the equivalents of being different codes.~~ They were all <sup>relatively minor</sup> ~~as~~ the equivalents of ~~that~~ one another. Also to be mentioned is the fact that in certain cases 3-digit numbers were added to or subtracted from the code numbers of a message and that in practically every case it was not difficult to determine the additive or subtractive.

In none of the cases or codes mentioned thus far was there one that could at least be considered to be a randomized, "hatted", or true two-part code [etc. continue with p. 33]

Some of these, besides the ones already  
mentioned (13040 and 5950), were designated  
by indicators, such as 12444, 1357, 18470, 1777,  
2815, 4565, 5717, 44499, 58585, 2310,  
98989, 1111, 80574. There were  
others besides these. [Insert over]

true two-part code, since the same book served  
for both encoding and decoding. However, the German  
Foreign Office later, <sup>on just complete, and using</sup> ~~that~~ <sup>truly randomized</sup> true two-part codes of  
10,000 groups numbered from 0000 to 9999. One such code  
indicator the number had as its, 7500. And <sup>that</sup> <sup>several</sup> <sup>like it</sup> there were others. I have no doubt.

When one reviews Dr. Mendelsohn's  
monograph one <sup>becomes</sup> overwhelmed by the ~~sheer~~ <sup>and variants thereof</sup> multi-  
plicity of the codes used by the German Foreign  
Office. ~~Not~~ Many were basic, ~~and how many were~~ <sup>or superimphetic variants thereof.</sup> ~~ascertain the exact number of~~  
derivatives, <sup>is even hard to</sup> <sup>different methods.</sup> Yet a  
great deal of the traffic in these codes was  
read. Considering the rather small number  
of persons on the <sup>cryptanalytic</sup> staff of G-2 <sup>in Washington</sup> and its ~~homolo-~~  
gous organization in the London, in the British  
Black Chamber, one can only be astonished by  
the <sup>great</sup> achievements of the collaborative efforts  
of these two <sup>collaborating</sup> organizations during World War I.

~~So much for the German diplomatic  
cryptosystems. What about the German military  
cryptosystems? In this area we must credit the Germans  
with being first to decide that the old idea that  
a code could not be practically or safely employed  
in actual communications was not valid.~~

Insert

It is my belief that ~~the~~ conversion tables were not used by the code clerks but by the compiling authorities in Berlin. In other words, the various versions of the basic code were <sup>not</sup> actually printed as separate books, ~~so that Code + Data ~~was~~ ~~was~~~~ <sup>but that the original page number on each page was altered by hand, the original number being crossed out and ~~entirely different~~ <sup>entirely different</sup> in its appearance, the new number written either at the top or <sup>the</sup> bottom of the page, perhaps in both places. Similarly, the block numbers were <sup>probably</sup> changed by hand. In both cases the alterations were ~~system~~ <sup>systematic</sup> in accordance with some system, the idea of randomness seems foreign to the ~~German~~ <sup>German</sup> mentality, and ~~for the Germans never do anything by random~~ I am sure that if randomness were a desideratum they would figure out a system therefore.</sup>

So much for German diplomatic secret communications. What about German military cryptocommunications? In this area it is necessary to mention a situation which is somewhat unique. When World War I commenced the German Army was very poorly prepared to meet the requirements for secure communications. It seems that up until the Battle of the Marne in 1914 several German Army radio stations went into the field without any provision having been made or even foreseen for the need for <sup>speedy and secure</sup> cryptocommunications. Numerous complaints were registered by German commanders concerning extensive loss of time occasioned by the far too complicated methods officially authorized for use and the consequent necessity for sending messages in the clear. Not only did this reveal intelligence of importance to their opponents but what is equally important the practice permitted the British and the French to become thoroughly familiar with the German telegraphic procedures, methods of expression, terminology and style, and these items <sup>became</sup> of great importance <sup>when German cryptosystems improved.</sup> in cryptanalysis. For the German Army learned <sup>by hard experience</sup> ~~and learned rapidly because~~ its shortcomings in this area of warfare and began to improve to the point where we must credit the Germans with being the inventors of most of this new and very important development.

developments in <sup>field</sup> military cryptography. In fact, the develop-  
 ments and improvements began not long after the outbreak  
 of the Battle of the Marne ~~of the war~~ and continued steadily until <sup>of the war</sup> the end, when  
 on 11 November 1918 the armistice ended active operations,  
 German military cryptography had attained a remarkably  
 high state of efficiency. The astonishing fact, <sup>however,</sup> is that,  
 although very proficient in cryptographic invention,  
 they were apparently quite deficient in the science  
 and practice of cryptanalysis. In all the years since the  
 end of World War I no books or articles telling of German  
 success with Allied traffic during that war have appeared  
 save for one very brief article by a not very bright German  
 cryptanalyst. One could of course assume that they  
 kept their successes very well hidden but the German  
 archives taken at the end of World War II contain  
 nothing significant in regard to cryptanalysis during  
 World War I although a great deal of important  
 information in this field during World War II was  
 found. A detailed account of the <sup>cryptologic</sup> war between the  
 Allied and German forces in World War II would  
 require scores of volumes, but [continue over]

In this lecture, however, we are <sup>principally</sup> ~~only~~  
 concerned with German military cryptography  
 during World War I, and I have already told you

There is one source of information which I can highly recommend to those of you who would like to know more details of the cryptologic warfare between the belligerents in World War I. That source is a book written <sup>and published in Stockholm in 1931</sup> by a Swedish cryptanalyst, Yves Gylden, under the title Chifferbyråernas Insatser I Världskriget Till Lands, a translation of which, with some comments of my own in the form of footnotes, you will find on file in the Office of Training, NSA, under the title The Contribution of the Cryptographic Bureaus to the World War, Government Printing Office, 1936.

something about the cipher systems that were used. There remain to be discussed the field codes. It was the German Army which first proved that the old idea that codebooks were impractical for use in the combat zone for tactical communications was wrong. They had two different types of field codes, one we called the "three-number code" which the Germans called the SCHLUESSELHEFT of "key" and the Germans called the SATZBUCH or "Sentence Book" but which we called the other, the "three-letter code". The former was a small standardized code with a frequently-used vocabulary of digits, letters and syllables totaling 1,000 words and expressions, which the code equivalents were 3-digit numbers. A cipher was applied only to the first two digits of the code numbers and this cipher consisted of a 10 x 10 matrix for the numbers from 00 to 99. The last digit of a code group remained unenciphered. Each division compiled and issued its own table, which was in two parts, one for encipherment the other for decipherment. The three-number code was intended for use in all forms of communication within or to and from a 3-kilometer front-line danger zone. Although this code was compiled by the end of January 1918 it was not put into use until the opening day of the last and greatest German offensive 10 March 1918. The nature of the new code was so essential and a few groups in it were solved the very same day because an operator who was

Here copy p. 3 of  
Field Codes used by the  
German Army



unable to translate a message in the <sup>new code</sup> requested and  
 received a repetition in the old code, the three-letter code, and  
 the latter had been solved to an extent which  
 made it possible to identify homologous code  
 groups in both messages. The three-number proved  
 rather easy to solve on a daily basis and much  
 useful intelligence was obtained thereby.

The <sup>solution of the</sup> three-letter code, however, proved  
 much more difficult. In the first place, it had a  
 much larger vocabulary, with nulls and many  
 variants for frequently-used words and numbers;  
 in the second place, ~~and what constituted~~  
~~but what became~~ the real stumbling block to  
 solution was the fact that it was a true two-  
 part randomized or "hatted" code; and in the  
 third place, each sector of the front used a  
 different edition of the code, so that traffic  
 not only had to be identified ~~but~~ as to the  
 sector from which it belonged but also it  
 was not possible to combine all the messages for  
 the purpose of building up frequencies of usage  
 of code groups. Working with the sparse  
 amount of traffic <sup>within</sup> a quiet sector of the front  
 and trying to solve a few messages in this code  
 was really a painfully slow, very difficult and

generally frustrating experience. On my reporting for duty Colonel Frank Moorman, who was chief of the whole unit and whose photograph I show you here, asked me whether I wished to be assigned to the cipher ~~section~~ section or to the code section. Having had considerable experience with the solution of the former types of cryptosystems but none with the latter, and being desirous of gaining such experience I chose ~~to be~~ <sup>to be</sup> assigned to the code solving unit. I gained the experience I wanted and needed to broaden <sup>knowledge and practice in</sup> my cryptology but little did I realize what ~~it was~~ a painful and frustrating period of learning and training I had undertaken. Still, I have never regretted the choice I made; in fact, it turned out to be a very wise and useful one. If any of you would like to read about my experience in this area, let me refer you to my monograph entitled Field Codes Used by the German Army during the World War, copies of which are on file in the Office of Training, NSA. I will quote a few [insert over]

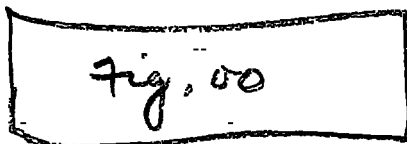
What sort of cryptosystems did the French Army use? First, as for ciphers, they put

Insert

paragraphs from my "estimate of the three-letter  
code" ~~taken~~ as it appears on p. 65 of that monograph;

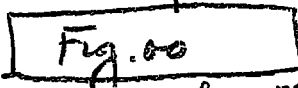
p. 65

much trust in transposition methods and here is an example of one type:

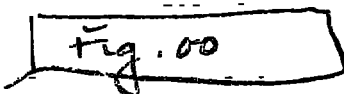


or an "Abbreviated Codebook!"

As for codes, like the Germans they <sup>called it "Carnet Reduit"</sup> used a small front-line booklet, <sup>had different editions</sup> of the front, and I will show a picture of one of them. Then, in addition, there was a much more extensive ~~the~~ code which was not only a two-part, randomized book <sup>of 10,000 four-digit code groups</sup>, but a superencipherment was applied to the code messages when transmitted by radio or <sup>by</sup> "TPS", that is, "telegraphic parol", or earth telegraphy. Here is one of the tables used for enciphering (and deciphering) the code groups:



And here is the example <sup>of superencipherment</sup> given in the code in my collection:



You will notice that the enciphering process breaks up the 4-digit groups in a rather clever manner by <sup>enciphering</sup> making the first digit of the first code group separately; the second and third

digits of the first group are enciphered as a pair; then the last digit of the first group and the first digit of the second code group are enciphered as a pair, and so on. This procedure succeeds in breaking up the <sup>digital</sup> code groups in such a manner as to reduce very greatly the frequency of repetition of 4-digit groups representing words, numbers, phrases, etc. of very common occurrence in military messages. My appraisal of this French Army cryptosystem is that, <sup>theoretically at least,</sup> it certainly was the most secure of all the systems used by the belligerents but I don't know how much usage was made of it. ~~But~~ I venture the opinion that it was not used often, or successfully, with the superenciphering method provided for the basic code.

Now how about the cryptosystems used by the British Army? First, they used the Playfair Cipher, a system of digraphic substitution considered in those days to be good enough for unimportant messages in the combat zone. But today, of course, its security is known to be so low as to be unworthy of placing any reliance in it. The British also used a field code. It ~~was~~ contained many common military expressions and sentences, grouped under various

headings or categories, and, of course, a very small vocabulary of frequently-used words, numbers, punctuation, etc. It was always used with super-encipherment, the nature of which was not disclosed even to their allies, so I unfortunately am not in a position to describe it. I don't <sup>even</sup> have a copy of their code - only a typewritten transcript which was furnished us quite reluctantly and I will show a typical page thereof.

Fig. 00

~~What about the cryptosystems used by the Italian Army? You may find it hard to believe but it was a simple variant of the very old Vigenere cipher and I show you a picture of it here:~~

~~Fig. 00~~

~~Whether a code book was used in addition, I do not know.~~

What about the cryptosystems used by the Italian Army in World War I? The general level of cryptologic work during that period was quite low in character, a fact which is all the more remarkable when we consider that the birthplace of modern cryptology was in Italy several centuries before this period. There appears to have been <sup>in Italy a far greater</sup> knowledge of cryptologic techniques in the 15th and 16th Centuries than in the 19th, paradoxical as this may seem to us today. Perhaps this can be considered as one of the consequences of a policy of secrecy which not only <sup>it makes</sup> filing away in dusty archives records of cryptanalytic successes a desideratum but also ~~prevents~~ hinders or absolutely prevents those who might have been born with what it takes to ~~pass~~ develop a flair for cryptologic work from profiting from the progress of predecessors who have been successful in such work. Should we be astonished to learn, therefore, that when Italy entered into World War I the Italian Army put its trust in a very

Simple variation of the ancient Vigenere cipher, a system called the "cifrario militare tascabile" or the "pocket military cipher"? It, as well as several others devised by the same Italian "expert", were solved very easily by the Austrian cryptanalysts during the war. The Italian Army also used codes, no doubt, but since encipherment of <sup>such</sup> codes consisted in adding or subtracting a number from the page number on which a given code number group appeared, the security of such systems was quite illusory. As late as in 1927 the <sup>same</sup> Italian "expert" announced his invention of an absolutely indecipherable cipher system which, Gylden says (p. 23) "still further demonstrates the astonishing lack of comprehension of modern cryptanalytic methods on his part."

What about Russian cryptologic work in World War I? So far as Russian cryptographic work is concerned we know that there was during Czaristic days an apparently well organized and effective ~~blank~~ <sup>constructing and compiling</sup> bureau for diplomatic codes and ciphers, organized by a Russian named Savinsky,

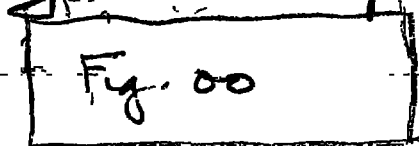


formerly Russian minister to Stockholm. He had all codes and ciphers in use up to then improved, introduced strict regulations for their use, and kept close watch over the service. He also was head of a cryptanalytic activity, and it is known that Turkish, British, Austrian and Swedish diplomatic messages were solved. After the Bolshevik revolution of 1916 some of the Russian cryptanalysts managed to escape from their homeland and I had the pleasure of meeting and talking with one of the best of them during his service in the ~~courts~~ black chamber of one of our allies in World War II. He wore with great pride on the index finger of his right hand a ring in which was mounted a beautiful large ruby, the ring having been presented him by the last Czar in recognition of his cryptanalytic successes while in his service.

But the story is altogether different as regards cryptology in the Russian Army. The military cryptographic service was poorly organized and, besides, it had adopted

enciphering the first set of letters (5, 7, etc), according to the indicator (by alphabet 1, the next set by alphabet 2, and so on). After the 8th set of letters which was enciphered by cipher alphabet 8, return is made to cipher alphabet 1, repeating the sequence in this manner until the entire message had been enciphered.

a cryptographic system which proved to be too complicated for the ignorant and poorly trained Russian cipher and radio operators to use when it was placed into effect toward the end of 1914. Here is an example of that cipher, which has an enciphering and a deciphering table:



In the enciphering table the <sup>letters of the</sup> Russian alphabet appear in the top line; the 2-digit groups <sup>in random order</sup> within the 8 rows below are their cipher equivalents and these ~~are in random order in each row~~, thus rows therefore constitute a set of 8 cipher alphabets ~~each of which~~ is preceded by a key number from 1 to 8 in random order, also subject to change. Indicators were used <sup>consecutively</sup> to indicate how many letters were enciphered in each alphabet, the indicator consisting of one of the digits from 1 to 9 repeated five times. The alphabets were then used in key-number sequence, in enciphering a long message the cipher operator could change the number of letters enciphered consecutively by inserting another indicator repeated five times and then continuing with the next alphabet in the sequence of alphabets. The cipher

text was then sent in 5-digit groups. The use of the deciphering table hardly requires explanation but a <sup>question</sup> ~~comment~~ may be in order: Why ~~was there an~~ <sup>the</sup> aversion to the use of zero and to the use of double digits such as 11, 22, 33, etc? This remains a puzzle to me.

I have told you that this cipher system proved too difficult to use, so difficult that messages had to be repeated over and over, with great loss of time. It is well known ~~was~~ that the Russians lost the Battle of Tannenberg in the autumn of 1914 was largely because of faulty communications. Poor cryptography or failure to use even simple ciphers properly on the field of battle, and not brilliant strategy on the part of the enemy, was the cause of Russia's defeat in that and in subsequent battles. The contents of Russian communications became known to the German and Austrian High Commands within a few hours after transmission by radio. The dispositions and movements of Russian troops, and Russian strategic plans were no secrets to the enemy. The detailed and absolutely reliable information obtained by intercepting and reading the Russian communications made it very easy for the German and Austrian commanders not only to take proper counter-measures to prevent the execution of Russian plans, but also to launch attacks on the weakest parts of the Russian front. Although the Russian ciphers were really not complicated their cipher clerks and radio operators found themselves unable to exchange messages with accuracy and speed. As a matter of fact they

were so inept that not only were their cipher messages easily solved but also they made so many errors that the <sup>intended</sup> recipients themselves had considerable difficulty in deciphering the messages even with the correct keys. In some cases this led to the use of plain language, so that the German and Austrian forces did not even have to do anything but intercept the messages and translate the Russians. To send out dispositions, <sup>impending</sup> movements, immediate and long-range plans in plain language was, of course, one cardinal error. Another was to encipher only words and phrases deemed the important ones, leaving the rest in clear. Another cardinal error, made when a cipher was superseded, was to send a message to a unit that had not yet received the new key and then repeat the identical message in the old one. I suppose the Russians committed every error in the catalog of cryptographic criminality. No wonder they lost the Battle of Tannenberg, which one military critic said was not a battle but a massacre, because the Russians lost 100,000 men in the 3-day engagement, on the last day of which the Russian Commander-in-chief committed suicide. Three weeks later another high Russian commander followed suit,

P. 46 ~~is~~  
Continued

and the Russian Army began to fall apart, completely disorganized, without leadership or plans. Russia itself began to go down in ruins when its Army, Navy and Government failed so completely, and this made way for the birth of the October revolution, ushering in a regime that was too weak to put things together again and to hold them together. The remnants, picked up by a small band of fanatics with military and administrative ability, with treachery, violence and cunning, welded together what has now become a mighty adversary of the Western World, the USSR.

I have left to be treated last in this lecture the cryptosystems used by the American Expeditionary Forces in Europe during our participation in World War I.

When the <sup>first</sup> contingents of the AEF arrived in France in the summer of 1917, there were available for secret communication within the AEF but three authorized means. The first was that extensive code for administrative telegraphic correspondence, the 1915 edition of the War Department Telegraph Code about which I've already told you something. Although it was fairly well adapted for that type of communication, it was not at all suitable for rapid and efficient strategic or tactical communications in the field, nor was it safe to use without a clumsy superencipherment. The second cryptosystem available was that known as the repeating-key cipher, which used the Signal Corps Cipher Disk, the basic principles of which were described as far back as about the year 1500. The third system available was the Playfair Cipher, which had been frankly copied from the British, who had used it as a field cipher for many years before World War I and continued to use it. In addition to these authorized means there were from time to time current in the AEF apparently several - how many,

no one knows - unauthorized, locally-improvised "codes" of varying degrees of security, mostly nil. I show one of these in Fig. 00, and will let you assess its security yourself.

Fig. 00

Seen in retrospect, when the AEF was first organized it was certainly unprepared for handling secret communications in the field, but it is certain that it was no more unprepared in this respect than was any of the other belligerents upon their respective entries into World War I, as I've indicated previously in this lecture. This is rather strange because never before in the history of warfare had cryptology played so important a role. When measured by today's standards it must be said that not only was the AEF unprepared as to secret communication means and methods and as to crypt-analysis, but for a limited time it seemed almost hopeless that the AEF could catch up with the times, because their British and French allies were at first most reluctant to disclose much of their hard-earned information about these vital matters.

Nevertheless, and despite so inauspicious a commencement, by the time of the Armistice, in

November 1918, not only had the AEF caught up with their allies but they had surpassed them in the preparation of sound codes, as may be gathered from the fact that their allies had by then decided to adopt the AEF system of field codes and methods for their preparation, printing, distribution, and usage.

Just as the invention of Morse wire telegraphy had a remarkable effect upon military communications, during the American Civil War, as related in the preceding lecture, so the invention of radio also played a very important role in field communications during World War I. Now, although it can hardly be said that all commanders from the very earliest days of the use of radio in military communications, <sup>acutely</sup> recognized one of the most important disadvantages of radio - namely, the fact that radio signals may be more or less easily intercepted by the enemy - it was not long before the consequences of a complete disregard of this obvious fact impressed themselves upon most commanders, with the result that the transmission of plain language became the exception rather than the rule. This gave the most momentous stimulus to the development and increased use of cryptology that this service had ever experienced.



Let us review some of the accomplishments of the Code Compilation Service under the Signal Corps, AEF. It was organized in January 1918, and consisted of one captain, three lieutenants and one enlisted man. Until this service was organized, that is, from the summer of 1917 until the end of that year the AEF had nothing for cryptocommunications except those three inadequate means I've mentioned. When it had been determined that field codes were needed little time was lost in getting on with the job that had to be done. Since I had no part in this effort I can say without danger of being misunderstood as to motives, that the Code Compilation Service executed the most remarkable job in the history of military cryptography up to the time of World War II.

The first work entrusted to it was the compilation of a ~~first-class~~ "Trench Code", of which 1000 copies were printed, together with what were called "distortion tables." These were simple monoalphabets for enciphering the 2-letter groups of the ~~code~~ code. I show a picture of a page of this code and of one of the "distortion tables."

Fig. 10

(p. 13)

Fig. 00

(p. 142)

The danger of capture of these codes was recognized as being such that the books were not issued below battalions. Hence, to meet the needs of the front line, a much smaller book was prepared and printed, called the "Front Line Code". Distortion tables, 30 of them in all, were issued to accompany this code, of which an edition of 3,000 copies was printed — but not distributed, because a study of its security showed defects. AEF cryptographers were groping in the dark, with little or no help from allies and with <sup>personnel</sup> inexperienced in cryptanalysis. Finally, the light broke through: the Code Compilation Service began to see the advantages of the German 3-letter randomized 2-part code known as the Satzbuch. I've told you about this code and what the AEF learned about its advantages. Here, then, was the origin of the AEF real Trench Codes — copying from the experience of German code compilation and then going them one better. The first code of the new series, known as the "Potomac Code", the first of the so-called "American River Series", appeared on 24 June 1918, in an edition of 2,000 copies. It contained approximately 1,700 words and phrases and, as the official report

so succinctly states, "was made up with a coding and decoding section in order to reduce the work of the operators at the front". The designation "two-part" or "randomized", or even "hatted" code was still unknown — but the principle was there, nonetheless. Let us see what the official report goes on to say on this point; let us listen to some sound common sense:

"The main point of difference from other Army codes lay in the principle of reprinting these books at frequent intervals and depending largely upon the rapidity of the reissuance for the secrecy of the codes. This method did away with the double work at the front of ciphering and deciphering [sic!], and put the burden of work upon general headquarters, where it properly belonged. Under this system one issue of codes could be distributed down to regiments; another issue held at Army Headquarters; and a third issue held at General Headquarters. As a matter of record this first book, the Potomac, was captured by the enemy on July 20, just one month after issuance, but within two days, it had been replaced throughout the entire Army in <sup>the</sup> field."

The replacement code was the Suwanee, the next in the River Series, followed by the Wabash, Allegheny, and the Hudson, all for the American First Army. In October 1918 a departure in plan was made and different codes were issued simultaneously to the First and Second Armies. This was done in order not to jeopardize unnecessarily the life of the codes by putting in the field at one time 5,000 and 6,000 copies of any one issue. Thus the Champlain, the first of what came to be called the "Lake Series" <sup>for the Second Army</sup> was issued with the Colorado of the "River Series" for the First Army; these were followed by the Huron and the Osage, the Seneca and the Niagara, in editions of 2,500 each.

In addition to the foregoing series of codes were certain others that should be mentioned, as for example, a short code of 2-letter code groups to be used by front line troops as an emergency code; a short code list for reporting casualties; a telephone code for disguising the names of commanding officers and their units, and so on. But there was in addition to all the foregoing one large code that must be mentioned, a code to meet the requirements for secure transmission of message among the higher commands.

in the field and between these and G.H.Q. This was a task of considerable magnitude and required several months' study of messages, confidential papers concerning organization, replacement, operations, and of military documents of all sorts. The code was to be known as the AEF Staff Code. In May 1918 the manuscript of this code was sent to press and the printing job was done in one month by the printing facilities of the AEF Adjutant General. Considering that the code contained approximately 30,000 words and phrases, accompanied by code groups consisting of 5-figure groups and 4-letter groups the task completed represents a remarkable achievement by <sup>an</sup> field printing organization and I believe that this was the largest and most comprehensive codebook ever <sup>compiled and</sup> printed by an army in the field. More than 50,000 telegraphic combinations were sent in tests in order to cast out combinations liable to error in transmission. One thousand copies of this code were printed and bound. With this code as a superencipherment system there were issued from time to time "distortion tables". There remain only to be said that the war was over before this

Code could be given a good work-out, but I have no doubt that during the few months it was in effect it served a very useful purpose. Moreover, the excellent vocabulary was later used as a skeleton for a new War Department Telegraph Code to replace the edition of 1915.

One more code remains to be mentioned: a "Radio Service Code", the first of its kind in the American Army. This was prepared in October, to be used instead of a French code of similar nature. Finally, anticipating the possible requirement for codes for use by the Army of Occupation, a series of three small codes, identical in format with the war-time trench codes of the river and lake series, was prepared, and printed. They were named simply Field Codes No. 1, 2, and 3, but were never issued because there was turned out to be no need for them in the quietude in Germany after the Army of Occupation marched into former <sup>enemy</sup> ~~hostile~~ but now very friendly territory.

I will bring this lecture to a close now by referring those of you who might wish to learn more about the successes and exploits of the cryptographic organization of the AEF

REF ID: A62846  
Copies are on file in the Office of  
Training.

in World War I to my monograph entitled  
American Army Field Codes in the American Expeditionary  
Forces during the First World War, Government  
Printing Office, 1942. In <sup>that monograph</sup> you will find many  
details of interest which I have had to omit  
in this talk, together with many photographs of  
<sup>the</sup> codes and ciphers produced and used not only  
by the AEF but also by our allies and enemies  
during that conflict.

~~SECRET~~A. Important Contributions to Communications Security, 1939-1945.

1. Converter M-134 A--On 25 July 1933 a secret patent application (Serial No. 682,096) was filed by the Chief Signal Officer, on my behalf, covering Converter M-134-T2, the predecessor of Converter M-134 C (Sigaba). The principle disclosed in Serial No 682,096 is of highest importance in that it was the first invention and disclosure covering Electrical control (as distinguished from mechanical control) of a set of cipher rotors in cascade, permitting a departure from the regular and periodic or metric angular displacements of such cipher rotors. The following is quoted from a Secret Navy report\* on the history of the development of the Sigaba (ECM):

"However, under date of 25 July 1933, The Chief Signal Officer filed on behalf of Friedman a patent application (Serial No. 682,096) covering a cryptographic system and machine in which the stepping of the code wheels was very irregular and under the control of a keying tape. Electric Control thus made its first appearance!"

A complete assignment of all rights to my invention was made to the Secretary of War on 10 September 1936, and the patent application was placed in the secret category on 9 September 1936, where it still remains.

Two service test models of Converter M-134-T2 were constructed by the Signal Corps Laboratories at Fort Monmouth, New Jersey in 1936 and service tests were conducted by an exchange of cryptograms between the War Department, Washington, and The Panama Canal Department, Balboa, C.Z., in November 1936. It demonstrated that the machine was operable at the rate of 30-35 words per minute and afforded the highest degree of security yet attained by any cryptographic machine for cryptonet communication (multiple holders of the same cryptographic key).

On 19 February 1937 the military characteristics of Converter M-134 were approved, soon thereafter a contract for the construction of 12 machines was placed with Wallace and Tiernan, Indiana, of Belleville, New Jersey. The machines were delivered to Washington on 2 August 1938.

I developed and wrote the cryptographic keying instructions and in October 1938 first shipment was made of the machines, two each, for the Headquarters of the Ninth Corps Area (San Francisco), Panama Canal, Hawaiian, and Philippine Departments. Four machines were kept in Washington. The machines were promptly put into service for all the highly secret communications between the War Department and the headquarters indicated. Later, as more machines became available, a further distribution was made to equip all Corps Areas and Departments, including the Puerto Rican, with a sufficient number of machines to meet

Declassified and approved for release by NSA on 07-18-2013 pursuant to E.O. 13526

\* See Enclosure labelled "Exhibit 4"

~~SECRET~~



~~SECRET~~

requirements. Eight machines were placed in the War Department Code Center. Only 75 of these machines were built in all but they formed the backbone of the quipment for high command secret and confidential communications of the War Department and the Army from the date of their introduction into service until the end of 1941, when they were replaced by Converter M-134-C, the Sigaba. In 1940 the War Department sent by special officer courier two of these machines to the U. S. Military Attache in London, to meet the very urgent needs for high speed, high-security communication between Washington and London. Later two more were sent there, making four for the Military Attache.

On 29 November 1941 the War Department provided the Department of State with four machines, two for Washington and two for the American Embassy in London; later on, four or more additional machines were provided the Department of State. During the vital years 1940-1942, confidential and secret intercommunication between these two points and among the offices indicated could not have been successfully conducted without these machines.

In January 1942 arrangements were made to use the M-134-A for direct communication between the President and the British Prime Minister and it was used for this purpose for a number of months. Later this machine in that circuit was replaced by Converter M-134 C, in a special adapter made under my supervision by the Signal Corps and the Western Union. This permitted of high speed, secure communication between the White House and Downing Street at a very critical period.

The M-134 was also used to a large degree by the Signal Intelligence Service itself for forwarding intercept traffic to Washington from overseas intercept stations. It replaced Cipher Device M-138 for this purpose and thus greatly facilitated the prompt receipt of the raw traffic for cryptanalysis.

Later on, a number of them (totaling 29 or 30 at the end) as they became available, were provided the Office of the Coordinator of Information (later the Office of Strategic Services) for secret communication between Washington, London and other capitals where the OSS maintained headquarters. Some of these machines (about 16) maybe and probably are still in service.

During the years from 1939 to 1942, when Converter M-134 was replaced by Converter M-134-C (Sigaba) it is doubtful if the voluminous secret and confidential traffic of the highest echelons of the Army and the War Department could have been handled as successfully as it was, had it not been for the invention, development and availability of this machine.

There is not a scrap of evidence in Ticom reports that either the Germans or the Japanese or any other government was able to solve any of the traffic enciphered by this machine.

~~SECRET~~

~~SECRET~~

2. Converter M-134-C (Sigaba).--In the course of studies of Converter M-134-T2 and before manufacture of the latter machine was well under way, my principal assistant, Mr. Frank B. Rowlett, and I investigated various means of improving the cryptographic machine with a view to eliminating the perforated tape which controlled the aperiodic stepping of the rotors. Various schemes were studied, including cam wheels with different diameters and variable "off" and "on" pin arrangements. About 15 June 1935 Rowlett conceived an idea which finally resulted in making it possible to eliminate the tape control. Basically his invention was that of using a set of rotors as a key generator, that is, using the rotors to generate a long keying sequence by sending electrical impulses through a set of rotors which themselves were caused to step in a regular manner. The successive elements of the keying sequence, as they were generated could control the stepping of the rotors actually employed to encipher the letters of the message to be enciphered. Rowlett and I then jointly developed the idea by setting down on paper various methods by which it could be applied to replace the tape control employed in Converter M-134-T2, and although no models were built the results of our theoretical studies were incorporated in a patent application filed on 23 March 1936 (Serial No. 70,412) in our name as joint inventors. A complete assignment of the invention to the Secretary of War was made on 2 April 1936 and the patent application was placed in the secret category, where it still remains.

The Navy was then trying to improve its own machine (Mark I E C M), the security of which was unsatisfactory. Though this machine generated a long keying sequence the number of available starting points in that sequence was so limited that considerable "depth", that is, messages enciphered in exactly the same key, could be expected every day and thus solution potentially made relatively easy. On three occasions, at Navy request, the drawings and principles later embodied in Serial No. 70,412 were shown and explained to Navy representatives several times in October and November of 1935, with the result that the Navy initiated a development contract with the Teletype Corporation and work thereon was started in January 1938. This was done, however, without advising us or anybody else in the Signal Corps until March 1939, when the Teletype Corporation engineers brought to Washington the first completed set of drawings of the Mark II E C M. Rowlett and I were invited to the conference with the Teletype engineers and in the course of the discussions it was brought out and acknowledged that the Navy had based the cryptographic features of the new machine upon the Army's disclosure. A first model was then built and delivered on 3 February 1940, when Major General Mauborgne, then Chief Signal Officer, Rowlett, and I were invited by Admiral Noyes and Captain Safford to see the model. On that occasion Captain Safford acknowledged, in the presence of all those witnessing the demonstration, the fact that the Navy had used the Friedman-Rowlett invention. Further development of the machine was thereafter on a joint Army-Navy basis, and on 19 June 1940 the Signal Corps added its order of an initial 85 machines to the Navy order, at a cost of \$1856.90 each.

~~SECRET~~

~~SECRET~~

The Mark II ECM (Navy nomenclature)—Converter M-134-C was adopted by the Army to replace Converter M-134 A, not because the former might afford greater security than the latter but because the M-134 C was not only a much more rugged, reliable and rapid machine but also because it dispensed with perforated tapes, thus being more practical than the M-134 C. The following is quoted from the Navy Department's "History of the ECM:"

"Electric control of the ECM by means of the Friedman-Rowlett 'Stepping Maze' is the essential feature that places the Mark II ECM in a class by itself as regards security."

On 17 March 1941 the first 10 machines were delivered to the Signal Corps and were given a prompt service test, which proved the machines to be highly satisfactory. On 4 October 1940 action was initiated by the Signal Corps to procure an additional 149 machines, and thereafter, in successive contracts several thousand more of them were procured, the production schedule in July 1942 calling for the delivery of the machines to the Signal Corps at the rate of 150 per month. By 31 August 1942 a total of 373 Sigabas had been delivered and 364 were already in service; by 30 April 1943 the total number ordered was 1867, the number delivered was 862, and the number in use 807; by 28 March 1944 a total of 333 machines had been ordered, 1827 delivered, and 1681 were in service. In all, the Signal Corps actually procured a total of 3392 of these machines for Army use, and the Navy procured more than that number for Navy use. In the Army the machines were distributed to all commands down to and including headquarters of Divisions. They were also used in all the important fixed headquarters in the Communications Zone, in all theaters and in the U. S. Under special precautions they were used in U. S. installations in foreign countries where we had no troops, as for example, in Moscow, for our special military mission. Whenever and wherever the late President went during the war, the Sigaba went too. They were installed in the late President's signal center whenever he visited his home at Hyde Park; they were on board the Presidential Train, etc.

The fact that identical machines were employed by the Army and the Navy at all high and intermediate headquarters not only speeded up the exchange of classified messages of all categories (secret, confidential, and restricted) within each of the Services but also facilitated Joint Communications. The following is also quoted from the Navy's History of the ECM:

"This use of an identical machine with interchangeable code wheels has been of great military value, particularly in the early stages of the war, when distribution of machines and code wheels was incomplete. In the Philippines, Java, Australia, and even in North Africa, Navy wheels have been used in Army ECM's, Army Wheels in Navy ECM's; machines have been borrowed back and forth between the two services; Army messages have been sent in Navy ECM ciphers and Navy messages sent in Army ECM ciphers."

~~SECRET~~

~~SECRET~~

We know now from Ticom reports that neither the Japanese nor the Germans had the slightest success in their efforts to solve messages in the Sigaba, though the Germans certainly tried hard enough. The absolute security of Army and Navy high command and high echelon communications throughout the war was made possible by the Sigaba. In view of the fact that the high-level communications of the German, Italian, and Japanese Governments and Armed Forces were successfully attacked by the U. S. and the British communications intelligence staffs, and that the intelligence resulting therefrom was of highest diplomatic, strategic, and tactical importance, whereas our own high-level communications were inviolate, it may be said that the Sigaba contributed materially to the successful outcome of the war.

3. Converter M-228 (Sigcum, Sighuad).--The need for a cryptographic mechanism to protect land-lines teletype communications was felt even in World War I. In 1936 the Army was anxious to have something practical developed for this purpose and studies that had been underway for a number of years culminated in 1939, when Rowlett and I, applying Rowlett's idea of using cascade rotors as a key generator, then jointly conceived the principles underlying what later became Converter M-228 (Sigcum). Patent Application Serial No. 443,320 was filed on 16 May 1942; assignment of rights to the Secretary of War was signed on 13 May 1942 and the application was placed in the Secret category, where it still remains.

On 16 July 1941 military characteristics were approved by The Adjutant General and the Signal Corps Laboratories at Fort Monmouth, New Jersey, undertook the development. On 12 March 1942 a satisfactory service test and working demonstration of the first two models of Converter M-228 was made; one machine was at Fort Monmouth, the other at the Bell Laboratories, New York City. The provided for automatic on-line keyboard encipherment, transmission, reception, decipherment and printing of messages at the rate of over 360 characters (= approximately 60 words) per minute, with good security.

On 7 April 1942 the budget for FY 1943 included provision for procurement of 2400 machines at \$500 each, a total of \$1,200,000.

On 18 June 1942 representatives of the Signal Corps and the Navy witnessed a demonstration of the machine in New York and as a result the Navy decided to procure 200 for its use.

On 24 November 1942 action was initiated to purchase 1467 machines and on 25 December the first 10 machines were shipped from the factory to Washington.

~~SECRET~~

~~SECRET~~

Although Converter M-228 was not intended for radio-teletype usage, the urgent need for speed in overseas communications and the availability of radio-teletype circuits practically forced the use of the machine on these circuits to protect these communications. On 9 January 1943 the first official message using Converter M-228 on a radio circuit was sent from Washington to Algiers, and thereafter extensive use of the machines for radio-teletype communications was made, although it was decided, for security reasons, to transmit only confidential and restricted messages by this means. (Secret and Top Secret Messages had to be enciphered by Sigaba or by Sigtot, the one-time tape System).

By 11 September 1943 a total of 3867 machines had been ordered, and 3044 had been manufactured. The rate of production was 500 per month. By that date the "stop-gap" teletype-encipherment system using two short loops of key tape was discontinued, because general distribution of the M-228 had been completed. On 31 May 1943 the A. C. of S., G-2, War Department, approved the installation of this machine for use on the Defense Teletypewriter Network linking the several U. S. Army Headquarters in the United Kingdom.

In April 1944 the War Department approved a policy under which the machine could be turned over to the British for the specific purpose of use in Combined Operations; and on 23 May 1944 the A. C. of S., G-2, War Department, approved disclosure of the principles of the machine to the British.

By 5 June 1944 a total of 3200 of these machines had been built and 1488 issued for use, including 200 to the Navy. The machine was employed to encipher a tremendous volume of traffic, including raw material for cryptanalysis from all intercept stations. Under the special conditions and with some modification (Sighuad) the machine was also used in special circuits in Washington, between Arlington Hall Station, the Military Intelligence Service in The Pentagon, of the highest classification. This same modification (Sighuad) permitted the machine to be used by the Air Forces in the U. S. and in the Pacific, to transmit, by radio meteorological and weather data, thus greatly facilitating operations.

The British did not have any machine similar to the Sigcum or Sighuad and only at the end of the war was their long-standing desire to be able to use it granted. The Germans had teletype encipherment equipment but a large volume of traffic in the various types of machines they built was solved and read on a current basis by the British. Toward the end of the war the Germans had improved models which resisted solution, but they came too late. The Japanese had no such equipment at all.

~~SECRET~~

~~SECRET~~

Results of Ticom operations have established that neither the Germans nor the Japanese were successful in their efforts to solve our Sigcun traffic, despite its great volume, and it is my belief that had we used this machine for secret radio-teletype communications no serious harm to our security would have followed. Although it was not used for secret radio-teletype communications, the machine was nevertheless widely used for secret, confidential, and restricted communications by land-line teletype and for a great volume of confidential and restricted communications by radio-teletype in the U. S. as well as in all overseas theaters. The Sigquad version of this machine was, however, used to a limited extent for secret traffic by radio. Had we not possessed such a machine our rapid communications would have been severely handicapped by the necessity of encipherment by slower means.

4. Cipher Device Type M-138.--Early experiments with the old cylindrical Cipher Device M-94, which had been introduced into the U. S. Army and U. S. Navy in about 1922, began in about 1933. Various modifications, in the form of a flat cipher device using variable, instead of fixed alphabets, were made, culminating in a device on which a patent application in my name was filed (Serial No. 300,212) on 19 October 1939. On 16 July 1940 the application, which the usual license rights were assigned to the Government on 16 October 1939, was placed in the secret category under the provisions of the Act of 6 October 1917 as amended 2 July 1940.

About five thousands of these devices were manufactured under War Department Contracts. They were used throughout the war and are still used by a large number of military fixed and mobile headquarters. In fact, until the manufacture of the automatic cipher machine (Sigaba) had progressed to the point where a sufficient number had been produced to meet distribution requirements, the Strip Cipher System using Cipher Device M-138 formed the backbone of Army Secret and Confidential communications; thereafter it served and still serves as the secondary or back-up system for the holders of the Sigaba. For stations not equipped with the Segaba the Strip Cipher System still constitutes the principal means for such communications. At the present in the U. S. all Posts, Camps and Stations use this device as the primary cryptographic means. Until recently it was also the primary means for communication between the War Department and all Military Attaches as well as for intercommunication among military attaches; at present it is employed only for circular messages to or among military attaches.

The same device was also provided by the War Department in large quantities for use by the Department of State, for Secret and Confidential Communications between that Department and its Embassies, Legations, and Consulates, as well as for intercommunication among those offices.

~~SECRET~~

~~SECRET~~

Certain Allied Services, such as the British, Italian, and Russian were also provided with these devices in small quantities both by the War and the Navy Departments. The U.S. Navy also adopted the device at first in practically identical form; the Navy produced some minor improvements later on and employed and is still employing the device very extensively in its own communications. In addition the Strip Cipher System was used during the war as a Joint Army-Navy system and as a Combined System. The fact that the same device was used by both the Army and the Navy greatly facilitated Joint Communications. The production of the paper strips bearing the variable cipher alphabets employed in the device presented numerous problems which were successfully solved by me or by people under my direction. I conceived the first rotary cutter for cutting the strips apart and had the first cutter built at the Government Printing Office. This machine greatly facilitated the production of the strips and made the matter practical.

5. General.--Throughout the years mentioned, in my capacity as Head Cryptanalyst and later as the Director of Communications Research, many problems directly related to our communications security were brought to my attention and I believe that my long experience in the field formed a solid foundation for mature, sound judgment in arriving at proper, practical, and satisfactory answers to those problems.

Before our Converter M-228 was ready for distribution the urgent need for a means of enciphering teletype communications for the Military Intelligence network in the United States led to my suggesting the adoption of a temporary expedient for this purpose. This took the form of double-loop, key-tape encipherment system which had been tried out in a small way at the end of World War I. Having studied this method in 1919-1921 and knowing the pitfalls to which such a system is subject from the security point of view, I was able to suggest ways of usage to minimize the dangers inherent in a double-tape encipherment method. The system was used for a number of months not only within the U. S. but also within theaters of operations, thus meeting an urgent need for teletype encipherment until the M-228 was ready for distribution.

Later on, when the one-time tape or Sigtot System was being considered for secret and top secret radio-teletype communications, I was consulted and in view of my experience with all preceding teletype encipherment systems was able to give technical approval on the new proposal and to insure that the production of keying tapes was properly safeguarded.

~~SECRET~~

~~SECRET~~EO 3.3(h)(2)  
PL 86-36/50 USC 3605

For a number of years prior to 1941 I had been more or less intensively studying all the various cryptographic devices and machines which had been invented and produced by private inventors both in the United States and in foreign countries. Files of patents issued domestically and abroad were kept, and theoretical studies made to ascertain the security of the products of invention in this field.

[REDACTED]

This resulted in improvements in the security of the machine and led finally to the adoption of Converter M-209 as a field instrument. Over 100,000 of them were manufactured, and used by both the Army and the Navy. While the machine was by no means perfect, it met a need that could hardly have been fulfilled otherwise.

For a number of years I served on the Joint and the Combined Codes and Ciphers Committee and the Joint and Combined Security Committee. I was a member of a special Ad Hoc Committee, consisting of two Navy officers, General (then Colonel) Corderman, and myself, appointed by the Joint Communications Board in 1944 to investigate the security of communications in all non-military bureaus and departments of the Government, making recommendations for improvement therein. The deliberations of the Ad Hoc Committee resulted in the establishment, by President Truman, of the Cryptographic Security Board for U. S. Government communications, consisting of the Secretaries of the three Departments, State, War, and Navy.

As technical adviser to the Chief, Signal Security Agency and to the Chief of the Security Division, I was constantly consulted by them in connection with the many problems affecting communications security. I also served in an advisory capacity in connection with all research and development of communications security equipment, including ciphony and cifax. One of my important contributions in this capacity was to urge the development of the voice security equipment, now known as the Sigsaly system, at a time when that project had been practically abandoned.

The new Synchronous Polarity Reversal System of Cifax recently developed by us is based upon an invention of mine (Serial No. 478,193) filed on 3 June 1943 and assigned to the Secretary of War on 18 October 1943. Lieutenant Colonel Rosen's invention of the important feature whereby the polarity reversals in the interaction of keying and picture elements are synchronized made the system practical and highly secure; in fact, there is reason to believe that the security of cifax transmissions by the Friedman-Rosen inventions can be made almost absolute.

~~SECRET~~



~~SECRET~~

In 1941 I undertook a study of the general basis of the distribution of Army cryptographic systems, evolving the new idea of "cryptonets", and thus improving security of communications. By isolating cryptographic systems according to levels of command and reducing the amount of intra-net traffic within any one system, the security of all systems is enhanced at the same time that provision is made for inter-net traffic. The cryptonet system has worked in a highly satisfactory manner in practice.

B. Important Contributions to Communications Intelligence, 1939-1945

1. Solution of Japanese Diplomatic Communications.--On 20 February 1939 the Japanese Foreign Office began using a new machine called by them the "B-Machine" for the highly secret communications between Tokyo and its embassies throughout the world. We had been successfully solving and reading practically all of the communications of the Japanese Foreign Office up to that time; many of them were in a machine ("A Machine") which we had also solved and reconstructed by pure analysis in about the year 1937, but a large number were also in hand operated systems involving a small code, superenciphered by various schemes, usually transposition.

The urgency of solution of the new machine, in view of the increasingly difficult relations between the United States and Japan, was apparent. However, in view of the small number of trained cryptanalysts available, the pressure of work in the sections operating on currently readable systems and in the sections producing our own codes, ciphers, and key lists, the number of people who could be placed on this new and very difficult problem was very limited. By August 1939, no important progress having been made, the Chief Signal Officer directed that I drop, so far as practicable, certain administrative duties as assistant chief of Signal Intelligence Service (Major W. O. Reeder had been brought in as officer in charge in April 1938) and to participate actively in the studies of the "B Machine," in addition to generally supervising the technical cryptanalytic and cryptographic work of the office. Thus, from that month until success was attained, the "B-Machine" studies were under my active supervision but at the same time I had to carry on some other duties from which, it was impracticable to relieve me.

By the end of 1939, the machine having been in use almost a full year, hundreds of messages had accumulated; very occasionally a tiny fragment of a message was read; rarely, longer fragments. But no message was read in its entirety. Nevertheless important progress had been made. Intensive work was continued by me and my technical staff

~~SECRET~~

~~SECRET~~

of half a dozen cryptanalysts, with the clerical assistance of another half dozen people, and the occasional assistance of our two Japanese translators. On 20 September 1940 came the very first indication that we were on the right path and might be successful in solving the machine; under the pressure of great excitement, working almost day and night, by 27 September the first two translations representing the very first actual solution to the B-Machine were sent to G-2.

There remained, however, much work to be done, since only the data applicable to but one out of the whole set of 120 indicators were at hand. By 14 October 1940 solutions for over one-third of the 120 indicators were available and certain current messages could be read.

By careful analytical reasoning, by studying the external cryptographic phenomena manifested by the system, by correct reasoning and a knowledge of cryptographic mechanisms, the principles underlying the cryptographic functioning of the B-Machine were soon derived by induction and deduction. A hand-operated, crude model using flash-light bulbs was hurriedly constructed, while at the same time parts were ordered for two fully automatic, keyboard-operated machines, which were then constructed as rapidly as possible. All of this work also was under my general direction as Principal Cryptanalyst. By November 1940 the two fully automatic machines had been constructed and were in successful operation. We had, it is true, reconstructed the Japanese "A-machine" by pure analysis, too, but so far as I am aware, this is the first time in cryptanalytic history that a machine capable of deciphering traffic of the complexity of that produced by the Japanese B-Machine was completely reconstructed by pure analysis. When we began the study we had no inkling as to the nature of the machine; soon thereafter we had ascertained that the cryptographic textual letters fell into two classes, but to this day we have never seen a complete Japanese machine in working order. Some time in 1942, long after our work of analysis had been completed, we did see the smashed, burned and almost unrecognizable remains of a B-Machine which the Japanese had destroyed on or about 5 December 1941 in Mexico and which remains came into possession of the F. B. I., who were anxious to reconstruct the machine if possible; also, and as a result of European Ticom operations, we did find two or three of the rotary-switch assemblies in a box taken from the ruins of the Japanese Embassy in Berlin, but of course these glimpses of one of the most important elements of the machine were by this time only of academic interest.

In January 1941 a Joint Army-Navy Cryptanalytic Mission to GC and CS took with it one machine and a complete story of how to decipher diplomatic messages enciphered by the Japanese B-Machine. This system was one of the very few which had resisted all of GC and CS efforts to solve it.

~~SECRET~~

~~SECRET~~

As to the importance of the solution of the B-Machine, or Purple System, as it was designated soon after solution, I need only refer to the disclosures of the current Joint Congressional Investigation of the attack on Pearl Harbor and to certain statements relative to the solution of the Japanese diplomatic machine contained in the letter dated 27 September 1944, which the Chief of Staff sent to Mr. Dewey, a copy of which is attached hereto. While that solution represents the achievement of a cooperative effort by a number of people, it was made possible by good coordination and proper technical direction of a fair number of skilled cryptanalytic personnel who were selected and trained by me and who worked under my direction for over 18 months as a harmonious team. In addition, certain of the cryptographic phenomena which ultimately led to the solution were uncovered by me in the course of those studies. A more detailed history of the solution is attached hereto.

We know that the German cryptanalytic staffs tried to solve the B-Machine and failed; as noted above, even as competent as was the British staff, it also failed to solve this machine and we gave them the solution. There is reason to believe that the Russian staff did not succeed, if they even undertook the problem, which we do not know. I believe it is true that as a result of our reading certain messages early in 1941 the State Department was able to give the Russian Government early information as to the coming secret offensive by the Germans, which began on 21 June 1941. Had the Russians been able to read the Purple, this would not have been necessary. As to the Japanese diplomatic communications in other systems, their messages in those systems were being read as promptly as facilities and personnel permitted, with priority being given those in the Purple System, although many important messages were also read in the various other systems, such as PA-K2, CA, and LA.

2. General.--As Head Cryptanalyst in the years 1939-1941, I was in technical charge of a staff of people numbering several thousand, working on all problems in the communications intelligence field, and also supervised the selection and training of new personnel. Some of the problems being worked on during those years and successful in their outcome were those involving the diplomatic communications of several other governments than the Japanese such as the Italian, German, and Mexican. During the succeeding years, 1941-1945, the Agency accomplished many feats in cryptanalysis, too numerous to mention.

The diplomatic communications of many countries were read, some almost in toto; the communications of the Japanese Army and Air Force were read to a very large degree, contributing greatly to our victory in the Pacific.

~~SECRET~~

~~SECRET~~

The extent to which the Agency engaged in the research, development, and use of high speed analytic equipments to facilitate the application of cryptanalytic techniques and processing is worthy of mention and my technical advice and collaboration was used in all these cases. I was largely responsible for urging the development of the "oc3" equipment and had general supervision over its design, construction, and installation by the Bell Telephone Laboratories and the Western Electric Company. The fruits of that equipment and the modifications which followed and which were applied to the solution of German Enigma traffic represent some of the best achievements of the Agency. Our important developments in the field of photo-electric rapid analytical machinery also resulted from my insistence upon embarking upon such developments. In all these matters my advice was sought and obtained by the Chief of the Agency and special reports were prepared for him from time to time on these subjects. These equipments aided considerably in the solution of the diplomatic and military communications which were worked on by the Agency.

~~SECRET~~

# Introduction to Cryptology - IV

BY WILLIAM F. FRIEDMAN

Confidential

## Cryptology in the Civil War.

A detailed account of the...

Original  
National War College

1/27/76

1/27/76

National War College

National War College  
1/27/76

W

~~Introduction to Cryptology - IV~~  
~~Lecture No. 4~~  
**CRYPTOLOGY IN THE CIVIL WAR**  
~~Codes and Ciphers of the Civil War~~

BY WILLIAM F. FRIEDMAN

~~This lecture, the fourth in the series, deals with the crypto-  
systems used by both sides in the Civil War, the War of the Rebellion,  
the War Between the States - choose your own designation for that  
vicious, bloody, and very costly strife, when brother was pitted against  
brother. Civil strife is unhappily always very bitter and leaves scars  
which heal only extremely slowly with the passage of many years.~~

A detailed account of the codes and ciphers of the Civil War in the United States of America can hardly be told without beginning ~~it~~ with a bit of biography about the man who became the first signal officer in history and the first Chief Signal Officer of the United States Army, Albert J. Myer, the man in whose memory that lovely little U.S. Army post adjacent to Arlington Cemetery was named. Myer was born on 20 September 1827, <sup>and</sup> After an apprenticeship in the then quite new science of electric telegraphy ~~A Morse's patent is dated 1837~~ he entered Hobart College, Geneva, New York, from which he was graduated in 1847. From early youth he had exhibited a predilection for artistic and scientific studies, and upon leaving Hobart he entered Buffalo Medical College, receiving the M.D. degree four years later. His graduation thesis, "A Sign Language for Deaf Mutes," contained the germ of the idea he was to develop several years later, when, in 1854, he was commissioned a 1st Lieutenant in the Regular Army, made an Assistant Surgeon, and ordered to New Mexico for duty. ~~Myer's idea involved the development of an efficient system of military "aerial telegraphy", which was what~~ ~~systems~~ ~~visual signaling~~ <sup>was</sup> ~~were~~ then called. He had plenty of time at this <sup>developing an</sup> ~~the matter~~ far-away outpost to think about <sup>the matter</sup>. I emphasize the word "system" because, strange to say, although instances of the use of lights and other visual signals can be found throughout the history of warfare, and their <sup>use</sup> ~~use~~ between ships at sea had been practiced by mariners for centuries, yet down to the middle of the 19th Century surprisingly little progress had been made in developing methods and instruments for the systematic exchange of military information and instructions ~~in the~~ <sup>system of electric</sup> ~~by~~ by means of signals of any kind. Morse's practical telegraphy,

12/10/54  
Friedman

12/10/54  
Friedman

photo  
a myer  
about  
here

developed in the years 1832-35, served to focus attention within the military <sup>systems and methods</sup> upon ~~the matter~~ of inter-communication by means of both visual and electrical signals, ~~and~~ In the years immediately preceding the Civil War, the U.S. Army took steps to introduce and to develop ~~a~~ system of visual signaling for general use in the field. It was Assistant Surgeon Myer who furnished the initiative in this matter.

In 1856, ~~two years after he was commissioned assistant surgeon,~~ and had devoted much of his leisure time to the study of visual signaling and its developments, Myer drafted a memorandum on a new system of visual signaling

and obtained a patent on it. Two years later, a board <sup>was</sup> appointed by the War Department to study Myer's system, ~~reported favorably.~~ After some <sup>successful</sup> demonstrations by Myer <sup>and his assistants,</sup> ~~and as a result,~~ the War Department fostered a bill in Congress, which gave its approval to <sup>his ideas.</sup> ~~the system.~~ But what is more to the point, Congress appropriated an initial amount of \$2,000 to enable the Army and the War Department to

develop the system. The money, as stated in the Act was to be used "for the manufacture of purchase of apparatus and equipment for field signaling." The act also contained another important provision: it authorized the appointment, on the Army staff, of one Signal Officer with the rank, pay, and allowances of a major of cavalry. On 2 July 1860, "Assistant Surgeon Albert J. Myer (was appointed) to be Signal Officer, with the rank of Major, 27 June 1860, to fill an original vacancy" <sup>and</sup> ~~Two weeks~~ later Major Myer was ordered to report to the Commanding General of the Department of New Mexico for signaling duty. The War Department also directed that two officers be detailed as his assistants. During a several months' campaign against hostile Navajos, an extensive test of Myer's new system, using both flags and torches, was conducted / with much success. In October 1860, a Lieut. J.E.B. Stuart, later to become famous as a Confederate cavalry leader, tendered his services to aid in signal instruction; ~~Stuart~~

*It is interesting to note*  
~~interest you to learn~~ that one of the officers who served as an assistant to Myer in demonstrating his system before the board, ~~which made a study of Myer's system before it was adopted by the Army~~ was a Lieut. E.P. Alexander, Corps of Engineers. We shall hear more about him presently, but at the moment I will say that on the outbreak of ~~the~~ War, Alexander organized the Confederate Signal Corps. ~~Corps, which was established by the Act of the Confederate Congress "to organize a Signal Corps". The Act was approved on 19 April 1862 - nearly a year earlier than the Signal Corps of the Federal Army was likewise established as a separate Corps.~~

Less than a year after Major Myer was appointed as the first and, at that time, the only Signal Officer of the U.S. Army, *Fort Sumpter was attacked and, after a 36-hour bombardment, surrendered.* The bloody four-year war between the North and the South *began* ~~commenced~~. The date was 14 April 1861. Myer's system of aerial telegraphy was soon to undergo its real baptism under fire, rather than by fire. But with the outbreak of war, another new system of military signal communication, signaling by the electric telegraph, began to undergo its first thorough test in combat operations. This in itself is very important in the history of cryptology. But far more significant in that history is ~~the~~ *fact I mentioned at the close of the last lecture, viz, that* that, for the first time in the conduct of organized warfare, rapid and secret military communications on a large scale became practicable, because cryptology and electric telegraphy were now to be joined in a ~~constant~~ *lasting* wedlock. For when the war began, the electric telegraph had been in use for less than a quarter of a century. Although the first use of electric telegraphy in military operations was in the Crimean War in Europe (1854-56), its employment was restricted to communications exchanged among headquarters of the Allies, and some observers were very doubtful about its utility even for this limited usage. It may also be noted that in the annals of that war there is no record of the employment of electric telegraphy together with means for protecting the messages against their interception and solution by the enemy.

On the Union side in the Civil War, military signal operations began with Major Myer's arrival in Washington on 3 June 1861. His basic equipment consisted of kits containing a white flag with a red square in the center for use against a dark background; a red flag with a white square for use against a light background; and torches for night use. It is interesting to note that these are the elements which make up the familiar insignia of our Army Signal Corps. The most pressing need which faced Major Myer was to get officers and men detailed to him wherever signals might be required, and to train them in what *had come to* be called the "wigwag system"; *the motions of which are depicted in Fig. 1.* This training included learning something about codes and ciphers, and gaining experience in their usages.

But there was still no such separate entity as a Signal Corps of the Army. Officers and enlisted men were merely detailed for service with Major Myer for signaling duty. It was not until two years after the war started that the Signal Corps was officially established and organized as a separate branch of the Army, by appropriate Congressional action. ¶ In the meantime, another signaling organization was coming into being - an organization which was an outgrowth of the

*1/ And, of course, the S.I.'s of those days had a pet name for the users of the system. They called them "flag floppers."*



government's taking over control of the commercial telegraph companies in the United States on 25 February 1862. There were then only three in number: the American, <sup>the</sup> Western Union, and <sup>the</sup> Southwestern. The telegraph lines generally followed the <sup>right-of-way of the</sup> ~~routes of the~~ railroads. The then Secretary of War, Simon Cameron, sought the aid of Thomas A. Scott, of the Pennsylvania Railroad, who brought some of his men to Washington for railroad and telegraphic duties with the Federal Government. From a nucleus of four young telegraph operators grew a rather large military telegraph organization which was not given formal status until on 28 October 1861 President Lincoln gave Secretary Cameron authority to set up <sup>a</sup> "the U.S. Military Telegraph Department" under a man named Anson Stager, who, as general superintendent of the Western Union was called to Washington, commissioned a captain (~~later~~ later a colonel) in the Quartermaster Corps, and made superintendent of the Military Telegraph Department. ~~Only~~ Only about a dozen of the members of the Department became commissioned officers, and they were made officers so that they could receive and disburse funds and property. ~~All~~ All the rest were civilians. ~~The~~ The U.S. Military Telegraph "Corps", as it soon came to be designated, without warrant, was technically under Quartermaster <sup>General</sup> Meigs, but for all practical purposes it was under the immediate and direct control of the Secretary of War, a situation admittedly acceptable to Meigs. There were now two organizations for signaling in the Army, and it was hardly to be expected that no difficulties would ensue from the duality. In fact, the difficulties began ~~to break out~~ very soon, as can be noted in the following extract from a lecture before the Washington Civil War Round Table, early in 1954, by Dr. George R. Thompson, Chief of the Historical Division of the Office of the Chief Signal Officer of the U.S. Army:

The first need for military signals arose at the important Federal fortress in the lower Chesapeake Bay at Fort Monroe. Early in June, Myer arrived there, obtained a detail of officers and men and began schooling them. Soon his pupils were wigwagging messages from a small boat, directing the fire of Union batteries located on an islet in Hampton Roads against Confederate fortifications near Norfolk. Very soon, too, Myer began encountering trouble with commercial wire telegraphers in the area. General Ben Butler, commanding the Federal Department in southeast Virginia, ordered that wire telegraph facilities and their civilian workers be placed under the signal officer. The civilians, proud and jealous of their skills in electrical magic, objected in no uncertain terms and shortly an order arrived from the Secretary of War himself who countermanded Butler's instructions. The Army's signal officer was to keep hands off the civilian telegraph even when it served the Army.

Note that at the time of this episode the Signal Officer had ~~no facilities for electric telegraph signaling~~ - he was given control of such facilities in southeast Virginia by the commanding general of the Department, General Butler, and he kept <sup>it</sup> them for only a few hours.

I have purposely selected this extract from Dr. Thompson's presentation because in it we can clearly hear the first rumblings <sup>of</sup> that lengthy and acrimonious feud between two signaling organizations whose uncoordinated operations and rivalry greatly reduced the efficiency of all signaling operations of the Federal Army. As already indicated, one of these organizations was the U.S. Military Telegraph "Corps", ~~sometimes~~ hereinafter abbreviated as <sup>the</sup> USMTC, a civilian organization which operated the existing commercial telegraph systems for the War Department, under the direct supervision of the Secretary of War, Edwin M. Stanton. The other organization was, of course, the infant Signal Corps of the United States Army, which was not yet even established as a separate branch, whereas the USMTC had been established in October 1861, as noted above. Indeed, the Signal Corps had to wait until March 1863, ~~two years after~~ two years after the outbreak of war, before being established officially. <sup>In this connection it should be noted</sup> ~~You will recall that~~ the Confederate Signal Corps had been established a full year earlier, in April 1862: ~~Until then, as I've said before, for signaling duty on both sides, there were only officers who were individually and specifically detailed for such duty from other branches of the respective Armies of the North and the South.~~ Trouble between the USMTC and the Signal Corps of the Union Army began when the Signal Corps became interested in signaling by electric telegraphy and began to acquire facilities therefor.

As early as in June 1861, Chief Signal Officer Myer had initiated action toward acquiring or obtaining electrical telegraph facilities for use in the field but with one exception nothing happened. The exception was in the case of <sup>episode in the</sup> the military department in southeast Virginia, commanded by General Benjamin Butler, <sup>an episode that clearly foreshadowed the future road for the Signal Corps in regard</sup> ~~who was mentioned a few moments ago in the extract I read you from~~ to electrical signaling: <sup>the road was to be closed and barred.</sup> ~~Dr. Thompson's address.~~ In August 1861, Col. Myer tried again and in November of the same year he recommended in his annual report that \$30,000 be appropriated to establish an electrical signaling branch in the Signal Corps. The proposal failed to meet the approval of the Secretary of War. ~~However,~~ <sup>however,</sup> One telegraph train, <sup>The train</sup> which had been ordered by Myer, many months before; was delivered in January 1862, ~~and~~ was tried out in an experimental fashion, <sup>and</sup> under considerable difficulties, the most disheartening of which was the active opposition of persons in Washington, particularly the Secretary of War. So, for practically the whole of the first two years of the war, signal officers ~~on~~ the Northern side had neither electrical telegraph facilities nor Morse operators - they had to rely entirely on the wig-wag system.

However, by the middle of 1863 there were thirty "flying-telegraph" trains in use in the Federal Army. Here's a picture of such a train. The normal length of field telegraph lines was five to eight miles, though in some cases the instruments had worked at distances as great as twenty miles. But even before the Signal Corps began to acquire these facilities, there had been agitation to have them, as well as their Signal Corps operating personnel, all turned over to the USMTC, which had grown into a tightly-knit organization of over 1,000 men in Washington, and had become very influential, especially by virtue of its support from Secretary of War Stanton. As a consequence, the <sup>USMTC</sup> ~~Telegraph Corps~~ had its way. In the fall of 1863, it took over all the electric telegraph facilities and telegraph operators of the Signal Corps. Colonel Myer sadly wrote: "With the loss of its electric lines the Signal Corps was crippled".

Fig 3  
4.3

So now there were two competing signal organizations on the Northern side: The U.S. Army's Signal Corps, which was composed entirely of military personnel with no electric telegraph facilities (but was equipped with means for visual signaling), and the USMTC, which was not a part of the Army, being staffed almost entirely with civilians, and which had electric telegraph facilities and skilled Morse operators (but no means or responsibilities for visual signaling or "aerial telegraphy" which, of course, was old stuff). "Electric telegraphy" was now the thing. The USMTC had no desire to share electric telegraphy with the Signal Corps, a determination in which the ~~Corps~~ <sup>they were</sup> most ably assisted by Secretary of War Stanton, for reasons that fall outside the scope of the present lecture.

However, from a technical point of view it is worth going into this rivalry just a bit, if only to note that the personnel of both organizations, the military and the civilian, were not merely signalmen and telegraph operators: they served also as cryptographers and were therefore entrusted with the necessary ~~alphabets~~, cipher books and <sup>keys</sup>. Because of this, they naturally became privy to the important secrets conveyed in cryptographic communications and they therefore enjoyed status as VIP's. This was particularly true of members of the USMTC, because they, and only they, were authorized to be custodians and users of the cipher <sup>books</sup>. Not even the commanders of the units they served had access to <sup>them,</sup> ~~the ciphers~~. For instance, on the one and only occasion when General Grant forced his cipher operator, a civilian named Beckwith, to turn over the current cipher <sup>book</sup> to a colonel on Grant's staff, Beckwith was immediately discharged by the Secretary of War and Grant was reprimanded. A few days later, Grant apologized and Beckwith was restored to his position. But Grant never again demanded the cipher <sup>book</sup> held by his telegraph operator.

The Grant-Beckwith affair alone is sufficient to indicate the lengths to which Secretary of War Stanton went to retain control over the USMIC, including its cipher operators, and its cipher <sup>books</sup>. In fact, so strong a position did he take that on 10 November 1863, following a disagreement over who should operate and control all the military telegraph lines, Myer, by then full Colonel, and bearing the <sup>imposing</sup> ~~resounding~~ title "Chief Signal Officer of the United States Army", a title he had enjoyed for only two months, was preemptorily relieved from that position and put on the shelf. Not long afterward, and for a similar reason, Myer's successor, Lieut. Col. Nicodemus, was likewise summarily relieved as Chief Signal Officer by Secretary Stanton; indeed, he was not only removed from that position—he was dismissed from the Service without even the formality of trial by court martial. Stanton gave "phony" reasons for dismissing Col Nicodemus, but I am glad to say that the latter was restored his commission in March 1865, by direction of the President; *also by direction of the President, Colonel Myer was restored to his position as Chief Signal Officer of the U.S. Army on 25 February 1867.*

~~As for what happened to Colonel Myer, the record shows that he vacated his commission in July 1864; Colonel Nicodemus lasted about six months after he superseded Myer; and Colonel Benjamin F. Fisher became Chief Signal Officer on 26 December 1864, but his appointment was never confirmed by the Senate. (Photo-  
 1864-1865-214, 222) In August 1865 Colonel Myer requested that he be restored to the position of Chief Signal Officer of the Army. Accompanying his application were letters of recommendation from several high-ranking officers of the Army and the Navy, and Myer's application was forwarded to Lieutenant General Grant, who returned the application to the President, saying, "Unless there are reasons of which I know nothing, I deem A. J. Myer entitled to the position of Chief Signal Officer of the Army and recommend it accordingly." In a letter dated 30 July 1866 to Secretary of War Stanton, General Grant recommended "the appointment of Albert J. Myer to the place of Chief of the Signal Corps as provided for by Act of Congress. Colonel Myer is the inventor of the system used both in the Army and Navy, which would seem to give him a claim to the position of Chief, which he once held and which the Senate have refused to confirm any other person in." Apparently this last letter produced results, for Colonel Myer was reappointed Chief Signal Officer on 25 February 1867, to date from 25 February 1867.~~

~~Let's go back a bit in this part of the story.~~ When Col. Myer was relieved from duty as Chief Signal Officer in November 1863, he was ordered to

Cairo, Illinois, to await orders for a new assignment. Very soon thereafter he was either designated (or he may have himself decided) to prepare a field manual on signaling and there soon appeared, with a prefatory note dated January 1864, a pamphlet of 148 pages, a copy of which is now in the Rare Book Room of the Library of Congress. The title page reads as follows:

"A Manual of Signals: for the use of signal officers in the field.  
By Col. Albert J. Myer, Signal Officer of the Army, Washington,  
D.C., 1864."

Even in this first edition, printed on an Army press, Myer devoted nine pages to a reprint of an article from Harper's Weekly entitled "Curiosities of Cipher", and in the second edition, 1866, he expanded the section on cryptography to sixty pages. More editions followed and I think we may well say that Myer's Manual, in its several editions, was the pioneer American text on military signaling. But I'm sorry to say that as regards cryptology it was rather a poor thing. Poe had done ~~much~~ better twenty years before that in his essay entitled "A few words on secret writing".

Because of its historic nature, you may like to see what Myer's original ~~two-element signaling~~ or "wig-wag code" was like. It was called "a two-element code" because it employed only two digits, 1 and 2, in permutations of 1, 2, 3 and 4 groups. For example, A was represented by the permutation 22; B, by 2122; C, by 121, etc. In flag signaling, a "1" was indicated by a motion to the left, a "2" by a motion to the right. Later these motions were reversed, for reasons which must have been good but are now not obvious. Here is Myer's two-element code which ~~continued to be used until 1912:~~ <sup>continued to be</sup>

## GENERAL SERVICE CODE

A - 22	N - 11	& - 1111
B - 2122	O - 21	ing - 2212
C - 121	P - 1212	tion - 1112
D - 222	Q - 1211	
E - 12	R - 211	End of word - 3
F - 2221	S - 212	End of sentence - 33
G - 2211	T - 2	End of message - 333
H - 122	U - 112	Affirmative - 22.22.22.3
I - 1	V - 1222	Repeat - 121.121.121
J - 1122	W - 1121	Error - 212121
K - 2121	X - 2122	
L - 221	Z - 2222	

Note: No. 3 (end of word) was made by a forward downward motion, called "front". There were about a dozen more signals, for numerals, for frequently used short sentences, etc.

We must turn our attention now to the situation as regards the organization for signaling in the Confederate ~~States~~ Army. ~~As indicated a few minutes ago, the first great engagement of the War, that of the first Bull Run battle, the Confederate States Signal Corps was formally established nearly a year earlier than~~ <sup>It is of considerable interest to note that in the</sup>

Confederate signal officer was

~~its Federal counterpart. Perhaps this arose as a result of the far greater success that the Confederate Signal <sup>Corps had than did the Union equivalent</sup> officers enjoyed during the first great battle of the Civil War, that at Bull Run, ~~that the Union signal officers had the Confederate signal effect in that battle~~ was that young lieutenant, E. P. Alexander, who had assisted Major Myer in demonstrating the wig-wag system before a board appointed by the War Department to study Myer's system. Alexander, <sup>now</sup> a Captain in grey, used Myer's system during the battle, which ended in disaster for the Union forces; *and it is said that* Alexander's contribution <sup>by effective</sup> in signaling was an important factor in the Confederate victory. Dr. Thompson, whom I have quoted before, says of this battle:~~

Thus the fortunes of war in this battle saw Myer's system of signals succeed, ironically, on the side hostile to Myer. Because of general unpreparedness and also some disinterest and ignorance, the North had neither wig-wag signals nor balloon observation.

~~During the first battle of Bull Run~~ The only communication system which succeeded in <sup>signal work for</sup> ~~servicing~~ the Union Army was the infant USMTC. But the Confederate system under Alexander, off to a good start at Bull Run, throughout the war and operated with both visual/electric telegraphy, and the Confederates thought highly enough of their signal service to establish it on an official basis <sup>on 19 April 1862,</sup> less than a year after that battle. ~~The Signal Corps of the Confederate Army was established, by an Act of the Confederate States Congress on 19 April 1862, as a separate corps, to be attached either to the Adjutant and Inspector General's Department or to the Engineer Department. The Confederate States Secretary of War on 29 May 1862 attached the Signal Corps to the former organization.~~ Thus, although the Confederate Signal Corps never became <sup>a</sup> distinct and independent branch of the Army as did the Union Signal Corps, it received much earlier recognition from the Confederate ~~Government~~ Government than did the Signal Corps of the Federal Government. Again quoting Dr. Thompson:

The Confederate Signal Corps was thus established nearly a year earlier <sup>than</sup> its Federal counterpart. It was nearly as large, numbering some 1,500, most of the number, however, serving on detail. The Confederate Signal Corps used Myer's system of flags and torches. The men were trained in wire telegraph, too, and impressed wire facilities as needed. But there was nothing in Richmond or in the field comparable to the extensive and tightly controlled civilian military telegraph organization which Secretary Stanton ruled with an iron hand from Washington.

We come now to ~~an examination of~~ the codes and ciphers used by both sides in the war, and in doing so we must take into consideration the fact that on the Union side, there were, as I have indicated, two separate organizations for signal communications; <sup>one for visual signaling, the other for electric.</sup> ~~the Signal Corps and the USMTC. After warfare between them had been settled by ruthless action by Secretary of War Stanton, the Signal Corps <sup>was left with</sup> responsibility only for signaling by visual or aerial telegraphy, the USMTC <sup>was given sole</sup> responsibility for signaling by electric telegraphy.~~ We should therefore not be

too astonished to find that the cryptosystems used by the two competing organizations were different. On the other hand, on the Confederate side, as just noted, ~~in fact~~ there was only one organization for signal communications, the Signal Corps of the Confederate States Army, which used both visual and electric telegraphy, the latter facilities being taken over and employed when <sup>and where they were</sup> available. ~~perhaps~~

~~later on there will be opportunity to tell you what I think were the basic reasons.~~  
 There were reasons for this marked difference between the way in which the Union and the Confederate signal operations were <sup>organized and administered but I do not wish to go into them now. One reason,</sup> conducted, which strange to say, had to do with the difference between the crypto-communication arrangements in the Union and in the Confederate Armies.

We will discuss the cryptosystems used by the Federal Signal Corps first and then <sup>those</sup> ~~that of~~ the Confederate Signal Corps. Since both corps used visual signals as their primary means, we find them employing Myer's visual-signaling code ~~such as~~ ~~was~~ shown above. At first both sides sent unenciphered messages; but soon after learning that their signals were being intercepted and <sup>were being</sup> read by the ~~other side~~ <sup>enemies</sup>, each side decided to do something to protect its messages. ~~At~~ Initially both decided on the same artifice, viz, changing the visual-signaling equivalents for the letters of the alphabet, so that, for instance, "22" was not always "A", etc. This sort of changing-about of values soon became impractical, since it prevented memorizing the wig-wag <sup>equivalents</sup> ~~actions for letters~~ once and for all. The difficulty in the Union Army's Signal Corps was solved by the introduction into usage of a cipher disk invented by Myer himself. A full description of the disk in its various embodiments will be found in Myer's Manual, but here's a picture of three forms of it. You can see how ~~you know~~

Fig. 3 - (4-4)

(Leave Half-page)

readily the visual wig-wag equivalents for letters, <sup>figures, etc.,</sup> ~~of the alphabet~~ can be changed according to some pre-arranged indicator for <sup>juxtaposing</sup> ~~setting the~~ concentric <sup>disks in my</sup> ~~setting~~. Fig. 3. ~~The two left disks of Fig. 1 of Myer's Plate XXVI) show that~~ ~~disks into juxtaposition.~~ ~~(In Fig. 1 of the picture the letter A is represented~~ by 112, B, by 22, etc. By moving the two circles to a different juxtaposition a <sup>established.</sup> new set of equivalents will be ~~set up~~. Of course, if the setting is kept fixed for a whole message the encipherment is strictly monoalphabetic; but Myer recommends changing the setting in the middle of the message or, more specifically, at the end of each word, thus producing a sort of polyalphabetic cipher which would delay solution a bit. An alternative way, Myer states, would be to use what he called a "countersign word", but which we call a keyword, each letter of which

would determine the setting of the disk for a single word or for two consecutive words, etc. Myer apparently did not realize that retaining or showing externally, <sup>that is, in the cipher text,</sup> the lengths of the words of the plain text <sup>very seriously impairs the security of the cipher message.</sup> ~~is a very serious weakness.~~ A bit later we shall discuss the security afforded by the Myer disk in actual practice.

In the Confederate Signal Corps, the system used for encipherment of visual signals was apparently the same as that used for encipherment <sup>ing</sup> of telegraphic messages, signals, and we shall soon see what it was. Although Myer's cipher disk was captured a number of times, it was apparently disdained by the Confederates, who preferred to use a wholly different type of device, as will be described presently, for both visual and electric telegraphy.

So much for the cryptosystems used in connection with visual signals by the Signal Corps of both the North and the South, systems which we may designate as "tactical ciphers." We come now to the systems used ~~by the two Military Telegraph Corps (one in the North, one in the South), which had responsibility~~ for what we may call "strategic ciphers", because the latter were usually exchanged between the seat of Government <sup>and field commanders,</sup> ~~in the field,~~ or among <sup>the latter.</sup> ~~high commanders in the field.~~ In the case of these communications the cryptosystems employed by each side were quite different.

On the Northern side <sup>USMTC</sup> the ~~Military Telegraph Corps~~ used a system based upon what we now call transposition but in contemporary accounts they were called "route ciphers" and that name <sup>has</sup> stuck. The designation isn't too bad, ~~it is~~ because the processes of encipherment and decipherment, though <sup>dealing</sup> ~~they deal~~ not with the individual letters of the message but with entire words, involve following prescribed paths or routes <sup>in a diagram in which the message is written.</sup> I know no simpler or more succinct description of the route cipher than that given by one of the USMTC operators, J. E. O'Brien, in an article in Century Magazine, XXXVIII, September 1889, entitled "Telegraphing in Battle":

The principle of the cipher consisted in writing a message with an equal number of words in each line, then copying the words up and down the columns by various routes, throwing in an extra word at the end of each column, and substituting other words for important names and verbs.

A more detailed description in <sup>in</sup> modern technical terms would be as follows:

A system in which <sup>in</sup> encipherment the words of the plain-text message are inscribed within a ~~specified design, rectangle, or matrix, according to a prearranged~~ <sup>matrix of a specified</sup> number of rows and columns, inscribing the words within the matrix from left to right, in successive lines and rows downward / as in ordinary writing, and taking the words out of the matrix, that is, transcribing them, according to a prearranged route, to form the cipher message. These route ciphers were supposed to have been the



The specific routes to be followed were set forth in numbered booklets, <sup>each being labelled</sup> ~~designated~~ as "War Department Cipher" followed by an number. In referring to them hereinafter I shall use the term "cipher books", or sometimes, more simply, the term "ciphers", although the cryptosystem involves both cipher and code processes. It is true that the basic principle of the system, that of transposition, makes ~~the system technically~~ <sup>it partake of the nature</sup> of a cipher system as defined in our modern terminology; but the use of "arbitraries", <sup>as they were called, that is, words arbitrarily assigned</sup> ~~of arbitrary words~~ to represent the names of persons, geographical points, important nouns and verbs, etc., makes the system <sup>technically</sup> ~~partake~~ of the nature of a code system as defined in our modern terminology.

There were in all about a dozen cipher books used by the USMTC throughout the war. For the most part they were employed consecutively, but <sup>it seems that</sup> ~~sometimes~~ two different ones were employed concurrently. They contained not only the specific routes to be used but also indicators for the routes and for the sizes of the matrices; and, of course, there were lists of code words, with their meanings.

11A

invention of Anson Stager, whom I have mentioned before in connection with the establishment of the USMTC, and who is said to have first devised such ciphers for General McClellan's use in West Virginia, in the summer of 1861, before McClellan came to Washington to assume command of the Army of the Potomac.

Anson Stager <sup>and many others</sup> ~~may have~~ thought that he was the original inventor of the system, but <sup>such a belief.</sup> ~~if he did, he~~ was quite in error, <sup>because</sup> word-transposition methods, <sup>similar to Stager's</sup> were in use hundreds of years before his time. For instance, in 1685, in an unsuccessful attempt to invade Scotland in a conspiracy to set the Duke of Monmouth on the throne, Archibald Campbell, 9th Earl of Argyll, suffered an unfortunate "accident". He was taken prisoner and beheaded by order of James the Second. The communications of the poor Earl were not secure, and when they fell into government hands they were soon deciphered. The method Argyll used was that of word transposition, and if you are interested in reading a contemporary account of how it was solved, look on pages 56-59 of that little book I mentioned before as being one of the very first books in English dealing with the subject of cryptology, that by James Falconer, entitled Cryptomenysis Patefacta: Or the Art of Secret Information Disclosed Without a Key, published in London in 1685. There you will find the progenitor of the route ciphers employed by the <sup>USMTC,</sup> ~~Federal Army~~ ~~in the War of the~~ ~~Revolution,~~ <sup>180</sup> ~~which~~ ~~was~~ ~~used~~ ~~200~~ years after Argyll's abortive rebellion.

The <sup>route</sup> cipher systems employed by the USMTC, ~~for messages of the Federal Army in the years 1861-65~~ are fully described in a book entitled The Military Telegraph during the Civil War, by Colonel William R. Plum, published in Chicago in 1882.

I think Plum's description of them is of considerable interest and I recommend his book to those of you who may wish to learn more about <sup>them, but they are pretty much all</sup> ~~these systems~~ alike. If I show you one example of an actual message and explain its encipherment and decipherment I will have covered practically the entire gamut of the route ciphers used by the USMTC, so basically very simple and uniform were they. And yet, believe it or not, legend has it that the Southern Signalmen were unable to solve any of the messages transmitted by the USMTC. This long-held legend I find hard to believe. In all the descriptions I have encountered in the literature not one of them, save the one quoted above from O'Brien, tries to make these ciphers as simple as they really were; somehow, it seems to me, a subconscious realization on the part of Northern writers, usually ex-USMTC operators, of the system's simplicity prevented a presentation which would clearly show how utterly devoid it was of the degree of sophistication one would be warranted in expecting in the secret communications of a great modern army in the decade 1860-1870, three hundred years after the birth of modern cryptography in the papal states of Italy.

Let us take the plain text of a message which Plum (page 58) uses in an example of the procedure in encipherment. The cipher book involved is No. 4 and I happen to have a copy of it so <sup>we</sup> can easily check Plum's work. Here's the message to be enciphered:

Washington, D.C.  
July 15, 1863

For Simon Cameron <sup>2/</sup>

I would give much to be relieved of the impression that Meade, Couch, Smith and all, since the battle of Gettysburg, have striven only to get the enemy over the river without another fight. Please tell me if you know who was the one corps commander who was for fighting, in the council of war on Sunday night.

(Signed) A. Lincoln

<sup>2/</sup> Simon Cameron was Lincoln's Secretary of War until Jan. 1862, when he was replaced by Edwin M. Stanton. If this message cited by Plum is authentic, and there is no reason to doubt this, then Cameron was still in friendly contact with Lincoln, possibly as a special observer.

Plum shows the word-for-word encipherment in a matrix of seven columns and eleven rows. He fails to tell us why a matrix of those dimensions was selected; presumably the selection was made at random, which was certainly permissible.

Fig. 4

	1/	2/	3/	4/	5/	6/	7/
Cipher	(heavy) (null)				(county) (null)	(square) (null)	
Plain	Incubus/ Washington, D.C.	Stewart/ July	Brown/ 15th	Norris/ 18	Knox/ 60	Madison/ 3	for
Cipher	sigh	man	Cammer	on	flea	I	wood
Plain	Simon		Cameron		(Period)	I	would
	give	much	Toby	traveled	serenade	impression	that
	give	much	to be	relieved	of the	impression	that
	Bunyan Meade	bear , (comma)	ax Couch	cat , (comma)	children Smith	and and	and all
	bat , (comma)	since since	the the	knit battle	of of	get Gettys	ties
	large burg	ass , (comma)	have have	striven striven	only only	to to	get get
	village the enemy	skeleton over	turnip the river	without without	another another	optic fight	hound (period)
	Please Please	tell tell	me me	if if	you you	no know	who who
	was was	the the	Harry one	Madrid corps	locust commander	who who	was was
	for for	oppressing fighting	bitch , (comma)	quail in the	counsel council	of of	war war
	on on	Tyler Sunday	Rustle night	upright Signature	Adrian A. Lincoln	bless (null)	him (null)
NULLS		(Monkey) (null)	(Silk) (null)	(Martyr) (null)			(Suicide) (null)

Ruled paper was provided to aid in accuracy. In the diagram the upper part of lines of writing is the cipher, the lower part, the plain text.

*Handwritten notes:*  
 - circled "numbers" with an arrow pointing to the column headers.  
 - circled "move to bottom of page" with an arrow pointing to the null row.

Note the <sup>seven</sup> nulls (non-significant, or "blind" words) at the <sup>tops and certain</sup> bottoms of each column, these being added to <sup>the cipher text in order to</sup> confuse a would-be decipherer. At least that was the theory, but how effective this subterfuge was can be surmised, ~~very little~~ once it became known that <sup>employing nulls</sup> this was the usual practice. Note also the two nulls (bless and him) at the end of the <sup>last line to complete that line of the matrix.</sup>

The cipher message is then copied down following the route prescribed by the indicator "BLONDE", as <sup>given</sup> ~~can be seen~~ on page 7 of Cipher Book No. 4. The indicator could have also been "LINIMENT".

Fig. 5

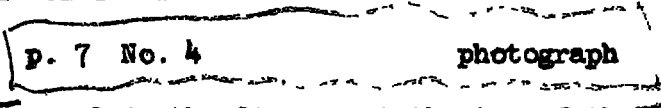
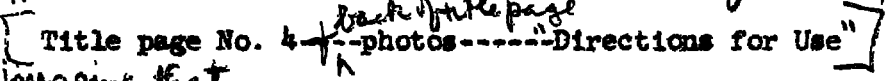


Fig. 5 I will

If you ask me to explain the diagram at the top of the picture I will simply show you the "Directions for Use" which appear on the reverse side of the title page of "War Department Cipher No. 4", because I'm afraid you wouldn't believe me if I merely <sup>told you what they say. In Fig. 6 is</sup> quoted from those directions. Here's a picture of the title page and I follow it with a photograph of what's on its reverse side of the title page:

Figs. 6+7



Do you imagine that ~~remember~~ the chap who was responsible for getting this cipher book approved

ever thought about what he was doing when he caused those "Directions for Use" to be printed? It doesn't seem possible. All he would have had to ask himself was, "Why put this piece of information in the book itself? <sup>Cipher books before this have been captured. Suppose this one</sup> Suppose the book falls into enemy hands; <sup>Can't he read, too,</sup> and at once learn about the intended deception? Why go to all the trouble of including "phoney" routes in the book? If the book doesn't fall into enemy hands what good are the "phoney" routes anyway? Why not just indicate the routes in a straightforward manner, as had been done before?

Thus: "Up the 6th column (since "6" is the first number at the left of the diagram), down the 3rd, up the 5th, down the 7th, up the 1st, down the 4th and down the 2nd.

This matter is so incredibly fatuous that it is hard to understand how sensible men - and they were sensible - could be so <sup>illogical in their</sup> ~~negligent in their logical~~ or thinking processes. But there they stand, for all the world to see and to judge.

Now for the transposition step. The indicator "BLONDE" signifies a matrix of seven columns and eleven rows, with the route set forth above, viz, up the 6th column, down the 3rd, etc., so that the cipher text with a "phoney" address and signature <sup>4/</sup> becomes as follows:

TO A. HARPER CALDWELL, Washington, D.C.  
Cipher Operator, Army of the Potomac:

Blonde bless of who no optic to get and impression I Madison square Brown canner Toby ax the have turnip me Harry bitch rustle silk Adrian counsel locust you another only of children serenade flea Knox County for wood that awl ties get hound who was war him suicide on for was please village large bat Bunyan give sigh incubus heavy Norris on trammled cat knit striven without if Madrid quail upright martyr Stewart man much bear since ass skeleton tell the oppressing Tyler monkey.

(Signed) D. HOMER BATES

4/

It was the usual practice to use for address and signature the names of the USMTC operators concerned.

Note that the text begins with the indicator "BLONDE". In decipherment the steps are simply reversed. The indicator tells what size matrix to outline; the words beginning "bless of who no optic . . ." are inscribed within the matrix: up the 6th column; then, omitting the "check word" or "null" (which in this case is the word "square"), down the 3rd column, etc. The final result should correspond to what is shown in Fig. 20. There then follows the step of interpreting orthographic deviations, such as interpreting "sigh", "man", "camer", and "ca" as Simon Cameron; the word "wood" for "would", etc. <sup>The final step</sup> which then reproduces the original plain text.

Save for one exception, ~~to be discussed in a moment or two~~, all the route ciphers used by the USMIC conformed to this basic pattern. The things that changed from one cipher book to the next were the indicators for the dimensions of the matrices and for the routes; and the "arbitraries" or code equivalents for the various items comprising the "vocabulary", the number of them increasing from one edition to the next, just as might be expected. <sup>The sole exception to this basic pattern</sup>  
~~The sole exception to this basic pattern of the transposition routes employed~~  
 by the USMIC is to be seen in Cipher Book No. 9 and on only one page of the book.

I will show you that page:

Fig. 9  
p. 12 - Cipher Book No. 9

What we have here is a deviation from the straightforward route transposition, up the <sup>columns</sup> ... down the <sup>columns</sup> ... etc. By introducing one diagonal path in the route (the 6th, 7th, 8th, 9th, 10th words in a message of five columns, and the 1st, 2nd, 3rd, 4th, 5th, and 6th words in a message of six columns) the simple up and down route no longer holds true. The words on the diagonal interrupt the normal up and down paths and introduce complexities in the method. In fact, the complexities seemed to be a bit too much for the USMIC cipher operators because, as far as available records show, these complicated routes were never used.

no space

I now wish to make a number of general and a few specific comments  
 on Plum's description of the cryptosystems used by the U/S/M/T/C/

~~set forth in Appendix A~~

Specify  
 here +  
 hereafter

<sup>have learned</sup>  
 First, we ~~note~~ that although Anson Stager, later Colonel Stager,  
 has been credited with inventing the type of cipher under consideration  
 in this study, he was anticipated in the invention <sup>by</sup> of about 200 years.  
 Also, he is given the lion's share of the credit for devising those ciphers  
 although he did have a number of collaborators. ~~Plum~~ Plum names four of them,  
 presumably because he thought them worthy of being singled out for  
 particular attention. Plum and others tell us that copies of messages  
 handled by the U/S/M/T/C/ (sometimes were) intercepted by the enemy but  
<sup>not</sup> ~~that none were~~ solved. He cites no authority for this last statement,  
 merely saying that such intercepts were published in the newspapers of the  
 Confederacy with <sup>the hope that somebody would come up with</sup> requests for help <sup>And</sup> in their solution. ~~But~~ it may be noted  
 that none of the Confederate accounts of war activities cite instances of  
 the solution of intercepted U/S/M/T/C/ messages, although <sup>there</sup> are plenty  
 of citations of instances of interception and solution of enciphered

<sup>the</sup>  
visual transmissions of Federal Army's Signal Corps. ~~Douglas-French's~~

~~See a Lieutenant's mention of a specific instance of solution.~~

*omit*

In referring hereinafter to the cryptographic books used by the U.S.M.T.C., I shall use the term "cipher books," or sometimes simply "ciphers," although the cryptosystem involves both code and cipher processes. Its underlying transposition feature makes it partake of the nature of a cipher system according to modern terminology; but the heavy use of "arbitraries," that is, of arbitrary words to represent the names of persons, places, rivers, etc., important nouns and verbs, etc., makes the system partake of the nature of code.

Plum states that 12 different cipher books were employed by the Telegraph Corps, but I <sup>think</sup> ~~think~~ <sup>actually</sup> ~~think~~ there were only eleven. The first one was not numbered, and this is good evidence that a long war was not expected <sup>was made for such a</sup> ~~that there were no preparations for a long war, and that heavy~~

~~impression on its outbreak.~~ This first cipher book had

16 printed pages. But for some reason, now impossible to fathom, the sequence of numbered books thereafter was as follows: Nos. 6 and 7, which were much like the first (unnumbered) one; then came Nos. 12, 9, 10--in

that strange order; then came Nos. 1 and 2; finally came Nos. 3, 4, and 5.

(Apparently there was no No. 8, or No. 11 → <sup>at least they are never mentioned.</sup> It would be ~~wisdom~~ <sup>for the purpose</sup> to think

that the irregularity in numbering the successive books was of communication-

but there are other things about the books and the cryptosystem that affect security. There must have been <sup>other</sup> reasons, <sup>but what they were is now</sup> unknown. Plum states that No. 4, the last one used in the war, was placed

into effect on 23 March 1865, and that it and all other ciphers were

discarded on 20 June 1865. However, as noted, there was a No. 5, which

Plum says was given a limited distribution. I have a copy of it, but

whether it was actually put into use I do not know. Like No. 4, it had

40 pages; about 20 copies were sent to certain members of the <sup>USMTC,</sup> ~~the~~ <sup>Military</sup> ~~Telegraph Corps,~~

scattered among 12 states; and, of course, Washington <sup>must have</sup> had at least one copy.

We may assume with a fair amount of certainty that the first (the unnumbered) cipher book used by the U/S/M/T/C/ was merely an elaboration of the one Stager produced for the communications of the governors of Ohio, Indiana and Illinois, and of which a copy is given by only one of the writers who have told us about these ciphers, <sup>namely,</sup> David H. Bates.



*Bates,*

~~He~~ in his series of articles entitled "Lincoln in the Telegraph Office"

The Century Magazine, Vol. LXXIV, Nos. 1-5, May-Sept, 1907\* shows a

facsimile thereof (p. 292, June 1907 issue), and I have had as good a

reproduction made of it as is possible from the rather poor photographic

facsimile. The foregoing cipher is the prototype upon which all subsequent

cipher books were based, the first of the War Department series being the

one shown by Plum, ~~in Appendix 1 to this lecture.~~

Fig. 9

to 1st Stage  
sent for  
Governor

When these ciphers came into use it was not the practice to misspell

certain words intentionally; but as the members of the U.S.M.T.C (who,

as I've told you, not only served as telegraph operators but also as

cipher clerks) developed expertness, the practice of using non-standard

orthography was frequently employed to make solution of messages more

difficult. *You have already seen examples of this practice, and one can*  
~~Thus, "meat" became "meat" or even "flesh"; "wood" is used in~~

~~place of "would", etc. In an actual case involving a message sent to~~

~~General Grant at Vicksburg the word "Arkansas" is spelled in three words:~~

"Art" "can" "ass," and one finds <sup>other</sup> hundreds of examples of this sort of

artifice. Then, further to increase security, more and more ~~"arbitrariness"~~

\*The series was then put out in book form under the same title by the D. Appleton-Century Company, New York, 1907, reprinted in 1939.

~~these~~ code equivalents were added to represent such things as ordinal and cardinal numbers, months of the year, days of the week, hours of the day, ~~geographical names of places and rivers~~, punctuation, etc. As a last <sup>additional</sup> step, code equivalents for frequently-used words and phrases were introduced. One good example of two typical pages from one of these books will characterize them all.

Photo of p. 14-15  
from No. 12

Fig. 10

You will notice that the code equivalents are printed but their meanings are written in by hand. This was usually the case, and the reason is obvious: for economy in printing costs, because the printed code equivalents of plain-text items in cipher books belonging to the same series are identical; only their meanings change from one book to another, and of course, the transposition routes, their indicators, and other variables change from one book to another. ~~As already indicated~~, I am fortunate in having six of these cipher books in my private collection, so that comparisons among them are readily made. The first feature to be noted is that the code equivalents are all good English dictionary words (or proper nouns), of not less than three nor more than seven (rarely eight) letters. A careful scrutiny shows that in the early editions the code

equivalents are such as are not <sup>very</sup> likely to appear as words in the plain-text

messages; but in the later editions, beginning with No. 12, more than 50%

of the words used as code equivalents are such as might well appear in the

plain-text of messages. For example, words such as AID, ALL, ARMY,

ARTILLERY, JUNCTION, CONFEDERATE, etc., baptismal names of persons, and

names of cities, rivers, bays, etc., appear as ~~the~~ code

equivalents. Among names used as code equivalents are SHERMAN, LINCOLN,

THOMAS, STANTON, and those of many other prominent officers and officials

of the <sup>Union</sup> ~~Federal~~ Army and <sup>The Federal</sup> Government, <sup>as well as of the Confederate Army and Government</sup> and, even more intriguing, such names

were employed as indicators for the number of columns and the routes used—

the so-called "Commencement Words." It would seem that names and words

such as those I've mentioned might occasionally have brought about instances

where difficulty in deciphering messages arose from this source of confusion,

but the literature doesn't mention them. <sup>I think you already realize</sup> ~~A bit later we shall see~~ why such

commonly-used proper names and words were not excluded. There was, indeed,

method in this madness.

But what is indeed astonishing to note is that in the later editions of

these cipher books, in great majority of cases the words used as

"arbitrarities," differ from one another by at least two letters (for example,

LADY and LAMB, LARK, and LAWN, ALBA and ASIA, LOCK and WICK, MILK and MINT),

or by more than two (for example, MYRILE and MYSTIC, CARBON and CANCER,

ANDES and ATLAS) ~~and~~ One has to search for cases in which two

words differ by only one letter, but they can be found if you search long

enough for them, as, for example, QUINCY and QUINCE, PINE and PIKE, NOSE

and ROSE. Often there are words with the same initial trigraph or

tetragraph, but then the rest of the letters are such that errors in

transmission or reception would easily manifest themselves, as, for example, *in the cases*

*of* MONSTER and MONARCH, MAGNET and MAGNOLIA. All in all, it is important to

note that the compiler or compilers of cipher books had adopted a principle

known today as the "two-letter differential," a feature found only in

codebooks of a much later date. In brief, the principle involves the use,

in a given codebook, of code groups differing from one another by at

least two letters. This principle is employed by knowledgeable code

compilers to this very day, not only because it enables the recipient of a

to correct them. This is possible <sup>made</sup>

message to detect errors in transmission or reception, but also <sup>because</sup>

<sup>are printed in the code books; so that most</sup>

if the permutation tables used in constructing the code words <sup>facilitate their</sup>

errors can be corrected

<sup>of the transmission.</sup>

<sup>corrected</sup> without calling for a repetition. It is clear, therefore, that

the compilers of these cipher books took into consideration the fact that

errors are to be expected in Morse telegraphy, and by incorporating, but

only to a limited extent, the principle of the two-letter differential,

they tried to guard against the possibility that errors might go undetected. Had artificial 5-letter groups been used as code equivalents, instead of dictionary words, possibly the cipher books would also have contained the permutation tables. But There is, however, another feature about the words the compilers

of these books chose as code equivalents. It is a feature that manifests

<sup>and you probably already have divined it,</sup>

real perspicacity on their part. A few moments ago I said that I would

explain why, in the later and improved editions of these books, words which

might well be words in plain-text messages were not excluded from the lists

of code equivalents: it involves the fact that the basic nature of the

cryptosystem in which these code equivalents were to be used was clearly

recognized by those who compiled the books. Since the cryptosystem was

based upon word transposition, what could be more confusing to a would-be

cryptanalyst, working with messages in such a system, than to find himself

<sup>of a message he is trying to solve</sup>

unable to decide whether a word in the cipher text <sup>is actually in the</sup>

It must be noted that permutation tables made their first appearance only about a quarter of a century after the Civil War had ended, and these only in the first advanced types of commercial codes.

original plain-text message and has its normal meaning, or is a code word with a secret significance--or even a null, a non-significant word, a "blind" or a "check word," as those elements were called in those days? That, no doubt, is why there are, in these books, so many code equivalents which might well be "good" words in the plain-text messages. And in this connection I have already noted an additional interesting feature: at the top of each page devoted to indicators for signaling the number of columns <sup>or rows</sup> in the specific matrix for a message, ~~these appear in several of these books~~ <sup>are printed the</sup> or what we now call "indicators." Now, there are nine, such so-called "commencement words," ~~with~~ <sup>or</sup> words, in sets of three, any one of which could actually be a real word ~~or name~~ in the plain-text message. <sup>Words when used as</sup> Such indicators could be very confusing to enemy cryptanalysts, especially after the transposition operation. Here, <sup>for examples</sup> are the "commencement words" on page 5 of Cipher Book No. 9: Army, Anson, Action, Astor, Advance, Artillery, Anderson, Ambush, Agree; on page 7 of No. 10: Cairo, Curtin, Cavalry, Congress, Childs, Calhoun, Church, Cobb, etc. Moreover, in Nos. 1, 3, 4, 5, and 10 the "line indicators," that is, the words indicating the number of horizontal rows in the matrix, are also words such as could easily be

words in the plain-text messages. For example, in No. 1, page 3, the

line indicators are as follows:

*break into two or more cols to save space*

Address	1	Faith
Adjust	2	Favor
Answer	3	Confine
Appear	4	Bed
Appeal	5	Beef
Assume	6	Bend
Awake	7	Avail
Encamp	8	Active
Enroll	9	Absent
Enough	10	Accept

*10 which*

Note two things in the foregoing list: first, there are variants--there are two indicators for each case; and second, the indicators are not in strict alphabetic sequence. This departure from strict alphabeticity is even more obvious in the pages devoted to vocabulary, a fact of much importance cryptanalytically. Note this feature, for example, in Fig. <sup>10 which</sup> 30, showing ~~pages~~ pages 14 and 15 of Cipher Book No. 12.

In this respect, therefore, these books partake somewhat of the nature of <sup>or "randomized"</sup> two-part codes, or, in British terminology, "hatted" codes. In the second lecture of this series the physical difference between one-part and two-part codes was <sup>briefly</sup> explained, ~~and it is therefore unnecessary to repeat that explanation here.~~ <sup>but</sup> an indication of the technical <sup>Cryptanalytic</sup> difference between these two types of codes ~~from the point of view of cryptanalysis~~ may be useful at this point. Two-part codes are much more difficult to

solve than one-part codes, in which both the plain-text elements and their code equivalents progress in parallel sequences. In the latter type of determination of the meaning of one code group quickly and rather easily leads to the determination of the meanings of other code groups above or below the one that has been solved. For example, in the following ~~example~~, *short but illustrative*

*meaning of*  
example, if the code group 1729 has been determined to be "then," the

meaning of the

1728---the  
1729---then  
1730---there

code group 1728 could well be "the," *and* that of the code group 1730, "there".

But in a two-part code, determining the meaning of the code group 0972 *to be*

7621---the  
0972---then  
1548---there

~~as being the word~~ "then," gives no clue whatever as to the meaning of

the groups 7621 or 1548. For ease in decoding messages in such a code

there must be a section in which the code groups are listed in numerical *and are accompanied by* sequence, *which, of course, will be* their meanings, ~~listed~~ in a random sequence. The compilers of

the U.S./M./T./C./ cipher books must have had a very clear idea of what I

have just explained, but, ~~as a matter of fact~~, they made a compromise

of a practical nature between a strictly one-part and a strictly two-part



for accuracy.

code, because they realized that a code of the letter sort is twice as  
*besides being much more laborious to compile and check the contents,*  
 bulky as one of the former sort, <sup>a</sup> The arrangement they chose wasn't ~~at all~~

too

bad, so far as crypto-security was concerned. As a matter of fact, and  
 ^

speaking from personal experience in decoding a rather long message

addressed to General Grant, I had a <sup>difficult</sup> trying time in locating many of the

code words in the book, because of the departure from strict alphabeticity.

I came across that message in a work-book in my collection, the work-book

of one of the important members of the U/S/M/T/C--none other ~~the Colonel~~ <sup>than our friend</sup>

Plum, from whose book, The Military Telegraph during the Civil War, comes

~~As you know~~ much of the data I've presented, <sup>in this lecture.</sup> On the ~~first~~ fly-leaf of

Plum's work-book there appears, presumably in his own handwriting, the

legend "W. R. Plum Chf Opr with Gen. G. H. Thomas". Here's one of the

messages he enciphered in Cipher Book No. 1, the book in which, he says,

more important telegrams were sent than in any other:

Fig. 11

Note how many "arbitraries" ~~or words with secret meanings~~, appear in

the plain-text message, that is before transposition. After transposition

*code words, indicators and nulls makes the cryptogram*

the melange of plain-text, ~~and code words must have been quite mystifying.\*~~ *appears rather*

And yet, was the system ~~so very~~ *as* inscrutable ~~after all? I don't think so.~~ *as its users apparently thought?*

Even in the case of the foregoing message there are enough unencoded words in ~~sequence in the plain-text version~~ So that with a bit of patience, ~~in working on the cipher version, I think the transposition could be removed~~ without too much difficulty and the general tenor of the message could be determined. There would remain, of course, the business of finding the specific meanings of the code words. In the case of cipher book No. 1, which, ~~was~~ according to Plum, the one that had the longest and widest use, an accumulation of messages would probably have given enough data for

determining the specific meanings of the code words. ~~But~~ It is to be

*of course,* remembered, ~~that these~~ *them* messages were transmitted by wire telegraphy, ~~and not~~ by radio, so that ~~opportunities for intercepting or "tapping" telegraph~~ *enemy messages could be obtained only by* or capturing couriers or headquarters with their files intact. Opportunities for these lines were not frequent, ~~but~~ they did occur from time to time, and in one

case a Confederate signalman hid in a swamp for several weeks and tapped a Federal telegraph line, obtaining a good many messages. What success, if any,

did Confederate cryptanalysts have in their attempts to solve such ~~problems~~

\*In searching for a good example my eye caught the words "Lincoln shot" at the left of the matrix and I immediately thought that the message had to do with Booth's assassination of the President. But after hurriedly translating the message and finding nothing in it having anything to do with the shooting it occurred to me to look up the indicators for a matrix of six rows and eight columns. They turned out to be LINCOLN (message of 8 columns), SHOP (6 rows) The word SMALL beneath the "Lincoln shot" is a variant for SHOT, also meaning "6 rows".

*methods of acquiring enemy traffic*

as  
 U.S.M.T.C cryptograms, they did intercept? We shall try to answer this question in due time, ~~but now we must hasten to a consideration of the cryptosystems employed by the Confederate States Army.~~

As indicated earlier, in the Confederacy there were no competing signal organizations, as there were on the Union side. There was nothing at the center of government in Richmond or in the combat zone comparable to the ~~extensive~~ <sup>extensive</sup> and tightly-controlled civilian military telegraph organization which Secretary Stanton ruled with <sup>such</sup> an iron hand from Washington. Almost as a concomitant it would seem, there was in the Confederacy, save for two exceptional cases, one and only one <sup>officially established</sup> cryptosystem to serve the need for protecting tactical as well as strategic communications, and that was the so-called Vigenere Cipher, which apparently was the cipher authorized in an official manual prepared by Capt. <sup>J.H.</sup> Alexander as the partial equivalent of Myer's Manual of Signals. You won't find the name Vigenere in any of the writings of contemporary signal officers of either the North or the South. The signalmen of those days called it the "Court Cipher," this term referring to the system in common use <sup>for</sup> in diplomatic or "court" ~~secret~~ communications about this period in history. It is ~~hardly necessary for me to tell you in detail about that cipher which employs~~ the so-called Vigenere Square with a repeating key.\* Here is the square which Plum <sup>tells the "Confederate States Cipher Key" and</sup> presents in his <sup>which is followed by his description of its manner of employment:</sup> ~~description, and for reasons that will soon become quite clear, I will~~ present his description exactly as he gives it:

\*A keyword is employed to change the alphabets cyclically, thus making the cipher what is called today a periodic or multiple-alphabet cipher controlled by the individual letters of a key, which may consist of a word, a phrase, or even of a sentence, repeated as many times as necessary.

*made  
plans*

CONFEDERATE STATES CIPHER KEY.

26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	
1	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
2	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	
3	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z		
4	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z			
5	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z				
6	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z					
7	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z						
8	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z							
9	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z								
10	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z									
11	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z										
12	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z											
13	m	n	o	p	q	r	s	t	u	v	w	x	y	z												
14	n	o	p	q	r	s	t	u	v	w	x	y	z													
15	o	p	q	r	s	t	u	v	w	x	y	z														
16	p	q	r	s	t	u	v	w	x	y	z															
17	q	r	s	t	u	v	w	x	y	z																
18	r	s	t	u	v	w	x	y	z																	
19	s	t	u	v	w	x	y	z																		
20	t	u	v	w	x	y	z																			
21	u	v	w	x	y	z																				
22	v	w	x	y	z																					
23	w	x	y	z																						
24	x	y	z																							
25	y	z																								
26	z																									

~~Key Words: Complete Victory. Manchester Bluff.~~

To put into cipher the first message, which is put up by using "Manchester Bluff" as the key, and the second by the key term, "Complete Victory," find at the left-hand side of the table the first letter of the first word to be ciphered, and at the top of the table, the first letter of the term. At the junction of the columns in which these letters are so found, will be seen the arbitrary letter which is to be used in lieu of the real one at the left. Continue in this way with each successive letter of the message and key term, repeating on the latter till finished. Thus, "Sherman is victorious," put in cipher by using the first key, would read, as shown by the capitals, c-o-m-p-l-e-t--ev--i-c-t-o-r-y. C-o-m-p- Of course, any

UVQG XEG MN DKV HFP KCGH.

change in the key word, term or phrase changes the arbitraries, and if neither the real message nor the key is known, it would be somewhat vexatious working it out, unless there were some such suggestive words as occur in Davis's message above, which indicate the ciphered words very clearly; e.g., "By which you may effect" o tpgexyk a crossing

"above that part" hj opg kmct This meaning occurred to the author, of the river.

at first sight, and doubtless would be to any one familiar with military affairs in that section. Having guessed real words, it is very easy to work out the letters of the key. The following two important ciphers were transmitted as divided below; i.e., each word was sent separately, not all mixed, as in the Pemberton cipher. This division does not facilitate translation by the key at all, but materially assists without it, and was, therefore, bad practice. We give below, each message, with its translation, because these telegrams were very important. The curious reader may, at his leisure, by using the key board, study out the key terms, one of which will be found entirely new and quite apropos, in the light of what speedily followed.

*chr part of  
house on West  
set left*

*July 12  
30*

CONFEDERATE STATES OF AMERICA, MILITARY TELEGRAPH, Dated  
Head-quarters, February 25, 1865. Received at Richmond,  
Va., 12:25 minutes, A.M.

TO HON. J.C. BRECKENRIDGE, Sec'y of War:--I recommend  
that the tsysmee fn qoutwp rfatvump ubwaqbqtm exfvxj and is-  
waqjru ktntl are not of immediate necessity, uv kppfmbpgr  
mpc thnlfl should be lmghtsp. (Signed) R.E. LEE

TRANSLATION.--I recommend that the removal of public  
property, machinery, stores and archives which are not of  
immediate necessity, be commenced. All powder should be  
secured.

more  
space

HEAD-QUARTERS C.S. ARMIES, March 24, 1865.

GEN. E. KIRBY SMITH, comdg. Trans-Miss. Dept., Gen:--  
Vvg ecilmympm rvcog ui lhommides kfch kdf wasptf us tfcfsto  
abxc bix azjkhmgjsiimivbceq qb ndel ueisu ht kfg auhd egh  
opcm mfs uvajwh xrymcoci yu dddxtmpt iu icjqkpxt es vvjau  
mvrr twhtc abxc iu eoiag o rdegx en ucr yv ntiptyaec  
rqvariyyb rgzq rspx rksjeph ptax rsp ekez raecdstrzpt  
mzmseb acgg nsfqvfv mc kfg smhe ftrf wh mvv kkgc pyh fefm  
ckfrlisytxl xj jtbbx rq httdl whz awvv fd acgg avwzv  
yciag ce nzyfet lgtz scuh.

I am most respectfully your obdt. servt.,  
(Signed) R.E. LEE

TRANSLATION.--Gen: The president deems it advisable  
that you should be charged with the military operations on  
both banks of the Miss., and that you should endeavor as  
promptly as possible to cross that river with as large a  
force as may be prudently withdrawn from your present Dept.  
You will accordingly extend your command to the east bank  
of the Miss., and make arrangements to bring to thi-side  
such of your present force as you may deem best.

I am most respectfully your obedient servant.

more  
space

There are certain comments to be made on the foregoing <sup>messages</sup> ~~which is all~~

~~right as far as it goes, but it just doesn't go far enough, unfortunately, for~~

~~the procedure plan given has two fatal defects.~~

no P In the first place, note that in the first message certain words are

left unenciphered; in the second place, in both the first and the second

message, the ciphers retain and clearly show the lengths of the words which

have been enciphered. Both of these faulty practices <sup>greatly weaken the security of ciphers</sup> ~~are rather failures in~~

~~because they leave good clues to their contents and can easily result in facilitation~~  
~~practices afford clues to solving the messages. We know today that cipher~~ <sup>resolution of</sup>

<sup>must</sup> messages ~~should~~ leave nothing in the clear. Even the address and the signature,

the date, time and place of origin etc., ~~it~~ should if possible be hidden; and  
 the cipher text should be in completely regular groupings, <sup>first,</sup> so as not to disclose  
 the lengths of the plain-text words, and <sup>second,</sup> ~~also~~ to promote accuracy in  
 transmission and reception.

So far as my studies have gone, I have not found a single example of  
 a Confederate Vigenere cipher which shows neither of these two fatal  
 weaknesses. ~~And~~ <sup>The</sup> second of the two ~~following~~ examples is the only case  
 I have found <sup>in</sup> which there are no unenciphered words in the text of the message.  
 And the only example I have been able to find in which word lengths are not  
 shown (save for one word) is in the case of the following message:

Vicksburg, Dec. 26, 1862.

GEN. J.E. JOHNSTON, JACKSON:

I prefer oaavvr, it has reference to xhvkjqchffabpzelreqpzwnyk  
 to prevent anuzeyxswstpjw at that point, raeelpsgghvelvtzfautililaslt  
 lhifnaigtsumlfgcajd.

(Signed) J.C. PEMBERTON,  
 Lt. Gen. Comdg.

Even in this case there are unenciphered words which afford <sup>ed</sup> a clue which enabled  
 our men <sup>to find the key and</sup> ~~to solve the message~~. It took some time, however, and the <sup>story is</sup>  
~~to solution~~ <sup>insert</sup> ~~attack~~

In the various accounts of these <sup>Confederate</sup> ciphers ~~I have encountered~~ <sup>there is</sup> one and only  
<sup>writer who makes a detailed comment on</sup> one ~~dissenting voice in regard to~~ the two fatal practices to which I refer.

A certain Dr. Charles E. Taylor, a Confederate veteran (in an article entitled  
 "The Signal and Secret Service of the Confederate States," published in the  
 Confederate Veteran, Vol. XL, Aug-Sept 1932), after giving an example of  
 encipherment according to the "court cipher" says:

Insert to  
p. 32

worth telling.

According to Plum, the foregoing cipher message was the very first one captured by USMTC operators, and it was obtained during the siege of Vicksburg, which surrendered on 4 July 1863. But note the date of the message: 26 December 1862. What was done with the captured message during the months from the end of December 1862 to July 1863? <sup>Apparently nothing.</sup> Here is what Plum reports:

Sample space

What efforts General Grant caused to be made to unravel this message, we know not. It was not until October, 1864, that it and others came into the hands of the telegraph cipherers, at New Orleans, for translation. ...

The New Orleans operators who worked out this key [Manchester Bluff] were aided by the Pemberton cipher and the original telegram, which was found among that general's papers, after the surrender of Vicksburg; also by the following cipher dispatch, and one other.

Plum gives the messages involved, and their solution, and the keys, the latter being the three cited above. It would seem that <sup>if the captured Pemberton message</sup> General Grant had been brought to General Grant's attention and he did nothing.

about it, he was not <sup>REF ID: A62851</sup> ~~much interested~~ in intelligence.

Secondly, the solution of the <sup>Pamberton</sup> message and the others apparently took some time, even though there was one message with its plain text (the Pamberton message) and two messages not only with interspersed plain-text words but also with spaces showing word lengths. But Plenum does not indicate how long it took for solution. Note that he merely says that the messages came into the hands of the telegraph operators in October 1864; he does not tell when solution was reached.



It hardly needs to be said that the division between the words of the original message as given above was not retained in the cipher. Either the letters were run together continuously or breaks, as if for words, were made at random. Until the folly of the method was revealed by experience, only a few special words in a message were put into cipher, while the rest was sent in plain language. This afforded opportunity for adroit and sometimes successful guessing. . . . I think it may be said that it was impossible for well prepared cipher to be correctly read by any one who did not know the key-word. Sometimes, in fact, we could not decipher our own messages when they came over telegraph wires. As the operators had no meaning to guide them, letters easily became changed and portions, at least, of messages rendered unmeaningly [*sic*] thereby.

Frankly, I don't believe Dr. Taylor's comments are to be taken as characterizing the ~~part~~ practices that were usually followed. No other ex-signalman who has written about the ciphers used by the Confederate Signal Corps makes such observations and I think we must simply discount what Dr. Taylor says in this regard.

It would certainly be an unwarranted exaggeration to say that the two weaknesses in the Confederate cryptosystem cost the Confederacy the victory for which it fought so mightily, but I do feel warranted at this moment in saying that further research may well show that certain battles and campaigns were lost because of <sup>insecure crypto-communications.</sup> ~~faulty cryptography leading to communications~~ ~~insecurity.~~

A few moments ago I said that, save for an exception or two, there was in the Confederacy one and only one cryptosystem to serve the needs <sup>for</sup> ~~of~~ secure tactical as well as strategic communications. One of these exceptions concerned the cipher used by General Beauregard after the battle of Shiloh (8 April 1862). This cipher was purely monoalphabetic in nature <sup>and</sup> ~~in one~~ ~~example a reciprocal cipher alphabet was used:~~

~~A B C D E F G H I J K L M  
N O P Q R S T U V~~

~~This simple cipher~~ was discarded as soon as the official cipher <sup>system</sup> was prescribed in Alexander's manual. *It is interesting to note that this was done after* ~~It was just as well that~~ Beauregard's cipher

~~was discarded because~~ the deciphered message came to the attention of

Confederate authorities in Richmond via a northern newspaper! It is <sup>also interesting</sup> curious

to note that the Federal War Department had begun using ~~cryptosystems for~~ <sup>the route cipher is the official system</sup>

<sup>for</sup> U/S/M/T/C/ messages very promptly after the outbreak of war, whereas not until

1862 did the Confederate States War Department prepare an official cryptosystem,

and then it adopted the "court cipher".

The other exception involved a system used at least once before the

official system was adopted and it <sup>was so different from the latter that it</sup> should be mentioned. On 26 March 1862,

the Confederate States President, Jefferson Davis, sent General Johnston by

special messenger a dictionary, with the following accompanying instruction:\*

I send you a dictionary of which I have the duplicate, so that you may communicate with me by cipher, telegraphic or written, as follows: First give the page by its number; second the column by the letter L, M or R, as it may be, in the left-hand, middle, or right-hand columns; third, the number of the word in the column, counting from the top. Thus, the word junction would be designated by 146, L, 20.

~~Here is a sample~~ <sup>The foregoing, as you no doubt have already realized, is</sup> of the types of cryptosystems used by both sides during

the American Revolutionary Period almost a century before, except that in

this case the dictionary had three columns to the page instead of two. I

haven't tried to find <sup>the</sup> ~~what~~ dictionary ~~was used~~ but it shouldn't take long to

locate it, since the code equivalent of the word "junction" was given: 146, L, 20.

Moreover, there is extant <sup>at least</sup> one fairly long message, with its decode, ~~given~~. How

many other messages there may be in National Archives I don't know.

\*Battles and Leaders of the Civil War, New York: The Century Co., 1884, Vol. I p. 581.

Coming back now to the "court cipher," you will probably find it just

as hard to believe, as I find it, that according to all accounts <sup>three</sup> ~~four~~ and

only <sup>three</sup> ~~four~~ keys were used by the Confederates during <sup>the three and a half</sup> ~~three whole~~ years of

warfare <sup>mid-</sup> from 1862 to 1865. It is true that Southern signalmen make mention

of frequent changes in key but ~~in all the literature~~ only the following

<sup>three</sup> ~~four~~ are specifically <sup>cited:</sup> ~~given:~~

- 1) COMPLETE VICTORY
- 2) MANCHESTER BLUFF
- 3) COME RETRIBUTION

*all on 1 line*

~~4) IN GOD WE TRUST~~

*There may have been a fourth key,*

It seems that all were used concurrently. ~~The first three were used~~

but I have seen it only once, and that is in a book explaining the "court cipher". ~~many times, the last well, I just don't know because only one example has~~

<sup>not</sup> ~~turned up.~~ Note that ~~in the case of the first three, the key consists of~~

~~each of the three keys listed above,~~ <sup>length was chosen</sup> exactly 15 letters, but why this ~~should be so~~ is not clear ~~to me~~.

Had <sup>contained only</sup> the rule been to make the cipher messages ~~of~~ 5-letter groups, the

explanation would be easy: 15 is a multiple of 5 and this would be of

practical value in checking the cryptographic work. But, as has been clearly

stated, <sup>disguising</sup> ~~the disguise of~~ word lengths was <sup>apparently</sup> ~~not even contemplated, let alone~~ <sup>not the practice even if it was</sup>

prescribed, so that there <sup>was</sup> ~~seems to be~~ no advantage in choosing ~~the~~ keys which

<sup>a multiple of 5.</sup> contain ~~exactly 15~~ letters. And, by the way, doesn't the key COME RETRIBUTION

<sup>even</sup> sound rather ominous to you these days?

~~An example or two of authentic Confederate messages which were~~

~~intercepted and deciphered by members of the U.S. M. T. C. may be of interest. Here~~

~~is one:~~

P. 42 - SIS monograph

And here is another:

~~Perhaps you will wish to decipher them, which should be quite easy in view of the fact that you will merely have to select the proper key from among those given above.~~

Sooner or later <sup>a</sup> ~~one of the~~ Confederate signal officers was bound to come up with a device to simplify ciphering operations, and a gadget devised by a Captain William N. Barker seemed to meet the need. In Myer's Manual there is a picture of one form of the device, shown here in Fig. ~~00.~~<sup>13-</sup> I

don't think it necessary to explain how it worked, for it is almost self-evident.

~~A~~<sup>Several</sup> number of these devices <sup>were</sup> captured during the war, one of them being among the items in the NSA Museum. <sup>(Fig. 14)</sup> But here's a photograph <sup>, Fig. 15,</sup> of the one found in the office of Confederate Secretary of State Judah P. Benjamin after the capture of Richmond.

CIPHER DEVICE

Fig. 15

How many of these devices were in existence or use is unknown, for their construction was an individual matter--<sup>apparently</sup> it was not an item of regular issue to members of the corps. ~~Here's a picture of one captured at Vicksburg and you can see that it was a do-it-yourself job, a rough piece of work.~~

In practically every account of the codes and ciphers of the Civil War you will find references, ~~some in much detail,~~ to ciphers used by Confederate secret service agents engaged in espionage in the North as well as in Canada.

In particular much attention is given to a set of letters in cipher which were intercepted by the New York City Postmaster and which were involved in a plot to print Confederate currency and bonds. Much ado was made about the solution of these ciphers by cipher operators of the U/S/M/T/C/ in Washington and the consequent breaking up of the plot. But I won't go into these ciphers for two reasons. First, the alphabets were all of the simple monoalphabetic type, a total of six altogether being used. Since they were composed of symbols, a different series for each alphabet, it was possible to compose a cipher word by jumping from one series to another without any external indication of the shift, <sup>however,</sup> but good eyesight and a bit of patience were all that was required for solution in this case because of the inept manner in which the system was used: ~~the~~ whole words, sometimes several successive words, were enciphered by the same alphabet. But the second reason for my not going into the story is that my colleague Edwin C. Fishel, whom I've mentioned before, has done some research among the records in our National Archives dealing with this case and he has found something which is of great interest and which I feel bound to leave for him to tell at some future time, as <sup>that</sup> ~~it~~ is his story, ~~and~~ not mine.

So very fragmentary was the amount of cryptologic information known to the general public in those days that when <sup>there was found</sup> on John Wilkes Booth's body <sup>a cipher square which</sup> ~~and in~~ ~~his trunk in the National Hotel in Washington~~ <sup>another copy was found and there were</sup> ~~there were found copies of what~~ ~~was obviously a cipher square~~ ~~since the Federal authorities in Washington~~ ~~had copies of a similar square, captured or taken from prisoners at various~~

~~By Federal authorities in Washington~~

~~times during the war, an attempt was made to implicate leaders of the~~

~~Confederacy in the plot to assassinate Lincoln. They offered as evidence,~~

~~was almost identical with~~  
~~in substantiation of the charge,~~ the cipher square which had been mounted

on the cipher reel found by ~~Union Asst. Secretary of War Charles J. Dins~~

in Confederate Secretary of State Judah P. Benjamin's office in Richmond, ~~the Federal authority~~

~~in Washington~~

Then they attempted to prove that this necessarily meant that the Confederate

were implicated in the plot to assassinate Lincoln and

leaders had been giving Booth instructions in cipher. ~~in regard to the~~ Here's a picture of  
the cipher square found on Booth, and also in a trunk in his hotel room in Washington.

~~assassination, but the attempt was not successful.~~ The following is quoted

15 from Philip Van Doren Stern's book entitled Secret Missions of the Civil War

(Rand McNally and Co., New York, 1959, p. 320):

Everyone in the War Department who was familiar with cryptography knew that the Vigenere was the customary Confederate cipher and that for a Confederate agent (which Booth is known to have been) to possess a copy of a variation of it meant no more than if a telegraph operator was captured with a copy of the Morse Code. Hundreds--and perhaps thousands of people were using the Vigenere. But the Government was desperately seeking evidence against the Confederate leaders so they took advantage of the atmosphere of mystery which has always surrounded cryptography and used it to confuse the public and the press. This shabby trick gained nothing, for the leaders of the Confederacy eventually had to be let go for lack of evidence.

omit

~~It is only fitting that what was probably the last official cipher message of the Confederacy was written in the Vigenere. This was a brief note from Jefferson Davis dated April 24, 1865, at Charlotte, North Carolina, and sent to his secretary, Burton H. Harrison, at Chester, South Carolina. It read: "The hostile government reject the proposed settlement, and order active operations resumed in forty-eight hours from noon today." By a curious coincidence, the key-words needed to decipher this communication were "Come Retribution."~~

To the foregoing I will comment that I doubt very much whether "everyone

in the War Department who was familiar with cryptography knew that the

Vigenere was the customary Confederate cipher." ~~I am sure that not one of~~

Probably

them had even heard the name Vigenere or had even seen a copy of the table,

~~except in such cases as were captured in operations.~~ I doubt whether anyone

on either side even knew that the cipher used by the Confederacy had a name; or,

least of all, that a German Army reservist named Kasiski, in a book published in 1863, showed how the Vigenere cipher could be solved by a straightforward mathematical method. Moreover, I believe that ignorance of cryptography and of its history was so abyssmal that the Union authorities sincerely believed that the cipher square used by the Confederates was actually invented by them and that possession of such a square was prima facie evidence of membership in or association with Confederate conspiracies.

I have devoted a good deal more attention to the methods and means for crypto-communications in the Civil War than they deserve, because professional cryptologists of 1961 can hardly be impressed either by their efficacy from the point of view of ease and rapidity in the cryptographic processing, or by the degree of the technical security they imparted to the messages they were intended to protect. Not much can be said for the security of the visual signaling systems used in the combat zone by the Federal Signal Corps for tactical purposes, because they were practically all based upon simple monoalphabetic ciphers, or variations thereof, as for instance, when whole words were enciphered by the same alphabet. *There is plenty of evidence that* ~~I have cited evidence indicating that~~ Confederate signalmen were more or less regularly reading and solving those signals. What can be said about the security of the route ciphers used by the U/S/M/T/C for strategic or highcommand communications in the zone of the interior? It has already been indicated that, according to accounts by ex-U/S/M/T/C men, *such ciphers* ~~they~~ were beyond the cryptanalytic capabilities of Confederate cryptanalysts, but can we really believe that this was true?

Considering the simplicity of these route ciphers and the undoubted intellectual capacities of Confederate officers and soldiers, why should messages in these systems have resisted cryptanalytic attack? In many cases the general subject matter of a message and perhaps a number of specific items of information could be detected by quick inspection of the message,

*Certainly,*  
~~because~~ if it were not for the so-called "arbitraries" ~~or code words~~ the general sense of the message could be ~~readily~~ found by a few minutes work, since the basic system must have been known through the capture of cipher books, a fact mentioned several times in the literature. ~~It seems almost certain that~~ capture of but one book (they were all generally alike) would have told Confederate signalmen exactly how the system worked and this

would naturally give away the basic secret of the superseding book. So we

must see that whatever degree of <sup>protection</sup> ~~security~~ these route ciphers <sup>afforded, message security</sup> ~~had~~ depended

almost entirely upon the number of "arbitraries" ~~or code groups~~ actually

used in practice. ~~As~~ A review of such messages as are available shows wide

divergencies in the use of the "arbitraries." ~~provided~~. In any event the

number actually present in these books must have fallen far short of the

number needed to give the real protection that a well-constructed code can

<sup>Thus</sup> give, ~~so that~~ it seems to me that the application of native intelligence, ~~should,~~

with some patience, <sup>should have been</sup> ~~be~~ sufficient to solve <sup>USMTC messages -</sup> ~~them~~--or so it would be quite

logical to assume. That such an assumption is well warranted is readily

demonstrable.

~~During the course of preparing this lecture, my friend and colleague,~~



It was, curiously enough, at <sup>about</sup> this point in preparing this lecture that my friend and colleague of my NSA days, Mr. Edwin C. Fishel, ~~a long term member of NSA~~, gave me just the right

material for such a demonstration. In June of 1960, Mr. Fishel had given

Mr. Phillip Bridges, who is also a member of NSA and who ~~know~~ nothing about

the route ciphers of the U/S M/T/C/, the following authentic message sent

on 1 July 1863 <sup>by</sup> from General George G. Meade, at Harrisburg, Pennsylvania,

to General Couch at Washington:

(Message to be furnished) *Fig. 17*

It took Mr. Bridges only a few hours, five or six, to solve the

cryptogram, and he handed the following plain-text to Mr. Fishel:

Thomas been it ←----"Nulls"  
 For Parson. I shall try and get to you by tomorrow morning a  
 reliable gentlemen and some scouts who are acquainted with a  
 country you wish to know of. Rebels this way have all concentrated  
 in direction of Gettysburg and Chambersburg. I occupy Carlisle.  
 Signed Optic. Great battle very soon. tree much deal ←"Nulls"

The foregoing solution is correct, save for one pardonable error:

"Thomas" is not a "null" but an indicator for the dimensions of the matrix

and the route. "Parson" and "Optic" are code names and I imagine that

Mr. Bridges recognized them as such but, of course, he had no way of

interpreting them, except perhaps by making a careful study of the events

and commanders involved in the impending action, a study he wasn't called

upon to undertake.

The foregoing message was enciphered by Cipher Book No. 12, in which

the indicator THOMAS specifies a "Message of 10 lines and 5 columns". The route

was quite simple and straightforward: "Down the 1st (column), up the 3rd; down

the 2nd; up the 5th, down the 4th."

It is obvious that in this example the absence of many "arbitraries" ~~that is, code words with specific plain-text meanings as assigned in the codebook,~~ made solution a relatively easy matter. What Mr. Bridges would have been able to do with the cryptogram had there been many of them is problematical. Judging by <sup>his</sup> ~~the~~ worksheets, <sup>it seemed to me that</sup> Mr. Bridges ~~submitted, it seems~~ <sup>clear that he</sup> did not realize <sup>when he was solving the message</sup> that a transposition matrix was involved; and on <sup>on this point,</sup> questioning him ~~as to whether he knew or suspected this when he commenced~~ <sup>his</sup> work, ~~His~~ answer was in the negative. He realized this only later.

A minor drama in the fortunes of Major General D. C. Buell, one of the high commanders of the Federal Army, is quietly and tersely outlined in two cipher telegrams. The first one, sent on 29 Sept. 1862, from Louisville, Kentucky, was in <sup>one of the USMTC</sup> ~~a~~ cipher book, ~~where I won't tell you,~~ and was externally addressed to Colonel Anson Stager, head of the <sup>USMTC,</sup> ~~Military Telegraph Corps,~~ ~~in Washington,~~ but the internal addressee was Major General H. W. Halleck, "General-in-Chief" [our present day "Chief of Staff"]. <sup>The</sup> ~~This~~ message was externally signed by William H. Drake, Buell's cipher operator, but the ~~real~~ <sup>actual</sup> name of the sender <sup>Buell,</sup> was indicated internally. ~~(For some years, most messages for Washington were externally addressed to Stager. On receipt they were deciphered by clerks of the Military Telegraph Corps and the plain text forwarded to the addressee whose name was enciphered.)~~ Here's the telegram:

COLONEL ANSON STAGER, Washington:

Austria await I is over to requiring orders reapture blissful for your instant command turned and instructions and rough looking further shall further the Camden me of ocean September poker twenty I the to I command obedience repair orders quickly pretty. Indianapolis your him accordingly my fourth received 1862 wounded nine have twenty turn have to to to alvord hasty.

WILLIAM H. DRAKE

Rather than give you the plain-text of this message, perhaps you would like to work it out for yourselves, for with the information you've already received the solution should not be difficult. The message contains one error, which was made in its original preparation: one word was omitted.

The second telegram, only one day later, was also from Major General Buell, to Major General Halleck, but it was in another cipher book--apparently the two books involved were used concurrently. Here it is:

GEORGE C. MAYNARD, Washington:

Regulars ordered of my to public out suspending received 1862 spoiled thirty I dispatch command of continue of best otherwise worst Arabia my command discharge duty of my last for Lincoln September period your from sense shall duties the until Seward ability to the I a removal evening Adam herald tribune.\*

PHILIP BRUNER

As before, I will give you the opportunity to solve this message for yourselves. (At the beginning of the next lecture I shall present the plain-text of both messages.)

*Insert* → To return to J. W. Brown, whom I've mentioned before and who gives us most

of what little sound information there is about the cryptanalytic successes of both sides. First, let's see what the Union signalmen could do with rebel ciphers. Here are the Federals, here are some which he reports: some statements he makes [p. 214]:

The first deciphering of a rebel signal code of which I find any record was that made by Capt. J. S. Hall and Capt. P. A. Taylor, reported Nov. 25, 1862. Four days later, Maj. Myer wrote to Capt. Cushing, Chief Signal Officer, Army of the Potomac, not to permit it to become public "that we translate the signal messages of the rebel army".

*move to left* [ April 9, 1863, Capt. Fisher, near Falmouth, reported that one of his officers had read a rebel message which proved that the rebels were in possession of our code. The next day he was informed that the rebel code taken (from) a rebel signal officer was identical with one taken previously at Yorktown.

He received from Maj. Myer the following orders:

\*A curious coincidence--or was it a fortuitous foreshadowing of an event far in the future?--can be seen in the sequence of the last two words of the cipher text. The message is dated September 30, 1862; the New York Herald and the New York Tribune combined to make the New York Herald-Tribune on March 19, 1924--62 years later!

Next you see a photograph of an important message which you may wish to solve yourself. It was sent by President Jefferson Davis to General Johnston, on "a very significant date," April 1865. For ease in working on it I give also a transcription, since the photograph is very old and in poor state. I believe that this message does not appear in any of the accounts I've read.

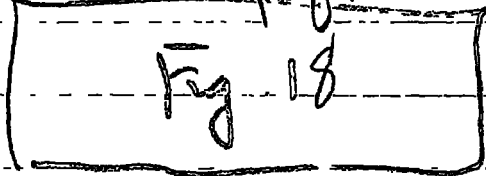


Fig 18

"Send over your lines, from time to time, messages which, if it is in the power of the enemy to decipher them, will lead them to believe that we cannot get any clew to their signals."

"Send also occasionally messages untrue, in reference to imaginary military movements, as for instance, -- "The Sixth Corps is ordered to reinforce Keyes at Yorktown'."

Undoubtedly, what we have here are references to the general cipher

system used by the Confederates in their electric-telegraph communications, for

Note the expression "Send over your lines". This could hardly refer to visual

communications. Here we also have very early instances, in telegraphic

communications, of what we call cover and deception, i.e., employing certain

ruses to try to hide the fact that enemy signals could be read, and to try

to deceive him by sending <sup>spurious</sup> messages for him to read, <sup>hoping the fraud will not</sup> and ~~be~~ <sup>be</sup> detected.

~~be detected.~~

~~spurious messages.~~

*of Union cryptanalytic successes*  
P Brown's account continues [p. 215]:

In October, 1863, Capt. Merrill's party deciphered a code, and in November of the same year Capt. Thickstun and Capt. Marston deciphered another in Virginia.

Lieut. Howgate and Lieut. Flock, in March, 1864, deciphered a code in the Western Army, and at the same time Lieut. Benner found one at Alexandria, Virginia.

Capt. Paul Babcock, Jr., then Chief Signal Officer, Department of the Cumberland, in a letter dated Chattanooga, Tennessee, April 26, 1864, transmitting a copy of the rebel signal code, says:

Capt. Cole and Lieut. Howgate, acting Signal Officers, occupy a station of communication and observation on White Oak Ridge at Ringgold, Ga. . . . On the 22nd inst. the rebels changed their code to the one enclosed, and on the same day the above-mentioned officers by untiring zeal and energy succeeded in translating the new code, and these officers have been ever since reading every message sent over the rebel lines. Many of these messages have furnished valuable information to the general commanding department.

*these were sent all matter on p. 45*

With regard to Confederate reading of Union visual signals, Brown makes ~~Brown continues with~~ the following observations of considerable interest [p. 274]:

The absolute necessity of using a cipher when signalling in the presence of the enemy was demonstrated during these autumn months by the ease with which the rebels read our messages. This led to the issuing of an order that all important messages should be sent in cipher. Among the multitude of messages intercepted by the enemy, the following were some of the more important: -

Brown thereupon cites 25 such messages but he gives no indication whatever as to the source from which he obtained these examples or how he knew they had been intercepted. They all appear to be tactical messages sent by visual signals.

*do not want make double space*

The following is also from Brown (p. 279):

About the first of June (1864), Sergt. Colvin, was stationed at Fort Strong, on Morris Island, with the several codes heretofore

*Union Signal Corps*

*move this up*

The following is also from Brown [p. 279]:  
 About the first of June (1864), Sergt. Colvin was stationed at Fort Strong, on Morris Island, with the several codes heretofore used by the rebels, for the purpose of reading the enemy's signals if possible. For nearly two weeks nothing could be made out of their signals, but by persevering he finally succeeded in learning their codes. Messages were read by him from Beach Inlet, Battery Bee, and Fort Johnson. Gen. J. G. Foster, who had assumed command of the Department of the South, May 26th, was so much pleased with Sergt. Colvin's work, that in a letter addressed to Gen. Halleck, he recommended "that he be rewarded by promotion to Lieutenant in the Signal Corps, or by a brevet or medal of honor." This recommendation was subsequently acted upon, but, through congressional and official wrangling over appointments in the Corps, he was not commissioned until May 13, 1865, his commission dating from Feb. 14, 1865.

(p-281) During the month, Sergt. Colvin added additional laurels to the fame he had earned as a successful interpreter of rebel signals. The enemy had adopted a new cipher for the transmission of important messages; and the labor of deciphering it devolved upon the sergeant. Continued watchfulness at last secured the desired result, and he was again able to translate the important dispatches of the enemy for the benefit of our commandants. The information thus gained was frequently of special value in our operations, and the peculiar ability exhibited by the sergeant led Gen. Foster once more to recommend his promotion.

(p-286) About the same time an expedition under Gen. Potter was organized to act in conjunction with the navy in the vicinity of Bull's Bay. Lieut. Fisher was with this command, and by maintaining communications between the land and naval forces facilitated greatly the conjoined action of the command. Meanwhile every means was employed to intercept rebel messages. Sergt. Colvin, assigned to this particular duty, read all the messages within sight, and when the evacuation of Charleston was determined upon by the enemy, the first notification of the fact came in this way before the retreat had actually commenced. As a reward for conspicuous services rendered in this capacity, Capt. Merrill recommended that the sergeant be allowed a medal, his zeal, energy and labors fully warranting the honor.

After the occupation of Charleston, communications was established by signals with Fort Strong, on Morris Island, Fort Johnson and James Island, Mount Pleasant, and Steymeyer's Mills. A line was also opened with the position occupied by the troops on the south side of the Ashley river.

In many of the cases cited by Brown it is difficult to tell whether wig-wag or electric telegraph messages were involved. But in one case, [evacuation of Charleston] it is perfectly clear that visual messages were involved, when Brown says that Sgt. Colvin "read all the messages within sight."

*Direct*  
~~Once before in this lecture it was mentioned that the visual signalmen of each side were reading the visual signals of the other side. This led to the use, by both sides, of ciphers to protect the signals transmitted by the visual method. But in addition, discovery that Confederate operators were~~

Further with regard to rebel cryptanalytic success with Union messages, Brown has this to say [p. 213]:

The reports of Lieut. Frank Markoe, Signal Officer at Charleston, show that during the siege thousands of messages were sent from one post to another, and from outposts to headquarters, most of which could have been sent in no other way, and many were of great importance to the Confederate authorities.

Lieut. Markoe says that he read nearly every message we sent. He was forewarned of our attack on the 18th of July, 1863. He adds regretfully, however, that through carelessness of the staff officers at headquarters it leaked out that he was reading our messages. Our officers then began to use the cipher disk. In August he intercepted the following message: "Send me a copy of rebel code immediately, if you have one in your possession." He therefore changed his code. ... A little later our officers used a cipher which Lieut. Markoe says he was utterly unable to unravel.

It is unfortunate that neither Lieut. Markoe the Confederate cryptanalyst, nor Brown, the Union

Signalman, tells us what part of cipher this was that couldn't be unravelled. I assume that it was the Myer cipher with a key phrase of some length and with

successive letters, not whole words, being enciphered by successive letters of the key. But this is only an assumption and may be entirely erroneous.

In the foregoing citations of cryptanalytic successes it is significant, <sup>to note, first,</sup> that visual messages were intercepted and read by both sides; <sup>second,</sup> that Confederate telegraphic messages protected by the Vigenere cipher were read by Union personnel whenever such messages were intercepted; and <sup>third,</sup> that USMTC telegraph messages protected by the route cipher<sup>1</sup> were apparently intercepted occasionally but never solved. Later I shall make some comments on this last statement, but at the moment let us note that technically the Vigenere cipher is theoretically much stronger than the route cipher, so that we have here an interesting situation; viz; the users of a technically inferior cryptosystem were able to read enemy messages protected by a technically superior one, but the users of a technically superior cryptosystem were not able to read enemy messages protected by a technically inferior one — a curious situation indeed.



N<sup>o</sup> 6  
1<sup>st</sup> draft

INTRODUCTION TO CRYPTOLOGY-VI

~~Confidential~~

REF ID: A62831  
INTRODUCTION TO CRYPTOLOGY - VI

By William F. Friedman

This lecture, the sixth and last in this series, deals with cryptology in the period from the end of World War I to the end of World War II (unclassified material only). The emphasis in this lecture is upon communications security (COMSEC) because <sup>not only</sup> ~~most of the information given in the~~ <sup>placed very</sup> five preceding lectures the emphasis was largely upon communications intelligence (COMINT) but also because <sup>although not as particular as COMINT,</sup> COMSEC, in the final analysis, is <sup>to national security</sup> really more vital than COMINT.

Insert attached →

X X X X X X

You will perhaps recall that in the very first lecture in this series reference was made to the role that COMINT (or "Magic") played <sup>not only</sup> in the events preceding <sup>Japanese sneak</sup> the attack on Pearl Harbor but <sup>also</sup> in the military, ~~and~~ naval, and air operations which followed that attack. This is not the place nor is there time to go into the complex problems involved in <sup>ascertain the names of the persons and to</sup> an attempt to ~~fix the responsibility upon~~ <sup>the blame for being caught by surprise</sup> them ~~whatever responsibility they may have~~.

Millions of words have been published on this subject and I do not propose to add to that voluminous literature whatever thoughts I may have thereon.

INSERT Type this on legal size paper, original + one carbon triple space. Number 1(a), 2(a), 3(a) etc on this set of pages. [Draw intro-duction for Section 126]

(2)

This, the sixth and final lecture in this series on the history of cryptology will be devoted to a presentation of events and developments of significance or importance in that history from the end of World War I to the end of World War II.

It would be entirely too ambitious a project even to attempt to compress, <sup>within a lecture of only 50 minutes,</sup> all that should or could be told in that segment of our history of cryptology. In a nutshell, however, it can be said that the most significant and important events and developments during that quarter of a century were directly concerned or connected with the advances made in the production of more complex mechanical, electrical and electronic cryptographic apparatus, and with the concomitant advances in the production of more sophisticated mechanical, electrical and electronic apparatus for the solution of the messages produced by these increasingly complex cryptographic machines. These two phases are inter-related because, <sup>a sort of simple analogy,</sup> to ~~use~~ cryptography and cryptanalysis represent the two faces of a single coin.

It would be nice if I could go a

bit into detail in regard to these increasingly complex matters but security considerations prevent my doing so because the classification of these lectures, viz, CONFIDENTIAL, is the lowest one now possible.

As to the advances in the development and use of more sophisticated cryptographic apparatus I will only note at this point a comment which

General Omar Bradley makes in his quiet but <sup>very</sup> interesting book entitled A Soldier's Story.<sup>1</sup>

<sup>indent  
+  
single  
space</sup> Signal Corps officers like to remind us that "although Congress can make a general, it takes communications to make him a commander."

It is immodest for me to try to amend General Bradley's remark but this is how I wish he had worded it:

Signal Corps officers like to remind us that "although Congress can make a general, it takes rapid and secure communications to make him a good commander."

This will in fact be the keynote of this lecture. In other words, communications security, or COMSEC, will be its main theme and the one I wish to emphasize.

<sup>1</sup> New York: Henry Holt and Co., 1951, p. 474.

But before coming to that part of our history perhaps a bit more attention must be devoted to events and developments of cryptanalytic significance or importance during the period 1918 to 1946. By far the most spectacular and interesting of these are the ones which were so fully and disastrously disclosed by the various investigations conducted <sup>by the Army and Navy</sup> very secretly while World War II was still in progress and both secretly and openly after the close of hostilities. The investigations were intended to ascertain why <sup>our Army and Navy forces in Hawaii</sup> we were caught by surprise by the sneak attack on Pearl Harbor by the Japanese on the morning of 7 December 1941. They were also intended to <sup>ascertain and</sup> pin the blame on whoever was responsible for the debacle. I don't think I should even attempt to give you my personal opinion on these complex questions, which were studied by seven different boards within the Services and finally by the Joint Congressional Committee on the Investigation of the Pearl Harbor Attack. I mentioned the latter investigation in my first lecture and now I must add to what I then said. The Committee published its findings

-4-

conclusions and recommendations in 1946. It began its work in September 1945 with secret hearings but on 70 days subsequent to 15 November 1945 up to and including 31 May 1946 open hearings were conducted in the course of which some 15,000 pages of testimony were taken and a total of 183 exhibits received incident to an examination of 43 witnesses. The Committee put out a final Report of 580 pages to accompany a set of 39 volumes of testimony and exhibits. In the Report there was one by the Majority (signed by six Democratic ~~members~~ and two Republican <sup>members</sup>) and one by the Minority (signed by two Republican members). The Minority Report was not nearly as long as that of the Majority but it brought into focus certain troublesome points which still form the subject of acrimonious discussions and writings who believe the attack was "engineered" by President Roosevelt.

For this history the interesting fact is that both the Majority and Minority Reports contain glowing tributes to the role played by COMINT before and during our participation in World War II. In my first lecture I presented a brief extract in this regard taken from the Majority

-5-

Report; but here is what the Minority Report says on the subject:

6. Through the Army and Navy intelligence services extensive information was secured respecting Japanese war plans and designs, by intercepted and decoded Japanese secret messages, which indicated the growing danger of war and increasingly after November 26 the imminence of a Japanese attack.

Indubitable  
&  
single  
phrase

With extraordinary skill, zeal, and watchfulness the intelligence services of the Army Signal Corps and Navy Office of Naval Communications broke Japanese codes and intercepted messages between the Japanese Government and its spies and agents and ambassadors in all parts of the world and supplied the high authorities in Washington reliable secret information respecting Japanese designs, decisions, and operations at home, in the United States, and in other countries.

Although there were delays in the translation of many intercepts, the intelligence services had furnished to those high authorities a large number of Japanese messages which clearly indicated the growing resolve of the Japanese Government on war before December 7, 1941.

P. 514 of Report

P. 5 of NSA Technical Journal (Vol. & date), quoting from p. 232 of the Report of the Majority.



-6-

The Majority Report made five main recommendations, of which the second is of special interest:

That there be a complete integration of Army and Navy intelligence agencies in order to avoid the pitfalls of divided responsibility which experience has made so abundantly apparent; that upon effecting a unified intelligence, officers be selected for intelligence work who possess the background, penchant, and capacity for such work, and that they be maintained in the work for an extended period of time in order that they may become steeped in the ramifications and refinements of their field and employ this reservoir of knowledge in evaluating material received. The assignment of an officer having an aptitude for such work should not impede his progress nor affect his promotions. Efficient intelligence services are just as essential in time of peace as in war, and this branch of our armed services must always be accorded the important role which it deserves.

indent  
to  
single  
space

④ P. 253 of Report of the Majority.

I assume that due note of this <sup>recommendation</sup> has been taken by the services, but how far it has been possible and practicable to <sup>by</sup> to ensure that the recommendation has been carried out we will be I do not know. In this connection I think it only to be of interest to cite what the distinguished commander whom I have already mentioned, General Omar Bradley, has to say on this point. ✓

In their intelligence activities at Allied Forces Headquarters, the British easily outstripped their American colleagues. The tedious years of prewar studies the British had devoted to areas throughout the world gave them a vast advantage which we never overcame. The American army's long neglect of intelligence training was soon reflected by the ineptness of our initial undertakings. For too many years in the preparation of officers for command assignments, we had overlooked the need for specialization in such activities as intelligence. It is unrealistic to assume that every officer has the capacity and the inclination for field command. Many are uniquely qualified for staff intelligence duties and indeed would prefer to devote their careers to those tasks. Yet instead of grooming qualified officers for intelligence assignments,

✓ Op. cit., p. 33.

Indent  
+  
para  
space

Indent  
&  
pencil  
space

we rotated them through conventional duty hours, making correspondingly little use of their special talents. Misfits frequently found themselves assigned to intelligence duties. And in some stations G-2 became a dumping ground for officers ill suited to line command. I recall how scrupulously I avoided the branding that came with an intelligence assignment in my own career. Had it not been for the uniquely qualified reservists who so capably filled so many of our intelligence jobs throughout the war, the army would have found itself badly pressed for competent intelligence personnel.

Have some of you pondered over the reason why an officer who reaches the highest level of command in an army, ours as well as in foreign armies, is called a "general officer" or "General"? It is because he is supposed to have learned something about everything connected with military operations - he is not a specialist. But how much can a general officer know about complexities of such very important areas of <sup>the</sup> military business?

and operations such as are involved in modern engineering, electrical communications, guided missiles, rockets, etc, etc? How much can be learned without first-hand experience in the tricky business of ordinary military intelligence operations let alone the much more complicated business of cryptology as applied in modern military operations?

But let us leave these speculations, interesting as they may be, and continue with our history. Let us first dispose of <sup>certain comments in the</sup> COMINT area of that history.

However, there is one small but extremely significant piece of information involved in this matter and I will say a few words about it. You will recall that in the ~~very~~ first lecture I called to your attention an article which appeared in the 17 December 1945 issue of TIME magazine and which was based upon a letter <sup>the late</sup> General George C. Marshall, then Chief of Staff of the U.S. Army, ~~from~~ ~~to~~ wrote to Governor Thomas E. Dewey, Republican candidate for President in the 1944 election campaign. <sup>which was written on 27 Sept 1944</sup> In that letter General Marshall practically begged Governor Dewey to say nothing during the campaign about a certain <sup>very vital</sup> piece of information which General Marshall had reason to believe had <sup>become</sup> known to ~~have~~ <sup>been</sup> Governor Dewey by persons not authorized to disclose it. The <sup>information</sup> dealt with the fact that the U.S. had <sup>been</sup> reading Japanese codes and ciphers even before the attack on Pearl Harbor. The vital point which General Marshall wanted to convey to Governor Dewey was that not only was ~~that~~ <sup>the</sup> piece of information which had surreptitiously ~~been~~ <sup>been</sup> given to Governor Dewey true

but more important were the facts that (1) the war was still in progress; (2) the Japanese were still using certain of the pre-Pearl Harbor cryptosystems, and (3) the U.S. was still reading <sup>the secret communications in</sup> these systems as well as certain other enemy communications. Therefore, it was vital that Governor Dewey not use the information which had come into his possession as to our reading Japanese <sup>secret</sup> communications prior to the attack on Pearl Harbor. I said in that first lecture that I might later give further extracts from TIME's account and, ~~here they are!~~ continuing the extracts printed on pages 3, 4, and 5 of the first lecture, here they are:

Copy material  
marked on accompanying photos in red

The Marshall-Dewey correspondence is so important in cryptologic history that I feel that the whole of it should be included, <sup>even</sup> in this brief history. When the letter was written it was,

- 3a -

not only on the very day that General Marshall had to place  
 it in evidence - the letter caused a great sensation in the  
 news papers - but also

~~but more importantly, the war was still in progress~~  
~~the Japanese were still negotiating the peace treaty with the U.S.~~  
~~and the U.S. was still pined by the internal~~  
~~other enemy communications. Therefore, it was vital~~  
~~that Governor Dewey not see the information~~  
~~had come into his possession, to our reading of~~  
~~some communications prior to the attack on Pearl~~  
 The letter is so important in cryptologic history  
 that I feel the whole of it should be brought  
 to your attention. When it was written it was,  
 of course, TOP SECRET and it was only under  
 great pressure by certain members of the Joint  
 Congressional Committee on the Investigation of  
 the Attack on Pearl Harbor, <sup>that General Marshall</sup> revealed the contents  
 of the letter. Thus the letter came into the public  
 domain when the <sup>40 volumes of the</sup> Hearings of that Committee were  
 published, by authority of the Committee, <sup>and</sup> put on  
 sale by the Superintendent of Documents of the  
 Government Printing Office. The <sup>disclosure of the contents of the</sup> Marshall-Dewey  
 were indeed such a sensation that LIFE magazine  
 printed the whole of it in its issue of 17 December,  
 1945, with the following introduction:

copy from LIFE-P19-21

So far as I am aware it has <sup>never been accepted (if known)</sup> ~~not~~ been disclosed, who gave  
 Governor Dewey the information. But it is a fact that ~~the~~  
 Dewey as a patriotic citizen, <sup>deeded to General Marshall's request</sup> ~~deeded~~ <sup>to</sup> General Marshall's request <sup>the</sup> ~~the~~  
- Re  
 Court

whatever made no use of the <sup>initial</sup> secret information during the campaign, no after it, so far as I am aware. TIME'S account specifically states that Dewey "held his tongue. The War Department's most valuable secret was kept out of the campaign."



Except for a change in the first <sup>two</sup> and last paragraphs this letter is identical with the first letter. The ~~change~~

At the end of the ~~second letter~~ <sup>the second letter as printed in parentheses and</sup> "LIFE" there appears in italics <sup>and the following:</sup>

(The second letter then repeated substantially the text of the first letter except for the first two paragraphs.)

LIFE failed to note that <sup>the last</sup> two sentences in the penultimate paragraph of the "First Letter" were omitted from that paragraph in the "Second letter," but there is no explanation for the omission. Perhaps it was simply for the sake of brevity, but this seems improbable.

~~There is no explanation for this omission: perhaps it was simply for the sake of brevity.~~

In my first lecture (p. 4 of NSA Technical Journal No. 7, date?) I called attention to the fact that the account given in the TIME article gives credit to the Army cryptanalysts for providing the secret communications "Intelligence" which enabled the US Navy to win such spectacular battles as those of the Coral Sea and Midway and to waylay Japanese convoys, whereas the credit

for the communications intelligence which enabled our  
 Navy to win these battles was produced by Navy  
 cryptanalysts. One cannot blame <sup>the editors of</sup> TIME for making  
 such a bad error because <sup>the source of the error was</sup> the letter which General  
 Marshall's <sup>brother</sup> wrote <sup>several years</sup> ago I asked  
<sup>my friend</sup> Col. Clarke, who <sup>had covered</sup> General Marshall's letter to  
 Governor Dewey and who was at the time a high  
 level officer in G-2 <sup>how such an error had crept into</sup>  
 General Marshall's letter, and <sup>it was</sup> told that the letter which  
<sup>was</sup> prepared for General Marshall's signature did  
 not meet with the General's whole-hearted approval  
 and that the General himself had modified it. Per-  
 haps that is how the error to which I have  
 referred crept into the letter. One could hardly  
 expect General Marshall to be entirely familiar with  
 the technical cryptanalytic details <sup>in what he wanted to tell Governor Dewey;</sup> involved <sup>and</sup> ~~not~~  
<sup>not</sup> ~~should~~ one. <sup>Surprised</sup> for not being able <sup>to bear it</sup> <sup>in his very busy days and under very heavy</sup>  
<sup>to bear it</sup> <sup>in his very busy days and under very heavy</sup>  
 pressure of events, the differences between the enemy  
 systems worked up by the <sup>respective and separate</sup> Army and ~~the~~ Navy  
 cryptanalytic organizations. <sup>[Insert over]</sup>  
 Since the <sup>period during which the disclosures</sup> disclosures <sup>were made,</sup> were made, disclosures which were  
 Congressional Investigation, so far as concerns <sup>the</sup> ~~the~~  
 the <sup>important accomplishments of</sup> two services <sup>accomplished</sup> before and after the

Insert

It is, of course, possible, indeed it may be probable, that certain  
EXMINT regarding the Battles of the Coral Sea and  
of Midway, as well as other important naval operations  
came from messages read by Army  
cryptanalysts, and this is what confused General  
Marshall.

Pearl Harbor attack, in the field of communications intelligence, much has been written and is now in the public domain regarding those accomplishments, but, <sup>fortunately</sup> no technical details of significance have been disclosed. Hints here and there are in abundance in the many books and articles that have been published by U.S. writers since the end of World War II; but more than hints of the great <sup>part played by</sup> COMINT ~~was~~ in U.S. military and naval successes are to be found in books and articles published by <sup>American officers as well as by</sup> officers of the beaten Japanese, and German, and Italian armed forces. Time does not permit ~~any~~ <sup>in this lecture</sup> citing ~~any~~ <sup>of these</sup> hints or definite statements, but the following <sup>two</sup> are of particular interest because they concern the ~~the~~ Battle of Midway, which is considered the one which turned the war in the Pacific from <sup>a possible Japanese</sup> victory to one of ignominious defeat:

identify  
single space  
what is written  
over

see over

It is the ~~first~~ <sup>above</sup> extract which is of special interest to us at the moment, and, in particular, the portion which refers to "the negatively bad and ineffective functioning of Japanese intelligence." The Japanese author is a bit too severe on the Japanese intelligence organization. I say

Enemy's intelligence on this occasion was the negatively bad and ineffective functioning of Japanese intelligence.

failure on our part - a failure to take adequate precautions for guarding the secrecy of our plans. Had the secret of our intent to invade Midway been concealed with the same thoroughness as the plan to attack Pearl Harbor, the outcome of this battle might well have been different. But it was a victory of American intelligence in a much broader sense than just this. Equally as important as the positive achievements of the

If Admiral Yamamoto and his staff were vaguely disturbed by the persistent bad weather and by lack of information concerning the movements of the enemy, they would have been truly dismayed had they known the actual enemy situation. Post-war American accounts make it clear that the United States Pacific Fleet knew of the Japanese plan to invade Midway even before our forces had sortied from home waters. As a result of some amazing achievements by American intelligence, the enemy had succeeded in breaking the principal code then in use by the Japanese Navy. In this way the enemy was able to learn of our intentions almost as quickly as we had determined them ourselves.

The distinguished American naval historian, Professor Samuel E. Morison, characterizes the victory of United States forces at Midway as "a victory of intelligence." In this judgment the author fully concurs, for it is beyond the slightest possibility of doubt that the advance discovery of the Japanese plan to attack was the foremost single and immediate cause of Japan's defeat. Viewed from the Japanese side, this success of the enemy's intelligence translates itself into an

Midway, the battle that doomed Japan: The Japanese Navy's Story by Mitsuo Fuchida and Matasake Okumura, 1955, pp. 131 and 232.

this because their cryptanalysts were up against much more sophisticated cryptosystems than they <sup>knew or</sup> were qualified to solve. In fact, even if they had been extremely adept in cryptanalysis it would have been of no avail — U.S. high-level communications were protected by cryptosystems of very great security.

This brings us to a <sup>phase of cryptology</sup> subject which is of highest importance — the phase which deals with communications security, or COMSEC, and I shall confine myself largely to its historical background in the U.S. Armed Forces. The background is a very broad one because it should include the background of the developments of each of the three components of COMSEC: cryptosecurity, transmission security, and physical security of cryptomaterials. But since time is limited and because I think you would be more interested in the phases pertaining to cryptosecurity, I will omit references to the history of the other two components. And even in limiting the data to cryptosecurity I will have opportunity only to give some of the highlights of the development of the items that comprise our cryptomaterials, <sup>omitting</sup> leaving out comments on the history of the development and im-

provement of our techniques, procedures and practices, all of which are extremely important.

→ More this down to p. 14 of this nos.

Coming directly <sup>now</sup> to the history of the development of our cryptomaterials themselves, I hardly need reiterate what was pointed out in previous lectures as to the profound effect of the <sup>advances in the science and art of</sup> electrical communications in the ~~19th~~ <sup>19th and 20th</sup> Century. These advances had a direct effect upon military communications and an indirect effect upon military cryptology. Hand-operated ciphers and of course, codebooks became almost obsolete with the need for greater and greater speed of cryptographic operations to match as much as possible the very great increase in the speed of communications brought about by inventions and improvements in electric telegraphy. The need for cryptographic apparatus and machines became quite obvious.

I shall begin the story with a definition which you will find in any good English dictionary, a definition of the word "accident." You will get the point of what may seem to you <sup>right now</sup> to be merely another of my frequent digressions from the main theme, but if it be a digression I think you will

nevertheless find it of interest. The word "accident" in Webster's Unabridged Dictionary is defined as follows:

1. Literally, a befalling.

a. An event that takes place without one's foresight or expectation; an undesigned, sudden, and unexpected event.

b. Hence, often, an undesigned and unforeseen occurrence of an afflictive or unfortunate character; a mishap resulting in injury to a person or damage to a thing; a casualty; as, to die by an accident.

There are further definitions of the word but what I've given is sufficient for our purposes. But why define the word; what has it to do with COMSEC?

During our participation in World War II the President of the United States, accompanied by many of his highest-level assistants, journeyed several times half-way around the world. He journeyed in safety — he met with no accident.

On the other hand, <sup>in April 1943</sup> Admiral Isoroku Yamamoto, <sup>Commander-in-Chief of the Japanese Navy</sup> started out on <sup>what was</sup> ~~be~~ just an ordinary ~~unplanned~~ <sup>planned</sup> trip ~~but~~ it turned out to be a ~~one-way~~ <sup>one-way</sup> trip ~~intended~~ <sup>intended</sup> to ~~take~~ <sup>take</sup> for the ~~admiral~~ <sup>admiral</sup>. His death was ~~announced~~ <sup>announced</sup> in an ~~official~~ <sup>official</sup> Japanese Navy ~~bulletin~~ <sup>bulletin</sup> ~~stating~~ <sup>stating</sup> that ~~then~~ <sup>then</sup> Admiral



had met a glorious <sup>REF ID: A02031</sup> ~~and while~~ directing operations  
in a naval engagement against ~~a~~ superior enemy  
forces. But we know that this was simply not true;  
Admiral Yamamoto "met with an accident." But  
some bright person, it was the late Jimmy Walker,  
when mayor of New York City, I think, who said  
that "accidents don't just happen — they are  
brought about." No; Admiral Yamamoto did not  
die simply by accident: he died because our Navy  
~~in detail~~ the schedule of his trip down to the  
last detail so that it was possible to set up an  
ambush with high degree of possible success. Here

Here is the story<sup>3</sup> as told in an interesting manner by Fleet Admiral William F. Halsey, US N.

I returned to Nouméa in time to sit in on an operation that was smaller but extremely gratifying. The Navy's code experts had hit a jack pot; they had discovered that Admiral Isoroku Yamamoto, the Commander in Chief of the Imperial Japanese Navy, was about to visit the Solomons. In fact, he was due to arrive at Ballale Island, just south of Bougainville, precisely at 0945 on April 18. Yamamoto, who had conceived and proposed the Pearl Harbor attack, had also been widely quoted as saying that he was "looking forward to dictating peace in the White House at Washington." I believe that this statement was subsequently proved a canard, but we accepted its authenticity then, and it was an additional reason for his being No. 3 on my private list of public enemies, closely trailing Hirohito and Tojo.

Eighteen P-38's of the Army's 339th Fighter Squadron, based at Henderson Field, were

13/ Admiral Halsey's Story, Mc Graw-Hill, New York, 1947, pp. 155-157.

assigned to make the interception over Buin, 35 miles short of Ballale. Yamamoto's plane, a Betty, accompanied by another Betty and covered by six Zekes, bore in sight exactly on schedule, and Lt. Col. Thomas G. Lamphier, Jr., dove on it and shot it down in flames. The other Betty was also shot down for good measure, plus one of the Zekes. ... We bottled up the story, of course. One obvious reason was that we didn't want the Japs to know that we had broken their code. ... Unfortunately, somebody took the story to Australia, whence it leaked into the papers, and no doubt eventually into Japan. ... But the Japs evidently did not realize the implication any more than did the tattletale; we continued to break their codes. ...

single  
space  
indent

Admiral Halsey's Story contains a good many more instances of <sup>cryptologic significance</sup> ~~of~~ <sup>of</sup> ~~interest to his~~ <sup>of</sup> ~~part of the Japanese~~ <sup>as well as</sup> ~~an excellent example~~ <sup>Other authors, both American and Japanese, <sup>cite</sup> similar instances.</sup> One Japanese author states <sup>in</sup> categorical language that Japan was defeated because of poor COMSEC on the part

of the Japanese Navy and good COMINT on the part of the American Navy.

But lest you get the impression that enemy intelligence agencies had no success at all with ~~the~~ secret communications of U.S. Armed Forces, let me tell you that they did have some success and in certain instances, very significant success. There is not time to go into this <sup>rather</sup> disappointing <sup>dissuasive</sup> statement but I can say that as a general rule the successes were attributable ~~not~~ to technical weaknesses in U.S. cryptosystems but to improper use, in the case, by unskilled, or <sup>or</sup> <sup>improperly</sup> insufficiently trained cryptographic clerks. I may as well tell you right now that this has been true for a great many years.

~~formation obtainable by procedures not the direct result of cryptosystems but by means and procedures connected with what we call matter of fact, because as long ago as the year 1605 who wrote the first treatise on English on the subject of cryptology, Francis Bacon, said, in The Advancement of Learning,~~

This Arte of Cyphering, hath for Relative, an

valiant +  
single  
space

Art of Discyphering; by supposition unprofitable; but, as things are, of great use. For suppose that Cyphers were well managed, there bee

indent  
+  
single  
space

Multitudes of them which exclude the Diagrams.  
But in regards of the Reasons and unskillful-  
ness of the hands, through which they  
pass, the greatest Matters, are many  
times carried in the weakest Cyphers.

When electrical and particularly radio  
transmission entered into the picture additional  
hazards to communications security had to be  
taken into account, but many commanders have  
failed to realize how much intelligence can be  
gained <sup>merely</sup> from a study of the procedures used in  
transmission, the direction and flow of com-  
munications, the call signs of the transmitting  
and receiving stations, ~~direction~~ etc., all  
without solving the ~~cryptic~~ communications even  
if they are in cryptic form. Following are a couple  
of extracts from a document entitled German Oper-  
ational Intelligence, published in April 1946 by  
the German Military Document Section, a Combined  
British, Canadian, and U.S. Staff:

indent  
single  
space

(P. 8) "Signal intelligence [etc.] as per cards  
attached. ..."

(P. 8) "Most of their signal intercept success etc."

(P. 22) "Importance of Signal Intelligence  
during the Normandy Invasion; During the  
invasion etc

indent  
&  
single  
space

A great many examples of intercepted messages of tactical content are cited in the above-mentioned document, which is replete with information of deep interest although the document was originally issued ~~as~~ with the lowest security classification then in use (U.S. "Restricted"; "British-Canadian" "For official use only.") I wish there were time to quote at greater length from this useful brochure.

Here insert matter  
on p. 8 of this  
ms.

Continuation of Lecture No. 5 by [Name] 1944 [Notes]

Here's a photo of Alberti's disk (Fig. 6) but I won't make the time to explain it, except to say that the digits 1, 2, 3, 4 were used to designate the four quadrants. Note the letters and that the letters of the cipher or revolving alphabet were in mixed order.

Until the advent of electronic cipher machines most cryptographic apparatus and devices were built upon or around circular rotating members or cipher wheels, cipher disks, etc. The very earliest such disks appears in a treatise by an Italian cryptologist named Alberti whose Treatise in cipher was written in Rome about 1470. It is the oldest tract on cryptography the world has possessed. In Porta's book, first published in 1563 in Naples, there appear several cipher disks and in the copy which I was given me as a gift by

Colonel Fabryan they are in working condition. Here is a picture of one of them. In this version the devices used symbols as cipher characters. And apparently nobody thought up anything much better for a long, long time. It seems that I did nobody think up any improvements on the original Porta disk, but those who did any thinking on the subject merely "invented" or "re-invented" the thing, and that happened, time and again, repeatedly in successive generations. For instance, in

Lecture No. 4 of this series if you were shown a picture of the "cipher disk" invented by Major Albert Mysar, the first Chief Signal Officer of the U.S. Army, who obtained a patent on his invention in 1865. We all know that it generally takes a pretty long time to get a patent through the complex workshops of the U.S. Patent Office, but in 1924 the ancient device

(45.5) The Cipher Disk used by the U.S. Army in 1865. It is a variation of the original Porta disk. (45.6) Here is a picture of the original Porta disk.

Invent to P15

REF ID: A62831

Here's a picture of ~~the~~ <sup>of it (Fig. 9).</sup> ~~the~~ <sup>the</sup> ~~original~~ <sup>original</sup> disk (Fig. 8) and the explanation,  
 And you will remember that ~~the~~ <sup>one</sup> of the Signal Officers  
 of the Confederate Signal Corps mechanized the <sup>old</sup> Vigenere  
 squares and put it out in the form of a cylinder  
 (see Figs. 13, 14 and 15) of Lecture No. IV. The cipher  
 disk used by the Signal Corps of the U.S. Army  
 during ~~the~~ <sup>the</sup> ~~period~~ <sup>period</sup> 1910 to 1920, that is, during the  
 period <sup>including</sup> World War I ~~(Fig. 16)~~ <sup>it</sup> was nothing but a  
 white <sup>Alberti's</sup> celluloid variation of the original <sup>disk</sup> of the  
 vintage of 1470, except that it was even simpler than  
 its progenitor because in the latter the cipher alphabets  
 produced were mixed alphabets whereas in the  
 Signal Corps disk the cipher alphabets are <sup>simple</sup> ~~the~~ reversed  
 standard sequences.



was patented <sup>by</sup> S.H. Huntington. Here you can see a great improvement over the Signal Corps version — a blank is added to both sequences so that the space between words could be enciphered. This, as you have learned, is a fatal weakness if seen in the cipher text, in the Huntington device the spaces between words would be enciphered but the cipher text would have space signs, although they would not correspond to the actual spaces <sup>between words</sup> in the plain text. ☺

It is interesting to note that <sup>in Austria, in 1936,</sup> during the days when the German National Socialists were banned as an organization, <sup>the Nazis</sup> Hitler and his cohorts used this variation of the old disk — it had the 10 digits on both the outer and the inner sequences <sup>for enciphering digits</sup> (Fig. 12).

The first significant improvement on the old cipher disk was that made by Sir Charles Wheatstone, who <sup>some time before 1837</sup> invented and <sup>described</sup> a cipher device which he called a cryptograph. <sup>He described it in a volume</sup> entitled The Scientific Papers of Sir Charles Wheatstone, published by the Physical Society of London. Here is a picture of <sup>which is in my private collection</sup> Wheatstone's device (Fig. 13). What Sir

Charles did was to make the outer circle of letters (for the plain text) comprise the 26 letters of the alphabet plus one additional character to represent "space". The inner circle, for cipher equivalents, contained only the 26 letters of the alphabet and these could be disarranged in a mixed sequence. Two hands, like the hour and minute hands of a clock, were provided, under control of a differential gear mechanism, so that as the <sup>or "minute"</sup> long hand is advanced to make a complete circuit of the <sup>letters on the outer circle of letters on the</sup> face of the cryptograph ~~rotates~~ the short or "hour" hand advances one space or segment of ~~the letters on~~ the inner circle of letters on the face of the cryptograph. In Fig. 13, for example, the plain-text letter G is represented by the cipher letter A. If the long hand is now advanced <sup>in a</sup> clockwise direction for one revolution, G<sub>p</sub> will be represented no longer by A, but by G. In encipherment the long hand is ~~plac~~ always moved in the same direction (clockwise, for example) and is placed over the successive letters of the plain-text message, the cipher equivalents being recorded by hand to correspond with the letters to which the short hand point at each encipherment.

In this way, successive identical letters of the plain text will be represented by different <sup>and varying</sup> letters in the cipher text, depending upon how many revolutions of the long hand intervene between the first and subsequent appearances of the same plain-text letter. Correspondents must naturally agree upon the mixed alphabet used in the inner circle, and the <sup>initial</sup> starting position of ~~each~~ of the two hands at the beginning of the encipherment of a message. In decipherment the operator <sup>moves the long hand counter-clockwise,</sup> passing the cipher letters in the inner circle, and noting the plain-text letters to which the long hand points in the outer circle.

During World War I, some time in 1917, the British Army resuscitated Wheatstone's cryptograph and improved it both mechanically and cryptographically. ~~As to~~ Here is a picture of the device (Fig. 14), in which it will be seen that there are now ~~now~~ longer the "minute and hour" hands but a single hand with an opening <sup>or window</sup> that ~~can~~ <sup>simultaneously</sup> discloses both the plain-text and cipher letters. ~~The~~ ~~the same~~ ~~is~~ ~~just~~ ~~as~~ ~~before~~. The inner circle <sup>of segments</sup> is just <sup>as</sup> posed in an eccentric manner against the outer circle of segments,

which  
 the ~~requirements~~ are made of a substance <sup>upon</sup> which letters may  
 be written in pencil or in ink. In this <sup>an improvement on the original</sup> Wheatstone device  
<sup>both sequences</sup> of letters are now mixed sequences. Making the  
 outer circle also a mixed sequence, <sup>added a</sup> considerable  
 degree of security to the cipher. When it was proposed  
 that all the Allied armies use this device for  
 field cryptocommunications and its security had  
 been approved by British, French, and American  
 cryptologists (both at G.H.Q.-A.E.F. and at Washington)  
 an opportunity to agree or disagree with the  
~~for~~ assessment of these cryptologists was given  
 me while <sup>I was still at the Riverbank laboratories.</sup> I was able to show that the modified  
 Wheatstone cryptograph was still insufficiently  
 secure for <sup>military</sup> ~~serious~~ purposes and the devices, thousands  
 of which had been <sup>manufactured and</sup> issued, were withdrawn. If  
 you are interested in the method of <sup>I used</sup> solution you  
 will find it in Riverbank Publication No. 20, <sup>entitled</sup>  
Several Machine Ciphers and Methods for Their  
1918. Solution. A better method of solution was devised by me <sup>later.</sup> some years <sup>later.</sup>  
 Many years later, and almost by sheer  
 good fortune, I learned that a cipher machine was  
 in the museum of a <sup>certain</sup> small town in <sup>named Stamford.</sup> Connecticut. I  
 was interested and wrote to the curator of the

1879  
1879  
62

museum, requesting that he lend the device for a  
 short period to me as principal cryptanalyst of  
 the War Department. Imagine my astonishment  
 and pleasure when I unpacked the box sent  
 me, and found a device, beautifully made and  
 encased in a fine mahogany case, with its  
 inventor's name, <sup>Darius Wadsworth,</sup> and the date, <sup>1817,</sup> engraved on the face  
 of the machine, which was nothing but another  
 version of the Wheatstone Cryptograph. <sup>(Here's a picture of it (Fig. 15). I believe</sup>  
<sup>the model was made by Eli Whitney. Most significantly</sup>  
 it was ~~more~~ similar to the British modification  
 except that the outer sequence had 33 characters,  
 the inner 26, so that the differential gear instead  
 of operating on the ratio 27 to 26 was now on the  
 ratio 33 to 26. ~~I forget~~ Thus, Darius Wadsworth,  
 an American Army Colonel, <sup>our</sup> first Chief of  
 Ordnance, and an associate of Eli Whitney, had  
 anticipated Sir Charles Wheatstone by over 60  
 years in this invention. He also anticipated the  
 British, <sup>by a whole century</sup> in their modification of Wheatstone's original,  
 because in the Wadsworth device, <sup>there was only one alphabet</sup> both alphabets  
 could be made mixed sequences. This is, <sup>very clearly</sup> shown  
 in Fig. 16 as regards the outer sequence and I believe  
 the inner one could also be disarranged but I  
 am now not sure as to this point. I returned the device

a good many years ago and it is now on display in the Eli Whitney Room of the New Haven Historical Society's Museum.

The next device I ~~wish to~~ <sup>a device</sup> bring to your attention is shown in Fig. 17, <sup>invented</sup> ~~by~~ <sup>by a</sup> French Army reservist, Commandant Bageries, who <sup>for some 10 years</sup> tried to get the French Army to adopt it. He was not successful and included a description of his <sup>which he called his "cryptographe cylindrique,</sup> device in a book published in 1901 in Paris.<sup>15</sup> He had, however, described his device in <sup>an</sup> ~~his~~ article entitled "Cryptographe à 20 rondelles - alphabets (25 lettres par alphabet," published in 1891.<sup>16</sup> In this device there is a central shaft on which can be mounted 20 <sup>numbered</sup> disks on the periphery of ~~each~~ <sup>of which are</sup> <sup>differently</sup> mixed alphabets of 25 letters each. The disks are assembled on the shaft in some prearranged or key sequence. The first 20 letters of the plain text of a message are aligned, as seen in Fig. 17 (JE SUIS INDECHIFFRABLE = "I am indecipherable") and as cipher text one may select any one of the other 24 <sup>which are recorded</sup> lines of letters, then the next set of 20 plain-text letters is aligned, etc. To decipher a

<sup>15</sup> Les chiffres secrets dévoilés.

<sup>16</sup> Comptes Rendus, Marseille, Vol. XX, pp. 160-165.

indication that the letters on the outer sequence are ~~not~~ -  
changeable, so that if Fig. 16 seems to ~~indicate~~ that  
those on the inner sequence are not, this may be an  
illusion.

message, one takes the first 20 cipher letters, aligns them on the device (the disks having been assembled on the shaft in accordance with the prearranged or key sequence) and then one turns the whole cylinder searching for a ~~line of plain~~ row of letters which form intelligible text. There will be only one such row, and the ~~letters~~ <sup>plaintext letters</sup> are recorded. Then the next 20 letters of cipher are aligned, etc.

In 1893 another French cryptologist, the Marquis de Vigaris, showed how messages prepared by means of the Bageries cylindrical cipher could be solved. <sup>✓</sup> Maybe that is why Bageries wasn't too successful in his attempts to get the French Army to adopt his device. But in the U.S. there were apparently none who encountered either what Bageries or de Vigaris wrote on the subject. Capt. Parker Hitt, U.S. Army, <sup>whom I have mentioned in a previous lecture,</sup> in 1915 invented a device based upon the Bageries principle but not in the form of disks mounted upon a central shaft. Instead of disks, Hitt's device used sliding strips and here is a picture of his <sup>very</sup> first model which he presented to me some time in 1923 or 1924 (Fig. 18). But I learned about his

<sup>✓</sup> L'Art de chiffrer et de déchiffrer les dépêches secrètes.  
Paris, 1893, p. 100



while still at Riverbank,

<sup>Sometimes</sup> device, in 1917, and solved one challenge message put up by Mrs. Hitt, <sup>a Riverbank guest for a day.</sup> I didn't <sup>use anything like what I could</sup> <sup>might have learned from de Vries</sup> in accomplishing the solution (which brought a box of chocolates to Mrs. Friedman) because at that time I hadn't <sup>yet</sup> come across the de Vries book. I solved the message by guessing the key Mrs. Hitt employed to arrange her strip alphabets. She wasn't wise to the quirks of inexperienced cryptographic clerks; she used RIVERBANK LABORATORIES as the key, just as I ~~the~~ suspected she would. The device she brought with her was an improved model: the alphabets were <sup>on paper strips</sup> ~~mounted~~ glued to strips of wood, as seen in Fig. 19.

Capt. Hitt brought his device to the attention of the then Major Mauborgne, whom I have also mentioned in a previous lecture and who was then on duty in the Office of the Chief Signal Officer in Washington. There is some question as to whether it was Hitt who brought his device to Mauborgne's attention; Mauborgne later told me that he had independently conceived the invention and, moreover, had made a model using ~~the~~ disks instead of strips. I have that model, a present from General

Mauborgne many years later. It is made of brass, very heavy, on the peripheries of the disks of which he had engraved the letters of his own specially-devised alphabets. In 1919, after my return to Riverbank from my service in the AEF, Mauborgne sent Riverbank <sup>the first 25 letters of</sup> a set of some 25 or more ~~beginnings~~ beginnings of messages enciphered by his device and alphabets. He also sent the same data to Major Yardley, in G-2. Nobody ever solved the messages, even after a good deal of work and even after Mauborgne told us <sup>that</sup> two consecutive words in one of the ~~test~~ challenge messages were the words "are you." Many years later I found ~~out~~ the reason for our complete lack of success, when I came across the plain texts of those messages in a dusty old file in the OC SigO. Here is a picture of the beginnings of the first six messages (Fig. 20). Mauborgne, when I chided him on the unfairness of his challenge messages, told me that he had not prepared them himself — he had an underling (Major Fowler was his name, I still remembered it!) prepare them. In our struggles to solve the challenge messages, <sup>had</sup> assumed that they would contain the usual sorts of words found at

the initial words of military messages. It was the complete failure by Riverbank and G-2 to solve the challenge messages that induced Mauborgne to go ahead with the development of his device. It culminated in what became known as Cipher Device Type M-94. Here is a picture of it (Fig. 21). That device was <sup>standardized and</sup> used for at least 10 years in the Army and Navy.

In 1922, a war-time colleague, the late Capt. John M. Manly (Prof. and Head of the Department of English at the University of Chicago) brought to my attention a photostat of a holographic manuscript in the collection of Jefferson Papers in the Library of Congress. It consisted of two pages, <sup>entitled "The Wheel Cypher"</sup> and here is a picture of the second page (Fig. 22) showing Jefferson's <sup>affordably</sup> basis for calculating the number of permutations <sup>of</sup> this set of 36 wheels of his device. He didn't attempt to make the multiplication; he didn't have <sup>an</sup> <sup>electronic</sup> digital computer — for the total number is astronomical in size. Jefferson anticipated Babbage by over a century.

It soon became apparent to both the Army and the Navy cryptologists that a great increase in crypto-security would be obtained if the alphabets

of the M-94 device could be made variable instead of being fixed. There began <sup>in both services</sup> efforts to develop a practical instrument based upon this principle. I won't take time to show <sup>all</sup> these developments but will show the final form of the Army Strip Cipher Device Type M-138-A (Fig. 23). This form used ~~an~~ <sup>an</sup> aluminium base into which channels were cut ~~to~~ to hold paper cardboard strips of alphabets which could be slid easily within the channels. It may of interest to you to learn that after I had given up in my attempts to find a firm which would or could make such a grooved device in quantity, Mrs. Friedman succeeded — on behalf of her own group in the U.S. Coast Guard. The aluminium Strip Cipher Device Type M-138-A was used from 1935 to 1940 or 1942 by the Army, <sup>the Navy,</sup> the Coast Guard, and the State Department. It was used as a back-up system even after the two services as well as the Department of State began <sup>employing</sup> ~~had jointly developed~~ an electrical cipher machines of high speed and security.

Thus far we have been dealing with cipher devices of the so-called "hand-operated" type. None of them <sup>can really</sup> be considered as being "machines", that is, apparatus <sup>of</sup> employing mechanically-driven <sup>mechanisms</sup> ~~mechanisms~~.

alphabetic sequences can be mounted so that a constantly-changing series of cipher alphabets are produced. We come now to a type of apparatus which can be called a machine, such as the one shown in Fig. 24, ~~It is~~ <sup>called</sup> the KRYHA, ~~after~~ the name of its German inventor, who unfortunately committed suicide a few years ago, perhaps because he failed to make a success of his invention. The Kryha has a fixed <sup>semi-circle of</sup> ~~letters~~ <sup>segments</sup> against which is juxtaposed a rotatable <sup>circle of letters.</sup> ~~sequence~~ Both sequences of letters can be made mixed alphabets (the segments are removable and interchangeable on each sequence). The <sup>large</sup> handle at the right serves to wind a rather powerful <sup>coiled</sup> steel spring which drives the rotating member on which the letters of the inner circle are mounted. In Fig. 25 ~~shown~~ can be seen something of the inner work mechanism. The large wheel at the right ~~is seen~~ <sup>has</sup> ~~apertures~~ <sup>segments</sup> some of which are open or closed, depending upon the "setting" of key. This wheel controls the angular displacement or "stepping" of the circular rotating platform upon which the <sup>letters of the</sup> ~~cipher~~

~~As shown in~~  
 Negatives are mounted. ~~A prearranged~~ <sup>The</sup> initial just-  
 position of the ~~two~~ <sup>inner or movable</sup> alphabets <sup>against the outer or fixed one,</sup> as well as the  
 composition of these alphabets is governed by  
 some key or ~~prearranged~~ <sup>by other</sup> prearrangement.  
~~Upon enciphering (and recording) the equivalent of the~~  
 The cipher equivalents must be recorded by hand.  
 After each encipherment, the button you saw  
 in the center of the panel in the preceding  
 Fig. 24 is pushed down, the inner wheel <sup>advances</sup>  
~~step one or more~~ <sup>1, 2, 3, 4... up to 7</sup> steps, <sup>depending on the key,</sup> and the next letter is  
 enciphered, etc. The pictures I've shown you  
 apply to the latest model of the Kryha; as  
 regards the first model, which came on the  
 market sometime in the 1920's, a German  
 mathematician produced an impressive brochure  
 showing how many different permutations and  
 combinations the machine afforded. Here's a  
 picture of a couple of pages of his dissertation  
 (Fig. 26) but even in those days, <sup>professional</sup> cryptanalysts  
 were not too impressed by calculations of this  
 sort. With modern electronic computers, <sup>such</sup> calcula-  
 tions have become <sup>of even less</sup> significance.

Let us <sup>now</sup> proceed with some more

Complex and more secure machines. In this next slide (Fig. 27) you see a <sup>machine which represents a</sup> rather marked improvement by a Swedish cryptographic firm <sup>upon the ones shown thus far.</sup> It is mechanical - electrical, <sup>machine designated as Cryptophone B-11. Here for the first time you see a cryptographic machine provided with a</sup> in character and <sup>keyboard similar to that on an ordinary typewriter.</sup> <sup>Depressing a key on this keyboard causes a lamp to light under one of the letters on the indicating bank above the keyboard. At the top of this machine can be seen four wheels, in front of two rear wheels. The <sup>four front wheels</sup> are the rotating elements which <sup>drive the two rear wheels. The latter are electrical commutators that to change the circuits</sup> serve as connection-changers <sup>between the keys of the keyboard and the lamps of the indicating board. There isn't time to show you the internal works of this machine, but I must show you <sup>the improvement of such</sup> the next step in cryptographic machines, which <sup>made it possible</sup> to eliminate the tedious job of recording, by hand on paper, the results of encipherment & decipherment. <sup>this was done by means of</sup> by a printing mechanism which was associated with the cryptographic machine.</sup></sup>

Here is a slide (Fig. 28) which shows the assembly - the B-211 connected to a Remington typewriter, modified to be actuated by impulses from the crypto-

it was natural that, graphic machine. Of course, the next step would be to make the recording mechanism an integral part of the cryptographic machine. This you can see in the next slide (Fig. 30), in which the four rotating members, referred to in connection with Fig. 27 and which control the two commutators also mentioned in connection with Fig. 27 are clearly seen. The mechanism at the right controls the <sup>slide-bar</sup> printing wheel in front of the slide-bar mechanism and causes the proper letter to be printed upon the <sup>moving paper</sup> tape seen at the front of the machine.

Now we come to the next and <sup>a</sup> very important development, one first conceived by a European inventor. He was followed <sup>hereafter but independently</sup> soon by an American inventor. In this advance the circuits between the keys of the keyboard and the lamps of the indicating board are varied by electrical <sup>rotating</sup> members called rotors, interposed between fixed electrical members called stators. In Europe the first of such machines put upon the market for purchase by anyone desiring one is shown in ~~Fig~~ the next slide (Fig. 31). The machine was appropriately <sup>enough</sup> named the ENIGMA — for solution of messages enciphered by its means was believed to be impossible, or nearly so.



(labeled I)

In Fig. 1 at the left, is seen the machine with the top cover plate closed. At the front is the keyboard; above it the indicator board, consisting of lamps underneath glass disks upon which letters have been inscribed. Above the indicator board, <sup>and to the left</sup> are seen the peripheries of four <sup>metal</sup> notched wheels; At the right in Fig. 1, the top cover plate has been removed, exposing the internal <sup>ciphering</sup> mechanism.

Three rotors or connection-changers "in cascade" can be seen, attached to notched rings. The rotors are rotatable and serve to change the circuits

between the keys of the keyboard to the lamps of the indicator board. In such a rotor there is a circle of <sup>26 equally-spaced</sup> contacts on the left face and a similar circle <sup>of contacts</sup> on the right face; wires passing through the rotor connect the contacts on the <sup>two by two</sup> left faces to those on the right face, and these connections are arbitrarily made. The rotors have on their peripheries the letters of the alphabet <sup>which</sup> <sup>are</sup> engraved or painted. These letters can be seen through small windows in the cover plate, so that the rotors can be

aligned to an initial <sup>setting</sup>. I used the expression "in cascade" a moment ago, <sup>in referring to the rotors,</sup> which simply means that the current, <sup>initiated by depressing</sup> ~~from~~ a key of the keyboard passes through <sup>the stator and then through</sup> all three rotors before reaching

at the left a switch button which can be set to "cipher", "decrypt" or "neutral" positions.

At the left of the first rotor is a stator, which is one also the 26 letters of the alphabet. This stator is important.

(labeled II)

front

and the contacts, are connected, <sup>26</sup> wires to double-throw switches operated by and associated with the 26 keys of the keyboard. The connections between the 26 contacts, and the 26 switches of the keyboard are fixed. <sup>on the stator</sup>

also has a ~~rod~~ circle of <sup>equally-spaced</sup> 26 contacts, but <sup>these are</sup> only on its right face. But the stator is also rotatable and its position <sup>at any time</sup> can also be seen through a window, (labeled 3 in Fig. 2(E), so that the initial setting of the stator and the <sup>three</sup> rotors can be seen through the four windows. The initial settings of these four elements constitute the key for the starting point in ciphering operations.

a lamp of the indicator board. In the ENIGMA, the current exits from the <sup>third, that is, the</sup> last rotor at the right and <sup>then</sup> enters into another stator having <sup>also</sup> 26 contacts, but <sup>these are</sup> only on its left face. This stator is fixed or non-rotatable, and <sup>its contacts are connected two by two by 13 internal wires.</sup> 13 of its contacts ~~are~~ <sup>are</sup> connected to the other 13, contacts <sup>for Fig. 32,</sup> by ~~was passing~~ <sup>is called the reflector;</sup> through this stator. This stator serves to return the current <sup>which exits from one of the 26 contacts on the right face of the</sup> that rotor into one of the 25 <sup>remaining</sup> contacts of the right face of that rotor, and ~~then~~ <sup>then</sup> back to through <sup>contact on the left face of that rotor into a contact on the right face of the second or middle rotor, which enters a contact on the right face of the</sup> left-hand stator. Thus the circuitry in this machine insures that if  $A_p = K_c$  <sup>for example,</sup> then  $K_p = A_c$  <sup>in the same position of the rotors.</sup> that is, the cipher process is reciprocal in nature. <sup>The circuitry can be seen in Fig. 32.</sup> It also has as a consequence that no letter can encipher <sup>itself</sup> itself, that is,  $A_p$  for example, can never be represented by  $A_c$  <sup>no matter what</sup> <sup>happens to be.</sup> <sup>three,</sup> position of the rotors and the left-hand stator. The same is true of all the other 25 letters of the alphabet. The three rotors are interchangeable, so that <sup>3! = 2 x 1 or</sup> six permutative arrangements of these rotors is the maximum, <sup>possible,</sup> since in this construction the rotors cannot be inserted in an "upside-down" position. In other types of such machines the rotors are made so that they can be inserted in either an



6 x 4 x 2

1  
 2  
 3  
 4  
 5  
 6  
 7  
 8  
 9  
 10  
 11  
 12  
 13  
 14  
 15  
 16

Of course, if there are more than three rotors are available from which a selection of 26 has can be made the possibilities increase very considerably.

"rightsided-up" or "upside down" position. This makes possible a maximum of  $6 \times 4 \times 2$  or 48 permutations of ~~the~~ three rotatable rotors. The ~~left-hand~~ <sup>left-hand</sup> stator <sup>is</sup> ~~can~~ be moved only by hand, the reflector at the right is fixed in this model of the ENIGMA.

Depressing the key of the keyboard causes the first rotor to advance one step, thus changing the circuit from the left-hand stator, thence through the rotors to the reflector, thence back through the rotors to the left-hand stator, thus causing a second depression of the same <sup>key</sup> to produce a different cipher equivalent.

I won't take the time to tell you about how the rotors are caused to advance so that over 17 thousand <sup>of</sup> letters can be enciphered before the window settings of stator and rotors return to their initial alignment.

(The total number is not in this case  $26^3$  or 17576 but <sup>(26 x 25 x 26)</sup> 16,900 for technical reasons ~~etc~~ which there isn't time to explain.) Power for the electrical circuits is provided by small dry cells in the box at the upper right in Fig. 31 (II).

The original ENIGMA enjoyed a fair degree of



<sup>additional</sup>  
One virtue of the Halvern machine was that the  
wiring in the rotor were variable, a feature not  
incorporated in the ENIGMA rotors.

0751-7

Navy had but two machines <sup>neither</sup> of which could be made available, so I induced the Chief Signal Officer to buy a couple of them for me. The rotor wirings were altogether different from those of the Navy, a fact which I discovered simply by asking Strubel to substitute a few letters on his machine using settings I specified.

Machine. Power was furnished by the small dry cell seen at the upper left. The Navy was considering purchasing a rather number of these machines and <sup>Lieut Strubel,</sup> then Chief of the Navy's Code and Signal Section of the Office of Naval Communications, asked me to study the machine for

its cryptosecurity. After some ~~weeks~~ study I reported that <sup>in my opinion</sup> I thought the security <sup>of the machine</sup> was not so great as Navy thought. The result was a challenge, which I

accepted. Navy gave me ~~some~~ messages put up on its machine and I was successful in solving them.

There isn't time to go into the methods used but if you are interested you can find them described in my brochure entitled

Hebern built several more models for Navy and these had printing mechanisms associated with them, but Navy dropped negotiations with Hebern when it became obvious that he was not competent to

build what Navy wanted and needed. Navy then established its <sup>cryptographic research and</sup> own development unit at what is now known as the Naval Weapons Plant in Washington.

Army and Navy went their separate ways in such work for a number of years, but finally, in 1938 or 1939, close collaboration <sup>brought</sup> as a result <sup>of which</sup> an excellent

Army developed at the Signal Corps Substation Converter M-134 at Ft. Monmouth a machine known as Converter M-134 and gave a slide (Fig. 35) showing what it looked like.

machine which <sup>in quantity</sup> was developed, <sup>by the Teletype Corporation in Chicago.</sup> produced, distributed and used very successfully <sup>by all our Armed Forces</sup> from 1940 to the end of World War II and for some years thereafter. This was a rather large ~~and~~ <sup>requiring considerable amount of electric power and</sup> machine, <sup>hence unsuited for use by small</sup> units in field operations. <sup>In the late 1930's the</sup> Army became interested in a small mechanical machine invented by a Swedish engineer, named Hagelin. Modifications desired by Army were incorporated <sup>which was called Converter M-209,</sup> in the machine, and over 100,000 <sup>in the years 1942-44</sup> of them were manufactured by the Smith-Corona Typewriter Co. at Boston, New York. Here's a slide (Fig. 36) showing Converter M-209, which was used by all our Armed Forces in World War II, <sup>and here is another (Fig. 37)</sup> When properly used it gave a high degree of security; when improperly used, as was often the case, its security was rather illusory. This machine operates on what is termed the key-generator principle and when two or more messages are enciphered by the same key stream or portions thereof, solution is relatively a simple matter but I cannot go into that now. With the world-wide <sup>adoption of automatic printing telegraph</sup> or teleprinter <sup>became pressing</sup> communications the need for a reliable and practical cryptographic mechanism to be associated <sup>or integrated</sup> with the teleprinter. The first <sup>apparatus</sup> development of this sort in the U.S., is shown in this slide (Fig. 38), <sup>developed</sup> was that by the American



and Telephone Co., in 1918, as a more or less simple but ingenious modification of its ordinary printing telegraph. First, a few explanatory words about the latter may be useful. It is based upon the use of <sup>what is called the "Baudot Code," that is, a system</sup> ~~of~~ <sup>in which there are five</sup> ~~elements~~ of two different kinds to represent characters of the alphabet. These <sup>two</sup> elements may be positive and negative currents of electricity, ~~or the~~ <sup>presence and absence of current.</sup>

Here is a slide (Fig. 39) which depicts the Baudot or 5-unit code <sup>in the form of a paper tape in which there are holes in certain positions - transversely to the length</sup> of the tape. The holes are produced by a perforating mechanism; the small holes running the length of the tape are "feed holes" by means of which the tape is advanced step by step. You will note that there are five levels on which the holes and spaces or blanks appear. The letter A, for example, is represented by a hole in the 1<sup>st</sup> and 2<sup>nd</sup> levels; the 3<sup>rd</sup>, 4<sup>th</sup> and 5<sup>th</sup> levels are blanks; the letter B, by holes in positions 2 and 3, etc. Toward the right-hand end of the tape are two permutations labeled "letters" and "figures", respectively. These are equivalent to the "shift" and "unshift" keys on a typewriter keyboard, or "lower" and "upper" case. When the "letters" key is depressed, the characters

Typed  
continue after p. 30 of 1st draft,  
discarding old page  
31 of 1st draft.

REF ID: A62831

This material is to be  
typed triple space, on  
1 carbon copy, on  
legal size sheets

designated as the ECM Mark II, ECM standing for "electric cipher machine," in the Army it was designated as the SIGABA, in accordance with a nomenclature in which <sup>items of Signal Corps</sup> cryptographic material are given ~~to~~ short titles beginning with the initial trigraph SIG.

The ECM-SIGABA is a rather large machine requiring <sup>a</sup> considerable amount of electric power and much <sup>too</sup> heavy to be carried <sup>about</sup> by a single operator performing field service. It was safeguarded with extreme care and under strictest security regulations during the whole period of World War II operations. None of our Allied <sup>even</sup> were permitted ~~to have or even~~ <sup>to see the</sup> ~~machines,~~ let alone have it. In order to ~~facilitate~~ <sup>facilitate</sup> inter-communication between <sup>U.S.</sup> and <sup>British</sup> <sup>forces,</sup> an adaptor was developed so that, by ~~the~~ use of the latter in connection with the <sup>American</sup> ECM-SIGABA, messages could be ~~sent~~ <sup>exchanged</sup> in cipher <sup>with</sup> British units <sup>possessing</sup> ~~with~~ a British machine called <sup>for which an</sup> ~~TYPEX~~ <sup>adaptor</sup> cryptographically equivalent to the American one had been developed. This system of inter-communication worked satisfactorily <sup>and</sup> <sup>securely.</sup>

Certain improvements in the method of usage and certain new components, to be associated with the ECM-SIGABA for automatic decipherment by perforated tapes, were introduced during the war-time employment of these machines. But the SIGABA-ECM as originally developed and produced became obsolete some years after the close of hostilities because newer machines, ~~developed~~ developed by NSA cryptologists and engineers, replaced them, but not because there were ever any indications that messages enciphered on the machine had been deciphered by the enemy. As a matter of historical fact it may be stated that all efforts to solve such messages were fruitless, and it is also a fact that no machines were ever captured by the enemy; nor were there ever any suspicions that a machine had been exposed to enemy inspection at any time. Once and only once were there any apprehensions in this regard, when, through a careless disregard of specific instructions, a truck, and an attached trailer, in which this machine and associated material were housed, were stolen from during the night when parked on the street in front of the headquarters of the 28th Division during the Battle of the Bulge. A great search was instituted during the course of which a river was diverted, and the trailer, with all its contents intact, was found resting on the bed of the diverted stream. The episode terminated in court-martial proceedings; and there were no further incidents of this sort. Let me

add that such apprehensions as were entertained at the time the machines were based not upon the possibility that the machine had been captured, but upon the possibility that the machine would be used in the Chicago episode and that it would be in a position to turn out way

years before the SIGABA was put into service. About five years ago the Army's small need for a cipher machine for field use became obvious. The strip cipher system for this purpose, nor was the Army's M-134 suitable, the electrical machine was not suitable, for reasons I already indicated. The sum of \$2000 was allotted by the Army to the Chief Signal Officer for the development of a suitable machine, but also affording adequate security. The funds were turned over to the Signal Corps laboratories at Fort Monmouth, New Jersey, the military director of the laboratories, <sup>technical guidance or assistance from the Signal Intelligence Service, outside assistance,</sup> <sup>and deciding that this staff had sufficient know-how without</sup> <sup>up all the funds allotted for the purpose.</sup> developed a machine which required no electricity, being all-mechanical. On its completion the model was sent to the Signal Intelligence Service for test. Two short messages were enciphered by the Chief of the S.I.S. <sup>using settings of his own selection. He then</sup> handed the messages and the model over to me as technical director, and I turned them over to two of my assistants. The reason for turning over the model with the messages was that it must be assumed that under field conditions machines will be captured. One of the two test messages was solved in about 20 minutes; the other took longer — 35 minutes. This was the ignominious end to the development, brought about by the failure to recognize that cryptographic invention must be guided by technically qualified cryptanalytic personnel. Unfortunately, all the available funds had been expended <sup>on this unsuccessful attempt</sup>; there was left for a fresh start



Insert

REF ID: A62831

This was because the Hagelin machine operates on what is termed the key-generator principle, so that when two or more messages are enciphered by the same key stream or portions thereof, solution of those messages is a relatively simple matter. Such solution permits recovery of the settings of the keying elements so that the whole stream can be produced and used to solve messages

[over]

Dickens, Charles:

Excerpt from:

The Pickwick Papers, Chapter XI: "Involving another journey and an antiquarian discovery."

Typescript of episode dealing with a fraudulent inscription.

REF ID: A62884  
 which have been correctly preserved  
 by the same party making  
 a duplicate copy made by  
 the enemy. I cannot go into details in  
 the report in this lecture.

Curiously enough, Francis Bacon was the first to employ such a "code" - many books in the early 17th century, and I showed you the one he used, in Section No. 2 (see Fig. 25, p. 42, of NSA Technical Journal, Vol. V, No. 2, April 1960).

large machine requiring considerable amounts of electric power and hence unsuited for use by small units in field operations. In the late 1930's the Army became interested in a small mechanical machine invented by a Swedish engineer named Hagelin. Modifications desired by Army were incorporated in the machine, which was called Converter M-209 and over 100,000 of them were manufactured in the years 1942-1944 by the Smith-Corona Typewriter Co. at Grafton, New York. Here's a slide (Fig. 36) showing Converter M-209, which was used by all our Armed Forces in World War II, and here is another (Fig. 37). When properly used it gave a high degree of security; when improperly used, as was often the case, its security was rather illusory. This machine operates on what is termed the "key-generator principle" and when two or more messages are enciphered by the same key stream or portions there of, solution is relatively a simple matter but I cannot go into that now.

Triple space 1 cc on legal size paper

introduction of With the ~~world-wide adoption of automatic~~ printing telegraph or teleprinter machines for electrical communications the need became pressing for a reliable and practical cryptographic

mechanism to be associated or integrated with ~~the teleprinter~~ such machines. The first apparatus of this sort in the U. S., shown in this ~~slide~~ photo (Fig. 38), was that developed by the American and Telephone Co., in 1918, as a more or less simple but ingenious modification of its ordinary printing telegraph. First, a few explanatory words about the latter

This principle employs may be useful. It is based upon what is called the "Baudot Code", that is, a system of permutations of two different elements taken in groups of five are employed in which there are ~~five elements of two different kinds~~ to represent characters of the alphabet. ~~in Bacon's "code" were a's and b's; he used but 24 of the 32 permutations~~ These two elements may be positive and negative currents of electricity, or the latter system being often referred to as being composed of "marking" and "spacing" elements the presence and absence of current. Here is a slide (Fig. 39) which depicts the

Baudot or 5-unit code in the form of a paper tape in which there are holes in certain positions transversely to the length of the tape. The holes are produced by a perforating mechanism; the small holes running the length of the tape are "feed-holes" by means of which the tape is advanced step by step. You will note that there are

available (2^5 = 32). For electrical communications the two elements



are used to represent the so-called "stunt" characters, which I will now explain. The third and fourth characters from the right-hand

five levels on which the <sup>perforations</sup> holes and spaces or blanks appear. The letter A, for example,

is represented by <sup>perforations only</sup> a hole on the 1st and 2nd levels; the 3rd, 4th and 5th levels <sup>remaining</sup>

<sup>imperforated</sup> are blanks; the letter I, <sup>is represented</sup> by holes in positions 2 and 3, <sup>no holes on the other three levels, etc.</sup> etc. toward the right-hand

English alphabet uses 26 of the 32 permutations; the remaining 6 permutations at the end of the tape are two permutations labeled "letters" and "figures", respectively.

These are equivalent to the "shift" and "unshift" keys on a typewriter keyboard, for

"lower" and "upper" case. When the "letters" key is depressed, the characters



26

printed are the letters of the alphabet (all capital letters); when the "figures" key is depressed the characters represented are similar to those printed on a typewriter when the "shift" key is depressed. <sup>second, third, and fourth</sup> permutations at the left-hand end of the tape are also stunts, characters and represent "line feed," "space," and "carriage return," and they perform <sup>electrically</sup> in a teleprinter what is done by hand on a typewriter: <sup>"line feed"</sup> causes the paper on which the message is printed to advance to the next line; the ~~space~~ "space" does exactly what depressing the space bar on a typewriter does, etc. When there are no holes anywhere across the tape, the character is called a "blank" or "idling" character — <sup>the printer does no</sup> nothing happens; ~~nothing~~ printing; nor is there any "stunt" <sup>functioning</sup> by the printer, but the tape merely advances. <sup>standard</sup> In modifying the printing telegraph machine to make it a printing telegraph cipher machine, or, to put the matter in a slightly different way, in developing the printing telegraph cipher machine the American Telephone and Telegraph Company ~~made good~~ <sup>was fortunate</sup> in having at its disposal the services of a ~~rather brilliant~~ <sup>brilliant</sup> ~~engineer~~ <sup>engineer</sup> named Gilbert S. Vernam who <sup>conceived</sup> had a brilliant principle. ~~It~~ <sup>That principle</sup> turned out to be so useful and valuable that it has come to bear his name and is often referred to as the "Vernam rule." Vernam saw that if in accordance with some <sup>general</sup> but invariant rule

Footnote 24) Parker, R.D. "Recollections Concerning the Birth of One-Time Tape and Printing-Telegraph Machine Cryptography." NSA Technical Journal, Vol. 11, No. 2, July 1963, pp. 103-114.

the marking and spacing elements of a 5-unit code group were combined with those of another 5-unit code group, which would serve as a keying group, ~~for the same system in accordance with some general rule~~ and the resultant 5-unit group transmitted over a circuit and combined at the receiver with the same keying group in accordance with the same general rule. The final resultant would be the original character. Vernam extended his idea to make it applicable to ~~any system for teleprinting~~ and an application in Vernam's name was filed in the U.S. Patent Office on 13 September 1918, and Patent No. 1,310,719 was granted on the invention entitled a "Secret Signaling System" on 22 July 1919.

The following more detailed description of Vernam's patent on the foregoing cipher system is <sup>extracted from a paper written by one of the other A.T.T. Company's engineers who was associated with Mr. Vernam at the time the invention was conceived and who, a few years after retirement from that company, became one of NSA's consultants:</sup>

Indent and single space  
copy matter indicated on attached sheet → (R.D. Parker p.108)

Here is an extract from a paper prepared by Vernam himself which in simple language explains

<sup>29)</sup> In this system which uses only two different symbols or elements, the so-called "binary code," the combinatory rule is its own inverse.

how his invention worked in a system developed during World War I for use of the Signal Corps, U.S. Army: <sup>22</sup>

CIPHER MACHINE - METHOD OF OPERATION

The messages are first punched in a paper tape by means of the keyboard perforator (Fig. 38 of this lecture). ...

\* \* \* \* \*

The cipher "key" may take the form of another tape [etc. as indicated on attached sheets labeled p. 17-21-]

indent  
+  
Single  
Space

on attached  
attached

<sup>22</sup> Vernam, G. S. "Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications," a paper presented at the Midwinter Convention of the A. I. E. E., New York City, 8-11 February 1926.

I wrote a monograph on the solution, consisting of a main paper of 2.5 pages, and 25 appendices, an Addendum 1 of 10 pages, and Addendum 2 of 2.5 pages, and together with the perforated cipher message table to each of the offices indicated above. In order to decipher these messages the Chief Signal Officer had to use two key tapes, the first of which had Riverbank solved the system. It was recognized both that tapes had to be made and employed in such a way as to challenge messages that Riverbank was in a position to produce the plain text of any of the latter on request if further proof of solution was needed or desired.

double-key-tape  
The foregoing system was placed into operation in 1918, on three start-stop circuits, for intercommunication among four stations serving Washington, New York, Hoboken and Norfolk, and which, according to Parker (see footnote 21 above), continued in operation for many months, even after the end of the war. In addition, a Signal Corps Company was organized to go to Europe with new equipment for installation of printing-telegraph circuits in France. This Signal Company was about ready to sail when the Armistice was signed November 11, 1918.

Upon my return to Riverbank, after being demobilized, in April 1919, I became an interested party in a rather warm argument conducted by letters exchanged between Colonel Fabryan, Director of Military Intelligence and the War Department, and the Chief Signal Officer, regarding the cryptosecurity of the cipher printing telegraph system as used by the Signal Corps. The argument ended by meeting successfully a test, which was tantamount to a challenge by the Signal Corps, to provide Fabryan, during one day's traffic in the system, the cipher tapes of 150 messages selected by the Director of Military Intelligence, who, having signed a letter prepared by Major Yardley, to the effect that the cipher system in question was "absolutely indecipherable," had then

~~exactly~~ how this invention and the system works:

indent of  
page  
Afraka

copy matter attached  
p.17

22

-96

duty and

courtesy of writing a congratulatory letter to Colonel  
 Fabyan, dated 24 March 1920, the <sup>final paragraph of</sup> which is as follows:

Your very brilliant scientific achievement  
 reflects great credit upon you and your whole  
 personnel. It would be impossible to exagger-  
 ate in paying you and Riverbank the deserved  
 tribute for this very scholarly accomplishment.

[Insert here  
 matter on this sheet (489) →  
 back of sheet number 488  
 + also on sheet number 485] The A.T. & T. Company's printing telegraphic cipher were  
 after Riverbank provided the double-key-tape system  
 with drawn soon insecure. The machines went into storage, where

in due course most of them were dismantled. But after  
 I left Riverbank at the end of 1920 and had  
 joined Chief Signal Officer's staff in Washington, I in-  
 duced the Chief Signal Officer to resuscitate two of the  
 equipments. These I employed, believe it or not, in  
 preparing the manuscripts for several editions of new  
 field codes for field use, called Division Field Codes,  
 for use in training or in emergency. I won't undertake  
 to explain how I performed this stunt, for it was a stunt, but it  
 worked very successfully, until there was no longer any  
 need for codes of this type. The codes were duly printed, and issued and used.

Cipher printing telegraphy was placed  
 upon the shelf and more or less forgotten by the Signal  
 Corps from 1920 until soon after Pearl Harbor. Although  
 beginning about 1938 <sup>communications engineers</sup> Mr. Frank B. Rowlett,  
 one of my associates, and I kept urging that there was

Insert to p. 48 (or reverse side)

The paper by Mr. Parker (see footnote 21) closes with the following ~~sentences~~ final paragraph:

ident  
+  
summary  
pp

Perhaps some day Mr. Friedman will tell of the part that he and the Riverbank laboratorians played in the cryptanalytic phases of this development.

Mr. Parker was not aware of the fact that what he ~~was~~ suggested had not only been done once <sup>but twice</sup>. The first time was immediately after the solution, ~~and the~~ copies of the write-up mentioned on p. 40 <sup>but they had</sup> had been sent to Washington, <sup>and the</sup> fate ~~is~~ <sup>is</sup> ~~unexplainable~~ <sup>or special technical</sup> that often happens to documents of limited interest — complete ~~and~~ ~~unexplainable~~ disappearance in the voluminous files of bureaucracy. <sup>The end of hostilities of World War II,</sup> The second time was soon after <sup>at a certain outfit I work</sup> when it was discovered that ~~an~~ <sup>many</sup> ~~persons~~ <sup>names</sup> were using the double-tape keying system for its teleprinter communications. I rummaged through my own files and uncovered the handwritten manuscript of <sup>certain parts of</sup> what I had written at the close of the successful solution of that system while at Riverbank. <sup>my second write-up</sup> ~~It~~ <sup>is</sup> a classified docu-

ment, dated 25 July 1948, <sup>sub-</sup> the title of which is "Can cryptologic history repeat itself?" It is possible that this write-up can be made <sup>but</sup> ~~but~~ <sup>it</sup> ~~may~~ <sup>is</sup> available to those of you who are interested in reading it if proper authority grants permission. [Insert continued on attached sheet]

p. 48





proved practical, too, ~~and~~ ~~from~~ ~~an~~ ~~occasional~~  
 error involving the re-use of a once-used tape,  
 the ~~system~~ of absolutely secure inter-communication  
 was assured and was used between and  
 by radio printing telegraphy among large headquarters  
 where the volume of traffic justified the use of  
 this equipment, ~~was assured~~. The principal advantage  
 was the simplicity of crypto-operation — no rotors  
 to be set, no settings of rotors to be deciphered, no  
 checking of encipherment by deciphering the message  
 before transmission, etc.

Sheet

leading members of the cryptanalytic  
 However, the S.I.S. maintained a theoretical interest in such  
 equipment and in 1937 <sup>there came an</sup> opportunity to test such theories  
 as were developed by them when a machine produced  
 by the International Telephone and Telegraph Company  
 evoked <sup>the</sup> interest of the Department of State as a possible  
 answer to the needs of that Department for rapid and  
 secure cryptocommunications by radio. The Secretary of  
 State requested the Secretary of War to <sup>study</sup> investigate the  
 machine from the point of view of security. <sup>For this purpose</sup> Messages deciphered by the Chief of the  
 and Records Division of the Department of State were provided. It is a  
<sup>surprise to participants</sup> <sup>able to tell you</sup> that the S.I.S. quickly solved  
 the text messages and therefore reported that the  
 machine was quite <sup>now</sup> successful; but it is with much regret  
 that I must tell you who invented and developed the  
 machine. It was <sup>a retired officer of the Signal Corps and</sup> none other than my old friend Colonel  
 Hitt. <sup>It was his ambassador to tell him about the results of our test</sup> <sup>as he was the first man to look to what I had to say</sup>  
 about the inadequacies of his brain child. As is so often  
 the case, when a competent technician has to <sup>neglect</sup> give up  
 his technical studies because of the pressure of admini-  
 strative duties, he <sup>unfortunately</sup> finds it very difficult  
 to keep abreast of new developments and progress in  
 the field <sup>in which he was at one time an expert.</sup> of his technical cognizance. The I.T. & T. Com-  
 pany having spent a great deal of money on <sup>the</sup> develop-  
 ment of a machine <sup>which hardly presented any room for improvement,</sup>  
 because the principles underlying it were so faulty, the company  
 dropped the further work on it. Colonel Hitt <sup>is</sup> glad to say that  
 the disappointment and was well enough in 1942 to be able to

retired to active duty during World War II  
 and returned a paroled time and of North Carolina  
 lives a quiet life now, on a small farm near Front  
 Row, Winton, N.C.

[Insert matter on reverse side of this page]

or would be real need for <sup>new and</sup> improved machines for <sup>not only</sup> protecting teleprinter communications, there was a <sup>complete</sup> lack of interest in such apparatus, but what was perhaps a more important factor <sup>in the failure to continue work in this field</sup> was the lack of <sup>Signal Corps</sup> funds for research and development <sup>for such work</sup> ~~of such a project~~.

<sup>more or less sudden</sup> entry into World War II, after 7 December 1941, immediately <sup>brought</sup> <sup>great</sup> <sup>need</sup> ~~pressure~~ for cipher printing telegraphy, especially for <sup>radio</sup> communications, <sup>whatever</sup> but there was no apparatus for it, — not a single one of those machines of 1918-1920 was in existence. <sup>A.T. & T. Company</sup> But <sup>S.I.S. did</sup> <sup>in readiness</sup> have drawings and the development of the machines <sup>was given a priority task to</sup> ~~was undertaken by~~ the Teletype Corporation because <sup>was known</sup> that firm had proved that it had the necessary know-how when it produced the SIGABA-ECM's for us. Navy had less need for cipher printing telegraphy <sup>than Army</sup> because the use of <sup>radio</sup> printing telegraphy by radio <sup>was</sup> <sup>than</sup> not practicable for ships at sea. However, Navy did have a need for such apparatus for its land communications and joined Army in the development thereof. The machines <sup>were</sup> produced with remarkable speed <sup>by</sup> Teletype Corporation. Most of them were allotted to Army, a few to Navy. The Army called the machine the SIGCUM; the Navy called it CSP-888. Under heavy

in the category of cryptographic equipment of the foregoing type fall because the latter employ letters of the alphabet; but apparatus for CIFAX transmissions, that is, pictures or facsimile transmissions, and apparatus for protecting CIPHERY transmissions, that is, tele-  
 phone communications, were also developed. But there is not time to go into details with regard to 62 machines and apparatus that have been developed in two categories of cryptographic equipment - namely, although the history of their development is not clear from any other very important. But I just

use in service improvements were made both in regard to mechanical and electrical features and in regard to methods of keying, the use of indicators, etc. But I must tell you that before those machines became available in quantity there was only one recourse: we went back to the use of the double-key-tape method of ciphering, <sup>using standard teletype apparatus. The cipher was</sup> practically the same as it was in 1920 but we had safer methods of key-tape production and indicators for their use. The S. I. S. and the equivalent unit in Navy were not happy because operators' errors left messages open to solution, so that when the new cipher machines were ready they were placed into service as soon as possible, priority being given to circuits with heavy traffic.

~~Other types of cryptographic apparatus were developed during World War II. <sup>called</sup> CIFAX machines for protecting facsimile transmissions.~~  
 I cannot refrain from adding that <sup>except one</sup> in every case the apparatus produced by <sup>commercial</sup> research and development firms that without direct guidance from the cryptologists of the Army and the Navy. The one exception is, I believe, in the case of the extremely high security cipher system <sup>and equipment</sup> developed and built


Cryptographic equipment of the foregoing type fall because the latter employ letters of the alphabet; but apparatus for CIFAX transmissions, that is, pictures or facsimile transmissions, and apparatus for protecting CIPHERY transmissions, that is, tele-  
 phone communications, were also developed. But there is not time to go into details with regard to 62 machines and apparatus that have been developed in two categories of cryptographic equipment - namely, although the history of their development is not clear from any other very important. But I just

by the A.T. & T. Company. It was called SIGSALY<sup>L</sup>.  
 There were six terminals, each of which cost over  
 \$1,000,000. But NSA cryptologists and engineers  
 have produced smaller and better <sup>equipments based upon</sup> SIGSALY principles  
 and such equipments are bound to play extremely  
 important roles in any future wars in the future.

So much for <sup>for the history of the development and progress</sup> cryptographic apparatus at this  
 point. I shall return to that phase of cryptologic  
 history before the close of this lecture. Right now I  
 shall say a few words about <sup>the history of the development and progress</sup> cryptanalytic ~~apparatus~~  
 apparatus.

The solution of modern crypto-communication systems has been facilitated and, in some  
 cases, made possible <sup>only</sup> by the invention, development, and  
 application of <sup>highly-specialized</sup> cryptanalytic machinery, including apparatus  
 for intercepting and recording certain types of transmissions before cryptanalysis  
 can be attempted. One must understand  
 the basic nature of the problem which confronts the  
 cryptanalyst when he attempts to solve one of these  
 modern, very complex cryptosystems. First of all he  
 must be given the crypto-communications in a form  
 which <sup>make them visible for inspection and study</sup> is suitable for study. Usually they are  
 characters <sup>(letters or numbers)</sup> in the case of literal communications, or they are

<sup>electrical</sup> signals of a recordable type in the case of cifax or  
 aphony communications. Next he must have ~~at his~~  
 available to him instrumentalities that will assist  
 him in his analytical work, such as machinery for  
 making frequency counts, comparisons of sequences,  
 etc., and this, in the case of complex systems, must be  
 done at high speed. Cryptanalysis of modern  
 cryptosystems requires testing a very great number  
 of assumptions and hypotheses because ~~of the~~  
 sometimes astronomically large number of <sup>possibilities, i.e.,</sup> ~~permutations~~  
 and combinations, <sup>one after the other</sup> must be tested until the correct answer  
 is found. Since the advent of high-speed machinery  
 for such purposes, including electronic digital  
 computers about which so much is being heard and  
 read nowadays, the cryptanalyst ~~doesn't~~ isn't  
 discouraged by these astronomically great numbers  
 of possibilities.

Perhaps long before my time cryptanalysts  
 in Europe discovered that the use of sliding strips of  
 paper could sometimes facilitate reaching a solution  
 to a cryptanalytic problem, but so far as I am aware  
 the very first cryptanalytic aid <sup>made</sup> in the U.S. is the one  
 shown in Fig. , which is a picture of what I <sup>made</sup> called

5251  
72607  
79721

Park Hill  
Box 884

0963

REF ID: A62831

Front Royal Va.

A proponent of ~~the~~ ~~or~~ ~~an~~ ~~epidemiologic~~  
history report itself. Dated 21 July 1948.



at Riverbank and which I called the Polyalphabet. It was useful in solving ciphers which today are regarded as being of the very simplest types. When I came to Washington after leaving Riverbank, I wasn't troubled by a plethora of ideas for cryptanalytic aids — I was pre-occupied with devising and inventing cryptographic aids and machines. But I did now and then develop and try out certain ideas for cryptanalytic aids, frequency counters, comparison or coincidence machinery and the like. Why didn't I think of IBM machines? I did, but what good did that do? Did the Signal Office have any such machines — or even one dollar for their rental? You know the answer to that without my spelling it out. There wasn't any use even in suggesting that IBM machines could be of assistance to me — remember, now, that ~~but~~ I'm talking about the years <sup>from</sup> 1921 to 1933, and in the last-named year we were in the depths of a great economic depression. But one <sup>the summer of</sup> day in 1934 I learned by a devious route, <sup>(Army and Navy were not then sharing secrets)</sup> that the Navy Code and Signal Section had ~~seen~~ <sup>seen</sup> IBM machines or two, and my chagrin was almost unbearable. Not long afterwards I learned that a certain division of the Office of the

Quartermaster General in the Munitions Building had an IBM installation which had been used for accounting purposes in connection with the C.C.C. - the Civilian Conservation Corps established to provide work and ~~subsistence~~ subsistence for young men who could find no ~~work~~ jobs in the depression. I also learned that a new officer had just been assigned to head that particular division - and that he just had no use for ~~such~~ <sup>the</sup> newfangled ideas of his predecessor and wanted to get rid of those nasty IBM machines. But the contract with IBM still had some months to go run before the lease expired and either the machines would sit idle or the Government would lose money by ~~cancel~~ terminating the contract before the due date of expiration. This annoyed me, but it also gave me an idea. I ~~just~~ wrote a memorandum and here's a picture of it (Fig. ). Do read you what it says:

Intent & purpose space

attached

Attached to the memo was a brief explanation amounting to <sup>IBM</sup> of what I've told you about that installation in the Office of the Quartermaster General. Note that I placed

[This belongs in  
envelope  
No 28]

30 October 1934

Major Akin: In many years service here I have never once "set my heart on" getting something I felt desirable. But in this case I have set my heart on the matter because of the tremendous load it would lift off all our backs.

The basic idea of using machinery for code compilation is mine and is of several year's standing. The details of the proposed system were developed in collaboration with Mr. Case, of the Int. Bus. Machines Corp.

I regard this as one of my most valuable contributions to the promotion of the work for which we are responsible.

Please do your utmost to put this across for me. If you do, we can really begin to do worthwhile cryptanalytic work.

F.

the emphasis upon the ~~load~~ burden that would be  
 lifted from cryptographic work, ~~that~~ by using  
 the IBM machinery, thus leaving more time for  
 cryptanalytic work. This was because the responsi-  
 bilities of the S.I.S. for cryptanalytic <sup>operations</sup> ~~the~~  
 were at that time restricted purely to theoretical  
 studies. Studies ~~on~~ or cryptanalytic work on  
 foreign cryptosystems, <sup>had been</sup> ~~was~~ a responsibility of  
 the ~~Signal Corps during peace time~~ <sup>the G-2 of the</sup>  
 General Staff <sup>until 1929, responsibility had</sup> ~~but that~~ been transferred to the  
 Chief Signal Officer and the Signal Corps in the  
 year named. But the Chief Signal Officer had  
 very little money to use for that purpose, and,  
 besides that, the Army Regulation applicable  
 thereto specifically ~~that~~ restricted cryptanalytic  
 operations on foreign communications to war-  
time. And, more to the point, was the fact that  
 there was no material to work on even if  
 funds were available, because <sup>the Army</sup> ~~we~~ had at  
 that time no intercept stations whatever, anywhere  
 in or outside the U.S. But that's another story and  
 I'll proceed to the next point, which is that my  
 memo to Major Akin produced results. Just a

half month after I wrote and put it in his "In" basket I got the machines moved from the Office of the Quartermaster General to my own warren in the Office of the Chief Signal Officer! That move must have been fortuitous magic.

Once having ~~proved~~ demonstrated their utility to the Chief Signal Officer the almost prematurely terminated contract with IBM was renewed — and soon expanded. I don't know how we could have managed without such machines during World War II. Here's a picture <sup>(Fig. 00)</sup> of one of two whole wings in one of our buildings at Arlington Hall filled with IBM machines — the biggest installation in the world at that time.

We built or had built for us by IBM and other concerns adaptors to work with standard IBM machines; we constructed or had constructed for us by commercial firms highly specialized cryptanalytic apparatus, machines, and complex assemblies of components. Under war-time pressures fantastic things were ac-

complished and many were the skills of grati-  
 fying achievement when things that <sup>just</sup> couldn't  
 be done were done — and were of high importance  
 in military, naval and air operations against the  
 enemy.

Even were time available I couldn't show  
 you pictures of some of the high-class gadgets we  
 used, neither is it permissible to say more than  
 I have already said about them, even though  
 it is no longer a deep secret that electronic ~~the~~  
 computers are ~~so~~ highly useful in cryptologic work.  
 For example, here is a paragraph <sup>Fig.</sup> taken from a  
 Russian book entitled  
 and below it is ~~the~~ what it says in English.

To the layman the exploits of pro-  
 fessional cryptanalysts, when those exploits  
 come to light as, for example, in the various  
 investigations of the attack on Pearl Harbor,  
 are much more fascinating than those of  
 cryptographers, whose achievements in their  
 field appear to be dull or tedious to the  
 layman. But long consideration of the <sup>military</sup> ~~total~~  
 importance of <sup>Cryptography and</sup> communication security as against

that of cryptanalysis and communication intelligence has induced me to formulate what I shall immodestly call Friedman's Law. It is quite simply stated. ~~You may~~ <sup>a commander</sup> If you keep the cryptanalytic or COMINT face of your cryptologic coin bright and shiny, <sup>he ~~has~~</sup> stands a good chance of winning a battle <sup>even if</sup> forces are inferior in <sup>size and</sup> ability compared with those of his enemy; but if he <sup>lets</sup> the cryptographic or COMSEC face of ~~the coin~~ that coin become dull from neglect, ~~or~~ indifference, or carelessness, <sup>almost</sup> he will ~~certainly~~ lose a battle <sup>even if</sup> of his forces are superior in size and ability compared with those of his enemy.

With the foregoing statement of <sup>an</sup> ~~well considered~~ <sup>distilling</sup> opinion founded upon a half century's <sup>study and experience in</sup> devotion to cryptology as a profession, I bring this series of lectures to an undramatic ~~close~~ <sup>hope,</sup> but <sup>meaningsful</sup> close.

Don't forget  
3649

~~SECRET~~

From: Tokyo  
 To : Washington  
 19 November 1941  
 (J19)

TRANSLATION REVISED 26 Sept. 44.

*(by Hunt)*

Circular #2353

Office Chief's Code.

I do not know but what, as a result of the terrible strain in our operations, we have at length come to stand amid the ultimate evil circumstances, and if this be so, our communications with the country (ies) we are dealing with will be cut. And in the event that our foreign relations fringe on catastrophe, then in the middle and at the end of our universal broadcasts, <sup>in</sup> the form of weather predictions, we will repeat and broadcast twice each the following:

(1) In the case of Japanese-American relations  
 (HIGASHI NO KAZEAME). *East wind rain*

(2) In the case of Japanese-Soviet relations  
 (KITA NO KAZEKUMORI). *North wind cloudy*

(3) In the case of Japanese-British relations  
 (including their implications in Thai along  
 with Malaya and the Netherlands East Indies),  
 (NISHI NO KAZEHARE). *West wind clear*

Hence you will know that you are suitably to destroy codes documents, etc.

You will please guard this in strictest secrecy.

*This for Voice Broadcast -  
 " Twice in middle and twice at end "*

*There is good evidence that "Nishi no Kazehare"  
 was really transmitted in this way. See  
 Doc N° 4 of FCC Statement.*

~~SECRET~~



~~SECRET~~

From: Tokyo  
 To : Washington  
 19 November 1941  
 (J19)

TRANSLATION REVISED 26 Sept. 44. (Hurt)

Circular #2353

Office Chief's Code.

I do not know but what, as a result of the terrible strain in our operations, we have at length come to stand amid the ultimate evil circumstances, and if this be so, our communications with the country (ies) we are dealing with will be cut. And in the event that our foreign relations fringe on catastrophe, then in the middle and at the end of our universal broadcasts, <sup>in</sup> the form of weather predictions, we will repeat and broadcast twice each, the following:

- (1) In the case of Japanese-American relations  
 (HIGASHI NO KAZEAME).  
*East wind rain*
- (2) In the case of Japanese-Soviet relations  
 (KITA NO KAZEKUMORI).  
*north wind cloudy*
- (3) In the case of Japanese-British relations  
 (including their implications in Thai along  
 with Malaya and the Netherlands East Indies),  
 (NISHI NO KAZEHARE).  
*West wind clear*

Hence you will know that you are suitably to destroy codes documents, etc.

You will please guard this in strictest secrecy.

*This for  
 Voice broadcasts of weather  
 Twice in middle and twice at end*

*There is good evidence that "Nishi no Kazehare"  
 was really transmitted in this way. See Doc  
 N-4 of FCC statement.*

~~SECRET~~

~~TOP SECRET~~

REF ID: A487457

~~CONFIDENTIAL RESTRICTED~~

TO \_\_\_\_\_ DATE 27 May 45 FROM \_\_\_\_\_

- \_\_\_\_\_ Commanding Officer
- \_\_\_\_\_ Assistant Commandant
- \_\_\_\_\_ Dir of Comma Research
- \_\_\_\_\_ Control O
- \_\_\_\_\_ Fiscal O
- \_\_\_\_\_ Administrative O
- \_\_\_\_\_ Post Adjutant
- \_\_\_\_\_ Intelligence O
- \_\_\_\_\_ Provost Marshal
- \_\_\_\_\_ 2nd Sig Serv Bn
- \_\_\_\_\_ Chief, Pers & Tng Div
- \_\_\_\_\_ Chief, Pers Br
- \_\_\_\_\_ Chief, Tng Br
- \_\_\_\_\_ O/C Officer Pers Sec
- \_\_\_\_\_ Chief, Oper Serv Div
- \_\_\_\_\_ Chief, Communications Br
- \_\_\_\_\_ Chief, Laboratory Br
- \_\_\_\_\_ Chief, Machine Br
- \_\_\_\_\_ Chief, Supply Br
- \_\_\_\_\_ O/C, SSA Mail Unit
- \_\_\_\_\_ Chief, Security Div
- \_\_\_\_\_ Chief, Protective Sec Br
- \_\_\_\_\_ Chief, Cryptographic Br
- \_\_\_\_\_ Chief, Development Br
- \_\_\_\_\_ Chief, Intelligence Div
- ✓ \_\_\_\_\_ Chief, Language Br
- \_\_\_\_\_ Chief, Mil Cryptanalytic Br
- \_\_\_\_\_ Chief, Gen Cryptanalytic Br
- \_\_\_\_\_ Chief, T/A and Control Br
- \_\_\_\_\_ Chief, I & L Br

- \_\_\_\_\_ As discussed
- \_\_\_\_\_ As requested
- \_\_\_\_\_ Comments and return
- \_\_\_\_\_ Information and file
- \_\_\_\_\_ Information and forwarding
- \_\_\_\_\_ Information and return
- ✓ \_\_\_\_\_ Recommendation
- \_\_\_\_\_ See note on reverse
- \_\_\_\_\_ Signature if approved
- \_\_\_\_\_ Your action

15-3-04900.

Declassified and approved for release by NSA on 11-08-2013 pursuant to E.O. 13526

I desire a fresh translation of these two messages. Please put your most competent man on it. In case any of the groups are garbled or in case of slightest doubt about any of the deciphered groups, please let me know.

Would appreciate having these back as soon as practicable

J.

These messages have been translated by Mr. Gerhard and Mr. Frank Faust in collaboration. I am sure translation can be depended upon as accurate.

W.S.H.

W. S. # \_\_\_\_\_

*Translation by  
Mr. Gerboud  
and Mr. Zanet*

Circ # 2354

Secret

Please note that in case our foreign relations are on the verge of a break the following words are to be inserted at the beginning and end of general information broadcasts, five times each.

1. In the event of tension in Japanese-American relations: "East."
2. In the event of [tension in] Japanese-Soviet relations: "North."
3. In the event of [tension in] Japanese-British relations (including occupation of THAILAND and invasion of Netherlands East Indies and Malaya):  
"West."

TRANS. # \_\_\_\_\_

CHECKER \_\_\_\_\_

NO. \_\_\_\_\_

W. S. # \_\_\_\_\_

*Translation by  
Mr. Gerhard +  
Mr. Faust*

Circ # 2353

Handle in office chief's code.

As a result of the tension in the international situation matters may come to the worst. Since in this event communications between us and the opposing countries will at once be suspended it has been decided that, in case our foreign diplomatic relations come to a crisis, the following is to be broadcasted as a weather forecast in the Japanese language overseas news broadcast to all areas, repeated twice at the middle and at the end.

1. In the event of [a crisis in] Japanese-American relations:

"East wind, rain."

2. In the event of [a crisis in] Japanese-Soviet relations:

"North wind, cloudy."

3. In the event of [a crisis in] Japanese-British relations (including occupation of THAILAND and invasion of Netherlands East Indies and Malaya):

"West wind, fair."

In accordance with the above please make suitable disposition of your codes, documents, etc.

This is to be treated with strictest secrecy.

TRANS. # \_\_\_\_\_

CHECKER \_\_\_\_\_

NO. \_\_\_\_\_

~~TOP SECRET~~

STATION S

11/26/41 MC-C (91)

FROM: TOKYO (TOGO)  
TO: WASHINGTON (KOSHI)

19 NOVEMBER, 1941

J-19

CIRC #2353 (COMPLETE)

MWZHU BUWTJ

*[Handwritten signature]*

XE	IC	NC	ST	WY	NY	KY	ES	NI	CU	KY	MT	AN	WE	UF
DB	TH	ZW	JX	HZ	US	GK	IY	IO	WV	MT	GS	WU	YK	UQ
EQ	XF	UX	KZ	RS	KH	SC	FW	AO	AD	CE	CY	SI	LW	BS
BN	XF	ZW	LU	GS	XE	YM	LZ	FF	US	TR	GD	UQ	EQ	
XG	FH	EK	FG	XJ	KC	KY	PE	IY	ZT	VE	FJ	NX	VA	TX
ZW	MS	ZP	KR	DB	NX	AE	NE	LZ	LJ	XJ	CT	NC	LA	BO
TM	WD	XE	YM	KY	UQ	EQ	XG	HL	GU	OM	LW	KY	FE	XD
DW	LD	VB	NC	JG	BO	EF	PB	XE	YM	ZW	UQ	EQ	XG	HL
VM	KY	FE	XD	CU	CN	JN	VB	NC	TK	BO	OC	XP	XE	YM
OV	ER	CX	NV	FA	XP	ZT	VB	HL	ZA	LW	KY	FE	XD	KP
QV	VB	NC	NV	JG	UP	QO	AF	UF	XE	EQ	XJ	KC	GG	BV
RE														

*[Extensive handwritten annotations in Japanese characters are present throughout the table, including names like 'YAGA', 'BEIJI', 'NIVWA', 'NICHIREI', 'KITA', 'NO', 'OV', 'QV', 'RE' and various symbols and numbers.]*



Office Chief's code.

I do not know but what, as a result of the terrible strains in ~~our~~ operations, ~~we~~ have at length come to stand ~~in~~ the ultimate evil circumstances, and if this be so, our communications with the country (ies) we are dealing with will be cut.

And in the event that our foreign relations fringe on ~~a~~ catastrophe, then in the middle ~~and~~ <sup>at the</sup> ~~end~~ of ~~our~~ ~~broadcasts~~, ~~and~~ ~~the~~ ~~form~~ of weather predictions, we will repeat and broadcast twice each the following:

1. In <sup>the</sup> case of Japanese American relations (Higashi no Kaze Ame).
2. In the case of Japanese - Soviet Relations (Kito no Kaze tumori).
3. In <sup>the</sup> case of Japanese - British relations (including their implications in Thai along with Malaya and the Netherlands East Indies), [Nishi no Kaze Kare.]

Since you will know that you are <sup>probably</sup> to ~~probably~~ destroy code documents etc.

You will please guard this in strictest secrecy.



I do not know but what we have arrived at the very worst as a result of the terrible <sup>industrial</sup> strain ~~of industry~~ here. If such be the case immediately communications between us and the nations we are dealing with will be broken. If our diplomatic relations should reach the "point of rupture," ~~that the~~ ~~Japanese~~ ~~broadcasting~~ of Japanese news to various areas of the world should be stopped, as a last resort, in the form of weather forecasts.

(1) In the case of Japanese-American relations: HIGASHI NO K

(2) In the case of Japanese-Soviet relations: KITA NO KAZE KOMORI

(3) In the case of Japanese-British relations (including Thai, Malaya, and the N.E.I.): NISHI NO KAZE HORO.

Since ~~times~~ ~~such~~ we will have these broadcasts repeated. Thereby you will know when to ~~to~~ burn up codes and pertinent documents. <sup>Furthermore</sup> you are ordered to keep the foregoing in the strictest secrecy.

Standard Form No 75  
February 1946

### UNITED STATES CIVIL SERVICE COMMISSION POSITION DESCRIPTION

1 Check one  
Dept  Field

2 Official headquarters

3 Reason for submission  
(a) If this position replaces another (i.e., a change of duties in an existing position) identify such position by title allocation (s.r., loc series, grade) and position number

(b) Other (specify) **New Position**

4 Agency position No

5 C S C certification No **92**

6 Date of certification **Mar 16, 1949**

7 Date received from C S C

8 **Class Act 1949**  
CLASSIFICATION ACTION

ALLOCATION BY	CLASS TITLE OF POSITION	CLASS			INITIALS	DATE
		Service	Series	Grade		
a Civil Service Commission						
b Department agency, or establishment	<b>Cryptologic Research Advisor</b>	<b>GS</b>	<b>1540</b>	<b>16</b>	<b>JWM</b>	<b>7-17</b>
c Bureau						
d Field office						
e Recommended by initiating office						

9 Organizational title of position **Special Assistant to the Director**

10 Name of employee (If agency specify V-1 S S or 4)

11 Department agency, or establishment **NATIONAL SECURITY AGENCY**

a First subdivision

b Second subdivision

c Third subdivision

d Fourth subdivision

e Fifth subdivision

12 This is a complete and accurate description of the duties and responsibilities of my position

(Signature of employee) \_\_\_\_\_ (Date) \_\_\_\_\_

13 This is a complete and accurate description of the duties and responsibilities of this position

**Spcl Asst Dir J. G. ...**

(Signature of immediate supervisor) \_\_\_\_\_ (Date) **28 FEB 1949**

Title **Director, National Security Agency**

14 Certification by head of bureau division, field office or designated representative

(Signature) \_\_\_\_\_ (Date) \_\_\_\_\_

Title \_\_\_\_\_

15 Certification by department, agency or establishment

(Signature) \_\_\_\_\_ (Date) \_\_\_\_\_

Title \_\_\_\_\_

16 Description of duties and responsibilities (See Guide to Position Classifiers, Employees and Supervisors for the Preparation of Position Descriptions Standard Form No 75A)

**See ATTACHED SUBSIDIARIES.**

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~SPECIAL ASSISTANT TO THE DIRECTORDUTIES AND RESPONSIBILITIES:

As the Cryptologic Research Advisor is the principal consultant to the Director, National Security Agency concerning the technical and exploitational aspects of all cryptologic activities. These activities encompass two very broad fields of endeavor, communications intelligence and communications security, and involve several unrelated technical, professional and scientific fields and programs which demand continued "pioneering" effort to keep abreast of advancements in the fields. Renders technical advice and assistance to the Director, staff divisions and operating offices in the formulation and execution of the broad over-all plans and programs of the National Security Agency and in the technical control and coordination of all activities. Is responsible for studying and evaluating the overall programs in terms of current and new technical tactical and strategic information for the purpose of recommending to the Director changes in programs which may be justified by any changes in trends or by the results of advances in the communications electronic field brought about by the research being carried on by various government agencies, universities and industrial laboratories. Investigates new discoveries with a view towards applying such discoveries or modifications thereof to the accomplishment of communications security and communications intelligence production programs.

HELP PROVIDED BY GUIDES:

Follows broad agency policy directives and regulations and is guided by past and current technical successes and accomplishments, but the present and advancing sophistication of the science of communications security and communications intelligence on a world-wide basis is such as to require cognizance of advances in these very broad fields and the ability to consider and apply this knowledge as guidelines in the solution of specific problems as well as in the continuing advancement of the art.

HELP PROVIDED BY SUPERVISOR:

Works under general administrative direction of the Director of the Agency acting independently on all scientific and technical matters. Receives no technical direction from higher echelons within the Agency.

ORIGINAL THINKING DONE:

Is responsible for initiating ideas and investigating and advancing techniques and programs in hitherto unexplored lines in a variety of scientific fields, especially the very broad field of communications-electronics, in order to advance the work of the Agency and to insure that the communications of the United States Armed Forces are the most secure in the world and the maximum production of communications intelligence.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~PERSONAL WORK CONTACTS:

Participates in high-level committee and conference work for coordinating communications intelligence and communications security activities within the Agency and with the requirements of cooperating groups outside the Agency; initiates and maintains relationships with professional, technical and scientific personnel of highest professional reputation and standing to secure information and assistance needed in solving cryptologic problems; maintains close technical liaison with Service Cryptologic Agencies and with other Agencies and governments and is recognized as an outstanding authority in the field of cryptology.

THE EXTENT TO WHICH DECISIONS AND JUDGMENTS MADE ARE CHECKED OR REVIEWED:

Advice, decisions and opinions are accepted as technically sound and valid and have considerable influence on national and international policies and agreements as well as on programs of the National Security Agency. Any review is in terms of administrative policies, budgetary and manpower considerations.

THE IMPORTANCE AND EFFECTS OF WORK DONE:

The functions and programs of the Agency are of vital importance to and are an integral part of the National Defense programs.

SUPERVISORY RESPONSIBILITIES:

Exercises no direct supervision, but recommendations, policies, plans and programs originated by the Research Advisor affect and control the efforts of several thousand personnel through <sup>out</sup> the agency.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

## National Security Agency

Cryptologic Research Advisor  
Vacancy

GS-1540-15

**BACKGROUND:**

The scientific advancements in the broad field of communications, and the importance of this field to world security, place increasingly complex demands upon the National Security Agency in the accomplishment of its missions in the Communications Intelligence, Communications Security, and Research and Development fields. These rapid advancements and the greater importance of this mission were recognized by the recent Presidential Executive Directive abolishing the Armed Forces Security Agency and reconstituting the organization as the National Security Agency. To efficiently and effectively accomplish the expanded mission, it is essential to attract and retain recognized authorities in the professional and scientific fields and to equitably compensate these authorities for their services. The present compression within the Agency at the GS-15 level does not meet this requirement. The attached position description generally outlines the scope of this highly technical mission but does not disclose some of the highly classified programs which are undertaken by this Agency.

**QUALIFICATIONS REQUIREMENTS:**

The incumbent of this position must possess outstanding qualifications in the field of cryptology. He must possess outstanding ability to conceive and initiate programs which will insure that the Agency not only keeps abreast of the advancing sophistication of the science of cryptology on a world-wide basis, but also continues the advancement of the art. He must also possess top recognition in this field to obtain technical assistance and cooperation in the various fields of endeavor.

**EVALUATION:**

The incumbent of this position will be the top cryptologic advisor in this highly technical and specialized field, supporting the security measures of the nation and the world. In addition to the importance of this position, the extremely complex and unprecedented nature of the work appears to warrant allocation to the proposed grade of GS-15. It is recommended, therefore, that the Civil Service Commission concur in this recommendation and submit the position to The President for final action.

WILMA FLYNN  
Chief, Civilian Position Classification Section  
National Security Agency

CONFIDENTIAL

## NATIONAL SECURITY AGENCY

Civilian Supergrade Positions

<u>Position</u>	<u>Organization</u>	<u>Proposed Grade</u>	<u>Authorized</u>
<u>Chief Communications Scientist.</u> Serves as the Deputy Director for Research and Development in the exercise of management and operational and technical control of cryptologic research and development vested in the Director of the National Security Agency.	R/D	GS-18	GS-18
<u>Cryptologic Research Advisor.</u> Serves as Special Assistant to the Director of the Agency and is responsible for advising the Director and Deputy Directors (Military - rotating between the services) concerning the technical and exploitational aspects of cryptologic activities of the Agency. Studies and evaluates the overall program for the purpose of recommending changes justified by any changes in trends or by results in advances in the cryptologic field.	Spec. Asst. to Director	GS-18	GS-18
<u>Chief Cryptanalyst.</u> Serves as Technical Director of a large organization responsible for all specialized classified communication activities of the Armed Forces.	PROD	GS-18	GS-16
<u>Communications Scientist.</u> Responsible for the performance of communication security functions under the cognizance of the National Security Agency. This includes the establishment and promulgation of the communications security doctrine, policy, techniques and instructional material of the Armed Forces.	COMSEC	GS-17	0
<u>Chief Physical Science Administrator.</u> Assistant Director, Research and Development, directs the research and development activities, the purpose of which is to augment the ability of the National Security Agency to perform its mission rapidly, thoroughly and economically. This involves work in several professional fields, including electronics, physics, mechanical and electrical engineering, mathematics, cryptology, and a variety of related fields, encompassing basic research, applied research, and pioneer development.	R/D	GS-17	GS-16

<u>Position</u>	<u>Organization</u>	<u>Proposed Grade</u>	<u>Authorized</u>
<u>Communications Specialist</u> . Responsible for providing the technical continuity in the current and long-range planning of the cryptologic activities of the Agency.	P/P	GS-17	0
<u>Cryptanalyst</u> . Serves as one of two Agency cryptanalytic authorities in a large organization, with responsibility for planning, coordinating and directing the Agency specialized cryptanalytic program, and for the suspension and termination of various phases of work.	PROD	GS-17 GS-17	0 GS-16
<u>Physical Science Administrator (Research)</u> . Serves as Chief of Office for Research, exercising technical control and guidance over the activities of a research group composed of an Engineering Research Division, Mathematical Research Division, and Physical Research Division, investigating areas having actual or potential value in meeting the special requirements of cryptologic equipment and techniques.	R/D	GS-16	0
<u>Physical Science Administrator (Development)</u> . Serves as Chief of Office for Development, exercising technical control and guidance over development activities, including the conduct and control of projects for development of cryptologic equipment and methods, and involves work in several scientific and technical subject matter fields.	R/D	GS-16	0
<u>Comptroller</u> . Responsible for analyzing and evaluating command programs to facilitate the accomplishment of objectives within available resources in the performance of accounting, budgeting, auditing, management analysis, and reporting functions to aid in the most effective utilization of personnel, equipment, and funds.	COMP	GS-16	0
<u>Cryptanalyst (Security)</u> . As the Chief Security Analyst, recommends new cryptosecurity and physical security policies, and directs the implementation in the services of established policies in these fields.	COMSEC	GS-16	0
<u>Cryptologic Statistician</u> . Is responsible for determining the feasibility of applying analytical machine processing equipment and techniques in the solution of problems, advising on such application, and devising and developing appropriate methods for the use of the equipment.	PROD	GS-16	0

<u>Position</u>	<u>Organization</u>	<u>Proposed Grade</u>	<u>Authorized</u>
<u>Cryptanalyst.</u> Makes recommendations on matters dealing with specialized activities, anticipating new cryptologic developments and conducting original research in cryptanalytic techniques, new systems, and new devices, from the viewpoint of the specialized interest.	PROD	<u>GS-16</u>	<u>0</u>
	TOTAL	14	5



Lecture 2

Final Version

~~CONFIDENTIAL~~LECTURE 2

As I said at the close of the preceding lecture, a bit of history is always useful in introducing a subject belonging to a special and not too well known field; therefore, I'll proceed with some historical information about cryptology, which, as you learned before, comprises two closely related sciences, namely, cryptography and cryptanalysis. I will repeat and emphasize that they are but opposite faces of the same valuable coin; progress in one inevitably leads to progress in the other, and to be efficient in cryptology you must know something about each of them.

Cryptography and cryptanalysis probably go back to the dawn of the invention and development of the art of writing itself. In fact, there is reason for speculating as to which came first--the invention of writing or the invention of cryptography; it's somewhat like the question as to which came first--the hen or the egg. It is possible that some phases of cryptography came before the art of writing had advanced very far.

I've mentioned the art of writing. As in the case of other seemingly simple questions, such as, "why is grass green?", when we are asked to define writing we can't find a very simple answer, just because the answer isn't at all simple. Yet, Breasted, the famous University of Chicago historian and Orientalist, once said: "The invention of writing and of a convenient system of records on paper has had a greater influence in uplifting the human race than any other intellectual achievement in the

~~CONFIDENTIAL~~

career of man." There has been, in my humble opinion, no greater invention in all history. The invention of writing formed the real beginning of civilization. As language distinguishes man from other animals, so writing distinguishes civilized man from barbarian. To put the matter briefly, writing exists only in a civilization and a civilization cannot exist without writing. Let me remind you that animals and insects do communicate--there's no question about that; but writing is a thing peculiar to and found only as a phenomenon in which man and no animal or insect engages, and let's never forget this fact. Mankind lived and functioned for an enormous number of centuries before writing was discovered and there is no doubt that writing was preceded by articulate speech for eons--but civilization began only when men got the idea of and invented the art of writing. So far as concerns Western or Occidental civilization, writing in essence is a means of representing the sounds of what we call speech or spoken language. Other systems of writing were and some still are handicapped by trying to represent things and ideas by pictures. I'm being a bit solemn about this great invention because I want to impress upon you what our studies in cryptology are really intended to do, namely, to defeat the basic or intended purpose of that great invention: instead of recording things and ideas for the dissemination of knowledge, we want and strive our utmost to prevent this aim from being realized, except among our own brethren and under certain special circumstances, for the purpose of our mutual security, our self-preservation. And that's important.

Writing is a comparatively new thing in the history of mankind. No complete system of writing was used before about 3500 B.C.

Ordinary writing, the sort of writing you and I use, is perhaps an outgrowth or development of picture writing or rebus writing, which I'm sure most of you enjoyed as children. A rebus contains features of both ordinary and cryptographic writing; you have to "decrypt" the significance of some of the symbols, combine single letters with syllables, pronounce the word that is represented by pictures, and so on. Here's an example which I have through the courtesy of the Bell Telephone Laboratories. Let's see how much of it you can make out in half a minute.

From rebus writing there came in due course alphabetic writing and let me say right now that the invention of the alphabet, which apparently happened only once in the history of mankind, in some Middle East Semitic region, in or near the Palestine-Syria area, then spread throughout the whole of the European continent, and finally throughout most of the world, is perhaps man's greatest, most important, and most far-reaching invention because it forms the foundation of practically all our written and printed knowledge, except that in Chinese. The great achievement of the invention of the alphabet was certainly not the creation of the signs or symbols. It involved two brilliant ideas. The first was the idea of representing merely the sounds of speech by symbols, that is, the idea of what we may call phoneticization; the second was the idea of adopting a system in which,

roughly speaking, each speech sound is denoted or represented by one and only one symbol. Simple as these two ideas seem to us now, the invention was apparently made, as I've said, only once and the inventor or inventors of the alphabet deserve to be ranked among the greatest benefactors of mankind. It made possible the recording of the memory of mankind in our libraries, and from that single invention have come all past and present alphabets. Some of the greatest of men's achievements we are now apt to take for granted; we seldom give them any thought. The invention of the art of writing and the invention of the alphabet are two such achievements and they are worth pondering upon. Where would we be without them? Note that among living languages Chinese presents special problems not only for the cryptologist but also for the Chinese themselves. No Sinologist knows all the 80,000 or so Chinese symbols, and it is also far from easy to master merely the 9,000 or so symbols actually employed by Chinese scholars. How far more simple it is to use only 20 to 26 symbols! Being a monosyllabic language, it seems almost hopeless to try to write Chinese by the sort of mechanism used in an alphabetic polysyllabic language; attempts along these lines have been unsuccessful and the difficulties in memorizing a great many Chinese characters accounts for the fact that even now only about 10% of the Chinese people can read or write to any significant degree. The spread of knowledge in China is thereby much hampered.

Probably the earliest reliable information on the use of cryptography in connection with an alphabetic language dates from about 900 B.C., Plutarch mentioning that from the time of Lycurgus there was in use among the Lacedemonians, or ancient Greeks, a device called the scytale. This device, which I'll explain in a moment, was definitely known to have been used in the time of Lysander, which would place it about 400 B.C. This is about the time that Aeneas Tacticus wrote his large treatise on the defense of fortification, in which there is a chapter devoted specifically to cryptography. In addition to mentioning ways of physically concealing messages, a peculiar sort of cipher disk is described. Also a method of replacing words and letters by dots is mentioned.

We find instances of ciphers in the Bible. In Jeremiah Chapter 25, Verse 26 occurs this expression: "And the King of Sheshakh shall drink after them." Also, again in Jeremiah 51:41: "How is Sheshakh taken!" Well, for perhaps many years that name "Sheshakh" remained a mystery, because no such place was known to geographers or historians. But then it was discovered that if you write the twenty-two letters of the Hebrew alphabet in two rows, eleven in one row and eleven in the other, like this, you set up a substitution alphabet whereby you can replace letters by those standing opposite them. For example, "Shin", is represented by "Beth" or vice versa, so that "Sheshakh" translates "Babel", which is the old name of "Babylon." Hebrew then did not have and still doesn't have vowels; they must be supplied.

This is an example of what is called ATBASH writing, that is, where Aleph, the first letter is replaced by Teth, the last letter; Beth, the second letter, by Shin, the next-to-the-last, etc. By sliding the second row of letters one letter each time there are eleven different cipher alphabets available for use. The old Talmudists went in for cryptography to a considerable extent. Incidentally, in mentioning the Bible, I will add that Daniel, who, after Joseph in Genesis, was an early interpreter of dreams and therefore one of the first psychoanalysts, was also the first cryptanalyst. I say that he was an early psychoanalyst, because you will remember that he interpreted Nebuchadnezzar's dreams. In the Bible's own words, "Nebuchadnezzar dreamed dreams, wherewith his spirit was troubled, and sleep brake from him." But, unfortunately, when he woke up he just couldn't remember those troublesome dreams. One morning he called for his wise men, magicians, astrologers, and Chaldean sorcerers and asked them to interpret the dream he'd had during the preceding night. "Well, now, tell us the dream and we'll try to interpret it", they said. To which King Nebuchadnezzar exclaimed, "The thing is gone from me. I don't remember it. But it's part of your job to find that out, too, and interpret it. And if you can't tell me what the dream was, and interpret it, things will happen to you." What the king asked was a pretty stiff assignment, of course and it's no wonder they failed to make good, which irked Nebuchadnezzar no end. Kings had a nasty habit of chopping your head off in those days if you failed or made a mistake, just as certain arbitrary

and cruel despots are apt to do even in modern times for more minor infractions, such as not following the Party Line. So in this case it comes as no surprise to learn that Nebuchadnezzar passed the word along to destroy all the wise men of Babylon, among whom was one of the wise men of Israel, named Daniel. Well, when the King's guard came to fetch him, Daniel begged that he be given just a bit more time. Then, by some act of divination, --the Bible simply says that the secret was revealed to Daniel in a night vision--Daniel was able to reconstruct the dream and then to interpret it. Daniel's reputation was made. Some years later, Nebuchadnezzar's son Belshazzar was giving a feast, and, during the course of the feast, in the words of the Bible, "came forth fingers of a man's hand and wrote over against the candlestick upon the plaster of the wall." The hand wrote a secret message. You can imagine the spine-chilling scene. Belshazzar was very much upset, and just as his father did, he called for his wise men, soothsayers, Chaldean sorcerers, magicians and so on, but they couldn't read the message. Apparently they couldn't even read the cipher characters! Well, Belshazzar's Queen fortunately remembered what that Israelite Daniel had done years before and she suggested that Daniel be called in as a consultant. Daniel was called in by Belshazzar and he succeeded in doing two things. He succeeded not only in reading the writing on the wall: "MENE, MENE, TEKEL, UPEARSIN", but also he was successful in deciphering the meaning of those strange words. His interpretation: "Mene" -- "God hath numbered thy kingdom and finished



it." "Tekel" -- "Thou are weighed in the balances and found wanting."  
 "Upharsin" -- "Thy kingdom shall be divided and given to the Medes and  
 Persians." Apparently the chap who did the handwriting on the wall knew  
 a thing or two about cryptography, because he used what we call "variants",  
 or different values, for in one case the last word in the secret writing on  
 the wall is "Upharsin" and in the other it is "Peres"; the commentators are  
 a bit vague as to why there are these two versions of the word in the Bible.  
 At any rate, Babylon was finished, just as the inscription prophesized; it  
 died with Belshazzar.

I think this curious biblical case of the use of cryptography is  
 interesting because I don't think anybody has really found the true meaning  
 of the sentence in secret writing, or explained why the writing on the wall  
 was unintelligible to all of Belshazzar's wise men. Here's a slide which  
 is supposed to give the best explanation of the enigmatical sentence that  
 has always been considered one of the most obscure of the many difficult  
 scriptural passages which have awakened the interest and baffled the ingenuity  
 of scholars. You see that this savant thinks that the cuneiform ideograms  
 were written without any division between the individual words, so that the  
 sentence "would be just as hard to read as a rebus and would puzzle the  
 most skillful decipherer." He goes on to say: "The difficulty would have  
 been still more increased if the ideograms had been grouped in some unusual  
 way, severing the natural connection of the component elements. If the

signs had been written in this manner it would have been almost impossible to arrive at their true meaning." But why could Daniel read and interpret the writing when his competitors couldn't? This our savant doesn't explain. Another savant offers as his explanation of the mystery the following hypothesis: That the words were written in columns, as shown in this slide, and that Daniel in solving the mystery read downwards or rather down, up, down. This explanation doesn't satisfy me any more than the other one.

The next slide I show you is the scytale, which I've already mentioned as one of the earliest cipher devices history records. The scytale was a wooden cylinder of specific dimensions around which they wrapped spirally a piece of parchment or leather; they then wrote the message on the parchment, unwound it, and sent it to its destination by a safe courier, who handed it over to the commander for whom it was intended and who, having been provided with an identically-dimensioned cylinder, would wind the strip of leather or parchment around his cylinder and thus bring together properly the letters representing the message. This diagram may not be accurate. I don't think anyone really understands the scheme. The writing was done across the edges of the parchment, according to some accounts, and not between the edges, as shown in this slide. Incidentally, you may be interested to learn that the baton which the European field marshal still carries as one of the insignia of his high office derives from this very instrument.

We don't know much about the use of cryptography by the Romans, but it is well known that Caesar used an obviously simple method; all he did was to replace each letter by the one that was fourth from it in the alphabet. For example, A would be represented by D, B by E, and so on. Augustus Caesar is said to have used the same sort of thing, only even more simple; each letter was replaced by the one that followed it in the alphabet. Cicero was one of the inventors of what is now called shorthand. He had a slave by the name of Tyro, who wrote Cicero's records in what are called Tyronian notes. Modern shorthand is a development of Tyro's notation system.

The next slide shows some cipher alphabets of olden times, alphabets used by certain historical figures you'll all remember. The first cipher alphabet on the slide was employed by Charlemagne, who lived from 768 to 814 A.D. The second one was used in England during the reign of Alfred the Great, 871 to 899. The third alphabet is called ogam writing and was used in ancient Ireland. The alphabets below that were used much later in England: the fourth one by Charles the First, in 1646; the fifth, the so-called "clock cipher", was used by the Marquis of Worcester in the 17th Century; finally, the last one was used by Cardinal Wolsey in about 1524.

In the Middle Ages cryptography appears first as a method of concealing proper names, usually by the simple substitution of each letter by the next one in the alphabet, just about as Augustus Caesar did hundreds of years

before. At other times the vowels were replaced by dots, without changing the consonants--a method that was used throughout Europe to about 1000 A.D., when letters began to be replaced by various signs, by other letters, by letters from another language, by runes which are found in abundance in Scandinavia, and by arbitrary symbols. Here's an example of a runic inscription on a stone that stands before Gripsholm Castle near Stockholm, Sweden. The word rune means "secret".

Within a couple hundred years the outlines of modern cryptography began to be formed by the secret correspondence systems employed by the small Papal States in Italy. In fact, the real beginnings of systematic, modern cryptology can be traced back to the days of the early years of the 13th Century, when the science began to be extensively employed by the princes and chanceries of the Papal States in their diplomatic relations amongst themselves and with other countries in Europe. The necessity for secret communication was first met by attempts inspired by or derived from ancient cryptography, as I've outlined so far. There was a special predilection for vowel substitution but there appeared about this time one of the elements which was later to play a very prominent role in all cipher systems, an element we now call a syllabary, or a repertory. These were lists of letters, syllables, frequently-used parts of speech and words, with additions of arbitrary equivalents for the names of persons and places. There is still in existence one such syllabary and list of arbitrary

equivalents which was used about 1236 A.D. and there are other examples that were used in Venice in 1350.

Among examples of ciphers in medieval cryptography is a collection of letters of the Archbishop of Naples, written between 1363 and 1365, in which he begins merely with symbol substitutions for the vowels and uses the letters that are actually vowels to serve as nulls or non-significant letters to throw the would-be-cryptanalyst off the right track. As a final development, the high-frequency consonants L, M, N, R, and S, and all the vowels, are replaced not only by arbitrary symbols but also by other letters.

About 1378 an experienced cryptologist named Gabriele Lavinde of Parma was employed as a professional by Clement VII and in the Vatican Library there is a collection of ciphers devised and used by Lavinde about 1379. It consists of repertoires in which every letter is replaced by an arbitrary symbol. Some of these ciphers also have nulls and arbitrary equivalents or signs for the names of persons and places. There is a court cipher of Mantua dated 1395 that used this system.

At the beginning of the 15th Century the necessity of having variants for the high-frequency letters, especially the vowels, became obvious. Here is an alphabet of that period which is interesting because it shows that even in those early days of cryptology there was already a recognition of the basic weakness of what we call single or monoalphabetic substitution, that is, where every letter in the plain-text message is represented by another and always the same letter. Solution of this type of cipher, as many of you may know,

is accomplished by taking advantage of the fact that the letters of an alphabetic language are used with greatly differing frequencies. I don't have to go into that now because many of you, at some time or other, have read Edgar Allan Poe's "Gold Bug", and understand the principles of that sort of analysis. This slide clearly shows that the early Italian cryptographers understood the fact of varying frequencies and introduced stumbling blocks to quick and easy solution by having the high-frequency letters represented by more than a single character, or by several characters, as you see in this slide. I will add that the earliest tract that the world possesses on the subject of cryptography, or for that matter, cryptanalysis, is that which was written in 1474 by a Neapolitan, whose name was Sicco Simonetta. He set forth the basic principles and methods of solving ciphers, simple ciphers no doubt, but he describes them and their solution in a very clear and concise form.

Cipher systems of the type I've described continued to be improved. In this slide is shown what we may call the first complete cipher system of this sort. There are substitution symbols for each letter; the vowels have several equivalents; there are nulls; and there is a small list of arbitrary symbols, such as those for "the Pope", the word "and", the conjunction "with", and so on. This cipher, dated 1411, was used in Venice, and is typical of the ciphers used by the Papal chanceries of those days. ✓

The step remaining to be taken in the development of these ciphers was to expand the "vocabulary", that is, the list of equivalents for frequently-used words, and syllables, the names of persons and places, parts of speech, and so on. This step was reached in Italy during the first half of the 15th Century and became the prototype of diplomatic ciphers used in practically all the states of Europe for several centuries. Here is one of 70 ciphers collected in a Vatican codex and used from about 1440 to 1469. Note that the equivalents of the plain-text items in this slide are Latin words and combinations of two and three letters, and that they are listed in an order that is somewhat alphabetical but not strictly so. I suppose that by constant use the cipher clerk would learn the equivalents almost by heart, so that an adherence to a strict alphabetic sequence either for the plain-text items or for their cipher equivalents didn't hamper their operations too much. In this next slide there is much the same sort of arrangement, except that now the cipher equivalents seem to be digraphs and these are arranged in a rather systematic order, for ease in enciphering and deciphering. Now we have the real beginnings of what we call a one-part code, that is, the same list will serve both for encoding and decoding. These systems, as I've said, remained the prototypes of the cryptography employed throughout the whole of Europe for some centuries. The Papal States used them and as late as 1793 we find them used in France. I wish here to mention specifically the so-called King's General Cipher used in 1572 by the Spanish Court, and I show here a picture of it.

But there were two exceptional cases which show that the rigidity of cryptographic thought was now and then broken during the four centuries we have been talking about in this brief historical survey. Some of the Papal ciphers of the 16th Century and those of the French Court under Kings Louis XIII and XIV exemplify these exceptions. In the case of these French Court ciphers we find that a French cryptologist named Antonio Rossignol, who was employed by Cardinal Richelieu, understood quite well the weaknesses of the one-part codes and syllabaries. It was he who, in about 1648, introduced a new and important improvement, the idea of the two-part code or syllabary, in which for encoding a message the items in the vocabulary are listed in some systematic order, nearly always alphabetical; the code equivalents, whatever they may be, are assigned to the alphabetically-listed items in random order. This means that there must be another arrangement or book for ease in decoding, in which the code equivalents are listed in systematic order, numerically or alphabetically as the case may be, and alongside each appears its meaning in the encoding arrangement, or book. The significance of this improvement you'll find out sooner or later. Codes of this sort also had variants--Rossignol was clever, indeed. One such code, found in the 1691 correspondence of Louis XIV had about 600 items, with code groups of two and three digits. Not at all bad, for those days!

Now this sort of system would appear to be quite secure, and I suppose it was indeed so, for those early days of cryptographic development--but it



wasn't proof against the cleverness of British brains, for the eminent mathematician John Wallis solved messages in it in 1689. Never underestimate the British in this science--as we'll have reason to note in another lecture in this series.

French cryptography under Kings Louis XV and XVI declined, reaching perhaps its lowest level under Napoleon the Great. It is a fact that in Napoleon's Russian enterprise the whole of his army used by a single code book of only 200 groups, practically without variants, even for the high-frequency letters. Furthermore, not all the words in a message were encoded--only those which the code clerk or the writer of the message thought were important. It's pretty clear that the Russians intercepted and read many of Napoleon's messages--this comes from categorical statements to this effect by Czar Alexander I himself. We won't be far wrong in believing that the weaknesses of Napoleon's crypto-communications formed an important factor in Napoleon's disaster. A hundred and twenty-five years later, Russian ineptitude in cryptographic communications lost them the Battle of Tannenberg and knocked them out of World War I.

The other 16th Century Papal ciphers that constituted the second exception to the general similarity of cryptographic systems of those days were quite different from those I've shown you. In this exception the ciphers were monalphabetic, but some letters had the same equivalent, so that on decipherment the context had to be used to decide which of two or more

possible plain-text values was the one meant by each cipher letter. Here's a slide which shows one such cipher used by the Maltese Inquisitor in 1585. You'll note that the digit 0 has two values, A and T; the digit 2 has three values, U, V, and B, and so on. There were two digits used as nulls, 1 and 8; digits with dots above them stood for words such as Qua, Que, Qui, and so on.

Here's a slide which shows how a message would be enciphered, and also how one would be deciphered. A bit tricky, isn't it? Many, many years later Edgar Allan Poe describes a cipher of this same general type, where the decipherer must choose between two or more possible plain-text equivalents in building up his plain text, the latter guiding the choice of the right equivalent. The trouble with this sort of cipher is that you have to have pretty smart cipher clerks to operate it and even then I imagine that in many places there would be doubtful decipherments of words. It wasn't really a practical system even in those days but it could, if used skillfully and with only a small amount of text, give a cryptanalyst plenty of headaches. But such systems didn't last very long because of the practical difficulties in using them.

The first regular or official cipher bureau in the Vatican was established in about 1540, and in Venice at about the same time, about one hundred years before a regular cipher bureau was established in France by Cardinal Richelieu. It is interesting to observe that no new or remarkable ideas for cryptosystems were developed for a couple of hundred years after the complex ones I've

described as having been developed by the various Papal cryptologists. One-part and two-part syllabaries and simple or complex ones with variants were in use for many decades, but later on, in a few cases, the code equivalents were superenciphered, that is, the code groups formed the text for the application of a cipher, generally by rather simple systems of additives. Governmental codes were of the two-part type and were superenciphered by the more sophisticated countries.

The first book or extensive treatise on cryptography is that by a German abbot named Trithemius, who published in 1531 the first volume of a planned 4-volume monumental work. I said that he planned to publish four volumes; but he gave up after the third one, because he wrote so obscurely and made such fantastic claims that he was charged with being in league with the Devil, which was a rather dangerous association in those or even in these days. They didn't burn Trithemius but they did burn his books. This may be a good place to present a slide which shows that the necessity for secrecy in this business was recognized from the very earliest days of cryptology, and certainly by Trithemius. Here is the sort of oath that Trithemius recommended be administered to students in the science of cryptology. All of you have subscribed to a somewhat similar oath, but we now go further and back up the oath with a rather strict law. You've all read it, I'm sure.

We come now to some examples from more recent history. This slide shows a cipher alphabet used by Mary, Queen of Scots, who reigned from 1542 to 1567

and was beheaded in 1587. In this connection it may interest you to learn that question has been raised as to whether the Queen was "framed" by means of this forged postscript in a cipher that was known to have been used by her.

The Spanish Court under Phillip II, in the years 1555-1598, used a great many ciphers and here's one of them. You see that it is quite complex for those early days and yet ciphers of this sort were solved by an eminent French mathematician named Vieta, the father of modern algebra. In 1589 he became a Councelor of Parliament at Tours and then Privy Councelor. While in that job he solved a Spanish cipher system using more than 500 characters, so that all the Spanish dispatches falling into French hands were easily read. Phillip was so convinced of the security of his ciphers that when he found the French were aware of the contents of his cipher dispatches to the Netherlands, he complained to the Pope that the French were using sorcery against him. Vieta was called on the carpet and forced to explain how he'd solved the ciphers in order to avoid being charged with sorcery, a serious offense.

The next cryptologist I want you to know something about is another Italian savant who wrote a book, published in 1563, in which he showed certain types of cipher alphabets that have come down in history and are famous as Porta's Alphabets. Here's an example of the Porta Table, showing one alphabet with key letters A or B, another alphabet with key letters C

or D, and so on. I don't want to go into exactly how the key letters are used; it is sufficient to say that even to this day cryptograms using the Porta alphabets are occasionally encountered.

That Porta's table was actually used in official correspondence is shown by this slide, which is a picture of a table found among the state papers of Queen Elizabeth's time; it was used for communicating with the English Ambassador to Spain. Porta was, in my opinion, the greatest of the old writers on cryptology. I also think he was one of the early but by no means the first cryptanalyst able to solve a system of keyed substitution, that is, where the key is changing consistently as the message undergoes encipherment. Incidentally, Porta also was the inventor of the photographic camera, the progenitor of which was known as the camera obscura.

The next slide shows a picture of what cryptographers usually call the Vigenere Square, the Vigenere Table, or the Vigenere Tableau. It consists of a set of twenty-six alphabets successively displaced one letter per row, with the plain-text letters at the top of the square, the key-letters at the side, and the cipher letters inside. The method of using the table is to agree upon a key word, which causes the equivalents of the plain-text letters to change as the key changes. Vigenere is commonly credited with having invented that square and cipher but he really didn't and, what's more, never said he did. Here's a picture of his table as it appears in his book, the first edition of which was published in 1586. It is more complicated than as described in ordinary books on cryptology.

Here is one more example of another old official cipher. Here are the alphabets on a card which could be slid up and down, as a means of changing the key. Here is another, called the "two-square cipher", or "two-alphabet cipher". It is a facsimile of a State Cipher used in Charles the First's time, in 1627, for communicating with France and Flanders. It involves coordinates and I want you to notice that there are two complete alphabets inside it, intended to smooth out frequencies. The letters of the keywords OPTIMUS and DOMINUS serve as the coordinates used to represent the letters inside the square. Here's part of a cipher used by George III dated the 1st of September 1799.

One writer deserving special attention as a knowledgeable cryptologist in the 17th Century, and the one with whose cipher I'll close this lecture, is Sir Francis Bacon, who invented a very useful cipher and mentioned it for the first time in his Advancement of Learning, published in 1604, in London. The description is so brief that I doubt whether many persons understood what he was driving at. But Bacon described it in full detail, with examples, in his great book De Augmentis Scientiarum, which was published almost 20 years later, in 1623, and which first appeared in an English translation by Gilbert Wats in 1640 under the title The Advancement of Learning. Bacon called his invention the Bilateral Cipher and it is so ingenious that I think you should be told about it so that you will all fully understand it.

In his De Augmentis Bacon writes briefly about ciphers in general and

says that the virtues required in them are three: "that they be easy and not laborious to write; that they be safe, and impossible to be deciphered without the key; and lastly, that they be, if possible, such as not to raise suspicion or to elude inquiry." He then goes on to say: "But for avoiding suspicion altogether, I will add another contrivance, which I devised myself when I was at Paris in my early youth, and which I still think worthy of preservation." Mind you, this was 40 years later! Let's consult Bacon for further details. Here is a slide showing a couple of pages of the Gilbert Wats' translation of Bacon's De Augmentis Scientiarum. Bacon shows what he calls "An Example of a Bi-literarie Alphabet", that is, one composed of two elements, which, taken in groupings of fives, yields 32 permutations. You can use these permutations to represent the letters of the alphabet, says Bacon, but you need only 24 of them, because I and J, U and V, were then used interchangeably. These permutations of two different things--they may be "a's" and "b's", "1's" and "2's", pluses and minuses, apples and oranges, anything you please--can be used to express or signify messages. Bacon was, in fact, the inventor of the binary code which forms the basis of modern electronic digital computers. Bacon gives a brief example in the word "FUGE" --the Latin equivalent for our modern "SCRAM". Here it is, as you see. Here's another example, which quite obviously isn't what it appears to be--a crude picture of a castle, in which there are shaded and unshaded stones. It was drawn by a friend who was a physician and the

message conveyed by it is:

My business is to write prescriptions  
And then to see my doses taken;  
But now I find I spend my time  
Endeavoring to out-Bacon Bacon.

And here's another example, not quite so obvious. The message conveyed is:

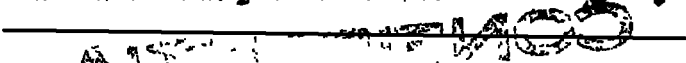
KNOWLEDGE IS POWER.

So far all this is simple enough--to much so, Bacon says, for the ✓  
example he used in the case of the word FUGE is patently cryptic and would  
not avoid suspicion under examination. So Bacon goes on to describe the next  
step, which is to have at hand a "Bi-formed Alphabet", that is, one in which  
all the letters of the alphabet, both capital and small, are represented by  
two slightly different forms of letters. Having these two different forms  
at hand, when you want to encipher your secret message you write another  
external and innocuous message five times as long as your secret message, using  
the appropriate two forms of letters to correspond to the "a's" and "b's"  
representing your secret message. Here's FUGE, enciphered within an external  
message saying "Manere te volo denac venero", meaning "Stay where you are  
until I come." In other words, whereas the real message says "SCRAM", the  
phony one says "Stick around awhile; wait for me." Bacon gives a much  
longer example, the SPARTAN DISPATCH; here it is, and here's the secret message  
which it contains.

Bacon's biliteral cipher is an extremely ingenious contrivance. There  
can be no question whatsoever about its authenticity and utility as a valid



cipher. Thousands of people have checked his long example and they all find the same answer--the one that Bacon gives.

Here's a modern example which uses two slightly different fonts of type  
  
 called Garamond and Imprint, and which are so nearly alike that it takes good eyes to differentiate them.

The fact that Bacon invented this cipher and described it in such detail lends plausibility to a theory entertained by many persons that Bacon wrote the Shakespeare Plays and that he inserted secret messages in those plays by using his cipher. If you'd like to learn more about this theory I suggest with some diffidence that you read a book entitled The Shakespearean Ciphers Examined. I use the word diffidence because my wife and I wrote the book which was published in late 1957 by the Cambridge University Press.

In the next lecture we'll take up cryptology as used during the period of the American Revolution by both the Colonial and the British Forces in America.

No 3 as revised

Insert for p.1

REF ID: A62852  
Information regarding the ~~war~~ and captives employed during that period has been rather sparse until quite recently, when a book entitled Jurcoats, Traitors and Heroes by Col John Bakeless, AUS, was published in 1959 by Hippincott. After a good many years of research Col. Bakeless brought together for the first time a good deal of authentic information on the subject and some of it is incorporated in this lecture.

According to Col. Bakers - and believe it  
or not I in early 1775 the British com-  
mander-in-chief in America, General  
Gage, had no code or cipher at all, nor  
even a staff officer who knew how to  
compile or devise one; he had to appeal  
to the commanding general in Canada,  
from whom he probably obtained the  
single substitution cipher which was  
used in 1776 by a British secret agent  
who - again, believe it or not - was

General Washington's own director-general  
of hospitals, Dr. Benjamin Church.  
General Washington had means for  
secret communication from the very be-  
ginning of hostilities, probably even be-  
fore the fighting began at Lexington  
and Concord. If the British under Gen-  
eral Gage were poorly provided in this  
respect, by the time Sir Henry Clinton  
took over from General Howe, who  
succeeded Gage, they were much

better off - they had adequate or  
REF ID: A62852  
apparently adequate means for secret  
communication.

## Summary

The third lecture in this series deals with the crypto-systems employed by the British Regulars and <sup>by</sup> the Colonials during the period of the American Revolution. This is followed by a brief explanation of the cryptanalytic nature of the initial breaks in the solution of the ~~age-old mystery~~ presented by the ancient Egyptian hieroglyphic writing.

LECTURE 3

(27)

Continuing [with] our survey of cryptologic history, the period of the American Revolution, in U.S. history, is naturally of considerable interest to us and warrants more than cursory treatment. <sup>^</sup> Are you astonished to learn that the systems used by the American colonial forces and by the British regulars were almost identical? You shouldn't be, because the language and backgrounds of both were identical. In one case, in fact, they used the same dictionary as a code book; something which was almost inevitable because there were, so few English dictionaries available. Here's a list of the [sort of] systems they used:

Insert

- (28)
- a. Simple, monoalphabetic substitution--easy to use and to change.
  - b. Monoalphabetic substitution with variants, by the use of a long key sentence. I'll show you presently an interesting example in Benjamin Franklin's system of correspondence with the elder Dumas.
  - c. The Vigenère cipher with repeating key.
  - d. Transposition ciphers of simple sorts.
  - e. Dictionaries employed as codebooks, with and without added encipherment. Two [such] were specially favored, [one,] Entick's "New Spelling Dictionary", the [other,] Bailey's English Dictionary. ~~Here I show~~ a couple of pages from

and/



Insert for p. 2

(1)

In the way REF ID: A62882 more complex than simple monoalphabetic substitution ciphers, the British under Clinton's command used a system described by Babbage in the following terms: "... a substitution cipher in which the alphabet was reversed, 'z' becoming 'a' and 'a' becoming 'z'. To destroy frequency clues, the cipher, changed in each line of the message, using 'y' for 'a' in the second line, 'x' for 'a' in the third, and so on. When the cipher clerk reached 's' in the middle of the alphabet, he started

[contin. over]

over again. A spy using this cipher did not have to carry <sup>REF ID: A62852</sup> ~~innumerable~~ papers, since the system was so easy to remember. The alphabets of this scheme are simple reversed standard sequences

(1a)

ABCDEFGHIJKLMN OPQRSTUVWXYZ

ZYXWUTSRQP ONMLKIHGFEDCBA

YXWUTSRQP ONMLKIHGFEDCBAZ

XWUTSRQP ONMLKIHGFEDCBAZY

ONMLKIHGFEDCBAZYXWUTSRQP

Butzless doesn't explain why the cipher sequences are only 12 in number — nor does the source from which he obtained the

information, a note found among the  
Clinton Papers REF ID: A62852 into Library at  
the University of Michigan.

Bates also continues:

- ② "Clinton also used another substitution cipher, with different alphabets for the first, second and third paragraphs. Even if an American cryptanalyst should break the cipher in one paragraph, he would have to start all over in the next. As late as 1781, however Sir Henry was using one extremely clumsy substitution cipher, in which 'a' was 51,

'd' was 54, 'e' 55. Judging that 51  
and 'd' was 50. I'd guess  
(correctly) that 'b' was 52, 'c' 53. Some-  
what more complex was his 'paper'  
cipher, in which twenty-five letters of the  
alphabet were placed in squares. Then  
an angle alone would represent a letter,  
the same angle with a dot another letter,  
the same angle with two dots still an-  
other. In some cases, cryptography was  
used only for a few crucial words in an  
otherwise clear message, a method also  
favored by certain American officials.

③

REF ID: A62852  
Of the first cipher mentioned in the preceding extract ~~there~~ much more to be said. Perhaps Bateless was limited by space considerations. In any case I will leave that story for another time and place. As for the second cipher Bateless mentions in the extract, I can give you the whole alphabet, for it exists among the Clinton Papers:

A B C D E F G H I K L M N O P Q R S T U W X Y Z  
51-52-53-54-55-60-61-62-63-64-65-66-67-68-69-70-71-72-73-74-75-76-77-78

There is no explanation why the

(3a) sequence beginning with 50 stops with E=55  
and then, started REF with ID: A62852, goes straight  
on without any break to Z=78. (Remember  
that in those days I and J were used inter-  
changeably, as were U and V).

Originally, as to what Bateles  
(and others) call the "pigpen" cipher, this  
is nothing but the rotary old so-called  
"Masonic" cipher based upon the 4-cross  
figure:  $\begin{array}{c} a|c| \\ \hline \\ \hline \\ \hline \\ \hline \end{array}$   $a = \perp, b = \lrcorner, c = \llcorner$

which can accommodate 27 characters, not  
25, as Bateles indicates. Letters can be inserted  
in the design in many different arrangements.

are shown in Fig. 1.

the former. To represent a word by code equivalent you simply indicated the page number, then whether Column 1 or Column 2 contained the word you wanted, and then the number of the word in the column. Thus: The word "jacket" would be represented by 178-2-2.

f. Small, specially compiled, alphabetic 1-part codes of 600-700 items and code names; our old friend the syllabary or repertory, of hoary old age *but* with new dress.

g. Ordinary books, such as Blackstone's on the Laws of England Commentaries, giving the page number, the line number and the letter number in the line, to build up, letter-by-letter, [by compound number] the word to be represented. Thus: 125-12-17 would indicate the 17th letter in the 12th line on page 125; it might be the letter T.

h. Secret inks.

i. Special designs or geometric figures, such as one I'll show you presently.

j. Various concealment methods, such as using *large feathers,* hollow quills of *or* hollowing out a bullet, and inserting messages written on very thin paper. Strictly speaking, however, this sort of stratagem doesn't belong to the field of cryptology. But it's a good dodge, to be used in special cases.

I've mentioned that code or conventional names were used to represent the names of important persons

and places in these American colonial and British

cryptograms of the Revolution. Here are ~~some~~ examples taken from a system of code names prepared by Major André, of the sort of names the British used as code names: *the British Spy, Chief of Intelligence under General Clinton:*

For American Generals - The names of the Apostles, for instance:

General Washington was "James"

General Sullivan was "Matthew"

Names of Cities Philadelphia - Jerusalem

X Detroit - Alexandria

Names of Rivers and Bays (Susquehanna - Jordan

(Delaware - Red Sea

Miscellaneous: Indians - Pharisees

Congress - Synagogue

*Inset*  
Names of Forts:  
Fort Wyoming - Sodom  
Fort Pitt - Gomorrah

*In Fig. 7, we see*

~~Here's a very interesting slide, a British cipher message of the vintage 1781. It was deciphered before finding the key, always a neat trick when or if you can do it. Here's the key--the title page of the then current British Army List - is shown in Fig. 8.~~

I'm sure you've learned as school children all about the treasonable conduct of Benedict Arnold when he was in command of the American Forces at West Point; but you probably don't know that practically all his exchanges of communications with Sir Henry Clinton, Commander of the British Forces in America, were in cipher, or in invisible inks. ~~Here's an interesting slide showing one of Arnold's cipher messages, in~~



Insert for p 4

Fig 2a being the secret version, Fig. 2b, the plain text. Arnold left a few words clear, the ones he considered unimportant; for the important ones he used a dictionary as a codebook, indicating the page number, column number and line number corresponding to the position in the dictionary of the plain-text word which the code group represents. Arnold added 7 to these numbers, which accounts for the fact that first number in a code group is never less than 8, the central number is always either 8 or 9, and the third number is never less than 8 or more than 36. The significant sentence appears near the middle of the

message: " If 198.9.34, 185.8.31 or 197.8.8... " REF ID: A62852  
yields the plain text: " point out a plan of  
cooperation by which S.H. [Sir Henry Clinton]  
shall possess himself of West Point, the  
Garrison, etc, etc, etc, of twenty thousand  
pounds Sterling I think will be a cheap  
purchase for an object of so much importance."  
The signature 172.9.19 probably stands for  
the word "Moor"; Arnold's code name in these  
communications was <sup>John</sup> "Moore". He had also  
another name, "Gustavus".

Fig. 3 at the top shows the code message; at  
the bottom is <sup>REF ID: A62852</sup> the main part. Arnold used  
the same additive as in the preceding  
example.

Insert #2 for p. 4

Insert #3 for p.4

REF ID: A62852

In Fig. 1 the left-hand portion shows the "phony" message, the right-hand one, the real message. To make it easy for the reader I give below in typed form both the "phony" and the ~~secret~~ ~~code~~, the latter being underlined words having small rectangular apertures etc

REF ID: A62852

Explain how ~~you~~ <sup>it</sup> is ~~in~~ <sup>in</sup> ~~the~~ <sup>the</sup> ~~list~~ <sup>list</sup>

1  
:  
1

Insert #1  
attached

which he offers to give up West Point for £20,000,  
is shown in Fig. 3. ~~Figure 3 is a message~~  
~~Here's another one in which he gave the British~~

information which might have led to the capture of

Insert  
#2 attached

his commander-in-chief, General Washington, ~~however,~~  
Washington, however, was too smart to be ambushed--he went by  
a route other than the one he said he'd take.

You may find ~~this next slide~~ <sup>Fig. 4</sup> interesting as  
an example of the special sort of mask or grille used  
by Arnold and by the British in their negotiations  
with him. The real or significant text is written  
in lines outlined by an hour-glass figure and then dummy  
words are supplied to fill up the lines so that the  
entire letter apparently makes good sense. To read  
the secret message you're supposed to have the same  
size hour-glass figure that was used to conceal the  
message. The significant text in this example is

underlined:

"You will have heard, Dr. Sir I doubt not <sup>long</sup> ~~only~~  
<sup>this</sup> before you can have reached you that Sir W. Howe  
is gone from hence. The rebels imagine that  
he is gone to the Southward ~~by this time~~  
However he has filled Chesapeake Bay with  
surprise and terror...etc."

l.c.

Ⓞ  $\frac{1}{m}$  sp

l.c.

Arnold even used the trick, mentioned above in  
method j, that was quite similar to one used recently

Insert for p. 5, transferred matter from p. 3.

REF ID: A62852  
The numbers in the line of a key text, the first series of numbers, viz, 22.6.7.39.5.9.17, indicating line number 22, letter numbers 6.7.39.5.9.17 in that line. Because of the many repetitions the plain text was obtained by straightforward analysis by an officer presently on duty in NSA, Capt Edward W. Knepper, <sup>US.N.</sup> to whom I am indebted for this interesting example.  
over

REF ID: A62852  
The plain text, once obtained, gave him clues to what the ~~key~~ text might be, simply by replacing the plain-text letters in their numerical equivalent order in the putative key text. This done, Capt. Knappen was quick to realize what the key text was: An Army List. The date of the message enabled him to find the list without much difficulty in the Library of Congress.



Insert for page 72

5 An interesting episode involving concealment of this sort is <sup>REF ID: A62852</sup> ~~recounted~~ ~~by the~~ Babelss, ~~in his recently published book~~ ~~concerning~~ ~~Spain and Greece~~. An urgent message of Sir Henry Clinton, dated 8 October 1777, and written on thin silk, was <sup>48</sup> concealed in an oval <sup>silver</sup> ball, about the size of a rifle bullet, which was "handed to Daniel Taylor, a young officer who had been promised promotion if he got through alive. The bullet was made of silver, so that the spy could swallow it without injury from corrosion. . . . Almost as soon as he started, Taylor



It is often referred to as "The Benedict Arnold's" Treasonable Cow Letter.

(Fig 5)

Quint attached

by the Russian spy, Colonel Abel, who was arrested in New York in June 1957, tried and convicted, and is still languishing in a Federal prison. Here's a picture of the gentleman. How would you like to meet up with

~~him suddenly some dark night at a secret rendezvous?~~

We next see (Fig. 6) one Benedict Arnold message that never was deciphered. Only one example is extant; certain words have

Present matter from p. 3 here

purely arbitrary meanings, as prearranged.

There was an American who seems to have been the Revolution's one-man National Security Agency, for he was the one and only cryptologic expert Congress had, and, it is claimed, he managed to decipher nearly all, if not all, of the British code messages obtained in one way or another by the Americans. Of course, the chief way in which enemy messages could be obtained in those days was to capture couriers, knock them out or knock them off, and take the messages from them. This was very rough stuff, compared to getting the material by radio intercept, as we do nowadays.

I think you'll be interested to hear a bit more about that one-man NSA. His name was James Lovell and besides being a self-trained cryptologist, he was also a member of the Continental Congress. There's on record a very interesting letter which he wrote to General Nathaniel Greene, with a copy to General Washington. Here it is.

Philadelphia, Sept. 21, 1780

1/

Sir:

*underline* You once sent some papers to Congress which no *underline*  
one about you could decipher. Should such be the  
 case with some you have lately forwarded I presume that  
 the result of my pains, herewith sent, will be useful  
 to you. I took the papers out of Congress, and I do  
 not think it necessary to let it be known here what  
 my success has been in the attempt. For it appears  
 to me that the Enemy make only such changes in their  
 Cypher, when they meet with misfortune, ~~as~~ makes a  
 difference <sup>of</sup> ~~in~~ position only to the same alphabet,  
 and therefore if no talk of Discovery is made by ~~me~~ *us*  
 here or by your Family, you may be in chance to  
 draw Benefit this campaign from my last Night's  
 watching.

I am Sir with much respect.

Your Friend,

JAMES LOVELL

*Maj. Genl. Greene  
 (with copy to Genl. Washington)*

In telling you about Lovell I should add to my  
 account of that interesting era in cryptologic history  
 an episode I learned about only recently. When a certain  
 message of one of the generals in command of a rather  
 large force of Colonials came into Clinton's  
 possession he sent it off post haste to London for

OK

solution. Of course, Clinton knew it was going to take a lot of time for the message to get to London, be solved and returned to America--and he was naturally a bit impatient. He felt he couldn't afford to wait that long. Now it happened that in his command there were a couple of officers who fancied themselves to be cryptologists and they undertook to solve the message, a copy of which had been made before sending the original off to London. Well, they gave Sir Henry their solution and he acted upon it. The operation turned out to be a dismal failure, because the solution of the would-be-cryptanalysts happened to be quite wrong! The record doesn't say what Clinton did to those two unfortunate cryptologists when the correct solution arrived from London some weeks later. By the way, you may be interested in learning that the British operated a regularly-established cryptanalytic bureau as early as in the year 1630 and it continued to operate until the end of July 1844. Then there was no such establishment until World War I. I wish there were time to tell you some of the details of that fascinating and little known bit of British history.

There's also an episode I learned about only very recently, which is so amusing I ought to share it with you. It seems that a certain British secret

agent in America was sent a message in plain English, giving him instructions from his superior. But the poor fellow was illiterate and there wasn't anything to do but call upon the good offices of a friend to read it to him. He found such a friend, who read him his instructions. What he didn't know, however, was that the friend who'd helped him was one of General Washington's secret agents!

*illustration (Fig. 9) is*  
 The next ~~slide~~ <sup>^</sup> shows a picture of one of several syllabaries used by Thomas Jefferson. It is constructed on the so-called two-part principle which was explained in the preceding lecture. *Figure 9 a* <sup>^</sup> is a portion of the encoding section, and *9 b* <sup>^</sup> is a portion of the decoding section, in which the code equivalents are in numerical order accompanied by their meanings as assigned them in the encoding section. This sort of system, which, as I've already explained, was quite popular in Colonial times as in the early days of Italian cryptography, is still in extensive use in some parts of the world. Jefferson was an all-around genius, and I shall have something to say about him and cryptography in a subsequent lecture.

A few minutes ago I mentioned Benjamin Franklin's cipher system, which, if used today, would be difficult to solve, especially if there were only a small amount of traffic in it. Let me show you what it was.

Franklin took a rather lengthy passage from some book in French and numbered the letters successively. These numbers then became equivalents for the same letters in a message to be sent. Because the key passage was in good French, naturally there were many variants for the letter E--in fact, there were as many as one would expect in normal plain-text French; the same applied to the other high-frequency letters such as R, N, S, I, etc. What this means, of course, is that the high-frequency letters in the plain text of any message to be enciphered could be represented by many different numbers and a solution on the basis of frequency repetitions would be very much hampered by the presence of many variant values for the same plain-text letter. *In Fig. 10* ~~Here you~~ can see this very clearly.

I know of but one case in all our U.S. history in which a resolution of Congress was put out in cryptographic form. *It is shown in Fig. 11 --* ~~Here's a slide which shows it--~~

a resolution of the Revolutionary Congress dated

8 February 1782. *I have in my collection not only a copy of the resolution but also a copy of the syllabary which it can be deciphered.*

Interest in cryptology in America seems to have died with the passing of Jefferson and Franklin. But if interest in cryptology in America wasn't very great, if it existed at all after the Revolution, this was not the case in Europe. Books on the subject were written, not by professionals, perhaps, but by learned

amateurs, and I think you will find some of them in the NSA library if you're interested in the history of the science. <sup>The next illustration (Fig. 12) is</sup> Here's the frontispiece of a French book the title of which I translate as "Counter-<sup>communications</sup> espionage, or keys for all secret <sup>correspondence."</sup> <sup>is/</sup> It was published in Paris in 1793. <sup>In the picture we see</sup> Here's Dr. Gryppy himself, and ~~this is~~ perhaps a breadboard model of a GS-11 research analyst, or maybe an early model of a WAC.

I am going to take a bit of time now to tell you something about Egyptian hieroglyphics, not only because I think that that represents the next <sup>^</sup> and <sup>1</sup> a great <sup>^</sup> landmark in the history of cryptology, but also because the story is of general interest to any aspiring cryptologist. About 1821 a Frenchman, Champollion, startled the ~~unscholarly~~ world by beginning to publish translations of Egyptian hieroglyphics, although in the budding new field of Egyptology much had already transpired and been published. <sup>In Fig. 13 we see</sup> ~~Here's a picture of~~ the gentlemen and <sup>in Fig. 14</sup> ~~here's a picture~~ of the great Napoleonic find that certainly facilitated and perhaps made possible the solution of the Egyptian hieroglyphic writing--the Rosetta Stone, <sup>The Rosetta Stone</sup> ~~which~~ was found in 1799 at Rashid, or, as the Europeans call it, Rosetta, a town in northern Egypt on the west bank of the Rosetta branch of the Nile. Rosetta was in the vicinity of Napoleon's operations which ended in disaster and when the peace treaty was written



Article <sup>16</sup>~~XVI~~ of it required that the Rosetta Stone, the  
 significance of which was quickly understood by both  
 the conquered French and victorious British commanders,  
 be shipped to London, together with certain other  
 large antiquities. The Rosetta Stone still occupies  
 a prominent place in the important exhibits at the  
 British Museum. The Rosetta Stone is a bi-lingual  
 inscription, because it is in Egyptian and also Greek.  
 The Egyptian portion consists of two parts, the upper  
 one in hieroglyphic form, the lower one in a sort of  
 cursive script, also ~~in~~ Egyptian but called "Demotic."  
 It was soon realized that all three texts were  
 supposed to say the same thing, of course, and since  
 the Greek could easily be read it served as what in  
 cryptanalysis we call a "crib." Any time you are  
 lucky enough to find a crib it saves you hours of work.  
 It was by means of this bi-lingual inscription that  
 the Egyptian hieroglyphic writing was finally solved,  
 a feat which represented the successful solution  
 to a problem the major part of which was linguistic  
 in character. The cryptanalytic part of the task was  
 relatively simple. Nevertheless, I think that anyone  
 who aspires to become a professional cryptologist should  
 have some idea as to what that cryptanalytic feat  
 was, a feat which some professor--but not of cryptologic  
 science, I think it was Professor Norbert Wiener, of

the Massachusetts Institute of Technology--said was the greatest cryptanalytic feat in history. We shall see how wrong the good professor was, because I'm going to demonstrate just what the feat really amounted to by showing you some simple pictures.

First, let me remind you that the Greek text served as an excellent crib for the solution of both Egyptian texts, the hieroglyphic and the Demotic, the latter merely being the conventional abbreviated and modified form of the Hieratic character or cursive form of hieroglyphic writing that was in use in the Ptolemaic Period.

The initial step was taken by a Reverend Stephen Weston who made a translation of the Greek inscription which he read in a paper delivered before the London Society of Antiquaries in April 1802.

In 1818 Dr. Thomas Young, the physicist who first proposed the wave theory of light, compiled for the 4th volume of Encyclo<sup>a</sup>pædia Britannica, published in 1819, the results of his studies on the Rosetta Stone and among them there was a list of several alphabetic Egyptian characters to which, in most cases, he had assigned correct values. He was the first to grasp the idea of a phonetic principle in the Egyptian hieroglyphs and he was the first to apply it to their

decipherment. He also proved something which others had only suspected, namely, that the hieroglyphs in ovals or cartouches were royal names. But Young's name is not associated in <sup>the</sup> public mind with the decipherment of Egyptian hieroglyphics--that of Champollion is very much so. Yet much of what Champollion did was based upon Young's work. Perhaps the greatest credit should go to Champollion for recognizing the major importance of an ancient language known as Coptic as a bridge that could lead to the decipherment of the Egyptian hieroglyphics. As a lad of seven he'd made up his mind that he'd solve the hieroglyphic writing and in the early years of the 19th Century he began to study Coptic. In his studies of the Rosetta Stone his knowledge of Coptic, a language the knowledge of which had never been lost, enabled him to deduce the phonetic value of many syllabic signs, and to assign correct readings to many pictorial characters, the meanings of which became known to him from the Greek text on the Stone.



The following step-by-step account of the solution is taken from a little brochure entitled The Rosetta Stone, published by the Trustees of the British Museum. It was written in 1922 by E. A. Wallis Budge and was revised in 1950. I quote:

"The method by which the greater part of the Egyptian alphabet was recovered is this: It was assumed correctly that the oval , or "cartouche" as it is called, always contained a royal name. There is only one cartouche (repeated six times with slight modifications) on the Rosetta Stone, and this was assumed to contain the name of Ptolemy, because it was certain from the Greek text that the inscription concerned a Ptolemy. It was also assumed that if the cartouche did contain the name of Ptolemy, the characters in it would have the sounds of the Greek letters, and that all together they would represent the Greek form of the name of Ptolemy. Now on the obelisk which a certain Mr. Bankes had brought from Philae there was also an inscription in two languages, Egyptian and Greek. In the Greek portion of it two royal names are mentioned, that is to say, Ptolemy and Cleopatra, and on the second face of the obelisk there are two cartouches, which occur close together, and are filled with hieroglyphs which, it was assumed, formed the Egyptian equivalents of these names. When these cartouches were compared with the cartouche on the Rosetta Stone it was found that one of them contained hieroglyphic characters that were almost identical with those which filled the cartouche on the Rosetta Stone. Thus there was good reason to believe that the cartouche on the Rosetta Stone contained the name of Ptolemy

written in hieroglyphic characters. The forms of the cartouches are as follows:

On the Rosetta Stone

On the Obelisk from Philae

In the second of these cartouches this single sign  ~~(point it out)~~ takes the place of these three signs  ~~(point the out)~~ at the end of the first cartouche.

Now it has already been said that the name of Cleopatra was found in Greek on the Philae Obelisk, and the cartouche which was assumed to contain the Egyptian equivalent to this name appears in this form:

Taking the Cartouches which were supposed to contain the names of Ptolemy and Cleopatra from the Philae Obelisk, and numbering the signs we have:

Ptolemy, A.

Cleopatra, B.

Now we see at a glance that No. 1 in A and No. 5 are identical, and judging by their position only in the names they must represent the letter P. No. 4 in A and No. 2 in B are identical, and arguing as before from their position, they must represent the letter L. As L is the second letter in the name of Cleopatra, the sign No. 1 ~~(point)~~ must represent K. Now in the cartouche of Cleopatra, we know the values of Signs Nos. 1, 2 and 5, so we may write them down thus:


In the Greek form of the name of Cleopatra there are two vowels between the L and the P, and in the hieroglyphic form there are two hieroglyphs, this ~~(point)~~ } and this ~~(point)~~, so we may assume that ~~this~~ <sup>the first</sup> is E and ~~this~~ <sup>the other</sup> is O. In some forms of the cartouche of Cleopatra, No. 7 (the hand) is replaced by a half circle, which is identical with No. 2 in A and No. 10 in B. As T follows P in the name Ptolemy, and as there is a T in the Greek form of the name of Cleopatra, we may assume that the half circle and the hand have substantially the same sound, and that that sound is T. In the Greek form of the name Cleopatra there are two a's, the positions of which agree with No. 6 and No. 9, and we may assume that the bird has the value of A. Substituting these values for the hieroglyphs in B we may write it thus:

Thomas Young noticed that these two signs <sup>o and o</sup> always followed the name of a goddess, or queen, or princess, and the other early decipherers regarded the two signs as a mere feminine termination. The only sign for which we have no phonetic equivalent is No. 8, the lens, and it is obvious that this must represent R. Inserting this value in the cartouche we have the name of Cleopatra deciphered. Applying now the values which we have learned from the cartouche of Cleopatra

2/ to the cartouche of Ptolemy, we may write it thus:

We now see that the cartouche must be that of Ptolemy, but it is also clear that there must be contained in it many other hieroglyphs which do not form part of his name. Other forms of the cartouche of Ptolemy are found, even on the stone, the simplest of them written thus:

~~(point out on slide)~~

 It was therefore evident that these other signs were royal titles corresponding to those found in the Greek text on the Rosetta Stone meaning "ever-living, beloved of Ptah." Now the Greek form of the name Ptolemy, i.e. Ptolemaios, ends with S. We ~~say~~ assume therefore that the last sign <sup>(CP)</sup> in the simplest form of the cartouche given above has the phonetic value of S. The only hieroglyphs now doubtful are ~~(this)~~ and ~~(this)~~, and their position in the name of Ptolemy suggests that their phonetic values must be M and some vowel sound in which the I sound predominates. These values, which were arrived at by guessing and deduction, were applied by the early decipherers to other cartouches, e.g.:

Now, in No. 1, we can at once write down the values of all the signs, viz., P. I. L. A. T. R. A, which

is obviously the Greek name Philotera. In No. 2 we know only some of the hieroglyphs, and we write the cartouche thus: It was

known that the running-water sign <sup>(running)</sup> occurs in the name Berenice, and that it represents B, and that this sign <sup>(B)</sup> is the last word of the transcript of the Greek title "Kaisaros," and therefore represents some S sound.

Some of the forms of the cartouche of Cleopatra begin with ~~(this sign)~~, and it is clear that its phonetic value must be K. Inserting these values in the above cartouche we have:

which is clearly meant to represent the name "Alexandros," or Alexander. The position of this sign <sup>(A)</sup> ~~(print)~~ shows that it represented some sound of E or A.

Well, I've showed you enough to make fairly clear what the problem was and how it was solved.

That's the way in which the initial break was made in the decipherment of Egyptian hieroglyphics, and, as you may already have gathered, the cryptanalysis was of a very simple variety. It was very fortunate that the first attacks on Egyptian hieroglyphics didn't have to deal with enciphered writing. Yes, the Egyptians also used cryptography; there are "cryptographic hieroglyphics!" Here, <sup>in Fig. --</sup> for instance, is an example of



Insert for p. 19

The following <sup>REF ID: A62852</sup> is a long article by Étienne Drouot in "Revue D'Égyptologie", Paris, 1933. It is subtitled "Essai sur la cryptographie privée de la fin de la XVIII<sup>e</sup> dynastie" and I quote from page 14 thereof:

"Finally, the playful tendency, already pointed out in the construction of the alphabet, appears in the orthography. Certain groups offer, when

REF ID: A62852  
read in clear, a fallacious meaning;  
they are intentional traps, and em-  
phasize the enigmatic character of this  
cryptography:

Fig. 17

*Insert attached*

substitution. ~~That character in place of this one means "to speak."~~

Before leaving the story of Champollion's mastery of Egyptian hieroglyphic writing I think I should re-enact for you as best I can in words what he did when he felt he'd really reached the solution to the mystery. I'll preface it by recalling to you what Archimedes is alleged to have done when he solved a problem he'd been struggling with for some time. Archimedes was enjoying the pleasures of his bath and was just stepping out of the pool when the solution of the problem came to him like a flash. He was so overjoyed that he ran, naked through the streets shouting "Eureka! I've found it, I've found it." *d/* Well, likewise, when young Champollion one day had concluded he'd solved the mystery of the Egyptian hieroglyphics, he set out on a quick mile run to the building where his lawyer brother worked, stumbled into his brother's office, shouted: "Eugene, I've got it!", and flopped down to the floor in a trance where he is said to have remained immobile and completely out for five days. Don't let that sort of thing happen to you around here when and if you find the answer to a complex problem. The char force will probably sweep you up and throw you into the secret trash bin ~~for disposition by burning.~~

I shouldn't leave this brief story of the crypt-analytic phases of the solution of the Egyptian hieroglyphic writing without telling you that there remain plenty of other sorts of writings which some of you may want to try your hand at deciphering when you've learned some of the principles and procedures of the science of cryptology. A list of thus-far undeciphered writings was drawn up for me by Professor Alan C. Ross of London University in 1945 and had 19 of them. Since 1945 only two have been deciphered, Minoan Linear A and Linear B writing. The Easter Island writing is said to have very recently been solved, but I'm not sure of that. There are some, maybe just a very few, who think the hieroglyphic writing of the Ancient Maya Indians of Central America may fall soon, but don't be too sanguine about that, either.

Should any of you be persuaded to tackle any of the still undeciphered writings in the list drawn up by Professor Ross, be sure you have an authentic case of an undeciphered language before you. Here's one that was written on a parchment, known as the Michigan Papyrus. It had baffled certain savants who had a knowledge of Egyptology who attempted to read it on the theory that it was some sort of variation--a much later modification--of Egyptian hieroglyphic writing. These old chaps gave it up as

Insert for p. 21

REF ID: A62852

The next period of importance in this brief account of the history of cryptology is the one which deals with the codes and ciphers used by the contestants in our Civil War, the period 1861-65. It is significant and important because, for the first time in history, rapid and secure communications on a large scale became practicable in the conduct of organized warfare.

and world-wide diplomacy. They became  
practicable ~~when~~ <sup>REF ID: A62852</sup> ~~the~~ <sup>technology</sup> and  
telegraphy were joined in happy,  
sometimes contentious, but long-  
lasting wedlock.

a bad job. Not too many years ago it came to the attention of a young man who knew very little about Egyptian hieroglyphics. He saw it only as a simple substitution cipher on some old language. He tackled the Michigan Papyrus on that basis and solved it. He found the language to be early Greek. And what was the purport of the writing? Well, it was a wonderful old Greek beautician's secret formulae for further beautifying lovely Greek young beauties--maybe the bathing beauties of those days.

27/ b1

insert

There is one person I should mention <sup>however,</sup> before coming to the period of the Civil War, ~~or, as some people prefer to call it, the war between the States, in U. S. history.~~ I refer here to Edgar Allan Poe, who

in 1842 or thereabouts, kindled an interest in cryptography in newspapers and journals of the period. <sup>both at home and abroad</sup> For his day he was certainly the best informed person in this <sup>Country</sup> U. S. on cryptologic matters outside <sup>of</sup> the regular employees of Government departments interested in the subject, and in saying this I am assuming that cryptology was used ~~to a limited extent~~ by our Department of State for communicating with ambassadors and consuls abroad.

27/

omit,

I suppose that the Army and Navy used codes <sup>and ciphers after the Revolution</sup> but the record is a bit fragmentary, and I won't be able to ~~we'll come to them a little later, when I'll show you examples of them.~~

To return to Poe, one of our early columnists, there's an incident I'd like to tell you about in connection with a challenge he printed in one of his columns, in which he offered to solve any cipher submitted by his readers. He placed some limitations on his challenge, which amounted to this--that the challenge messages should involve but a single alphabet, ~~with variants~~. In a later article Poe tells about the numerous challenge messages sent him and says: "Out of perhaps 100 ciphers altogether received, there was only one which we did not immediately succeed in resolving. This one we demonstrated to be an imposition--that is to say, we fully proved it a jargon of random characters, having no meaning whatever." I wish that cipher had been preserved for posterity, because it would be interesting to see what there was about it that warranted Poe <sup>to state</sup> in saying that "we fully proved it a jargon of random characters." Maybe I'm not warranted in saying of this episode that Poe reminds me of a ditty sung by a character in a play put on by some undergraduates of one of the colleges of Cambridge University, in England. <sup>At a certain point in the play,</sup> This character steps to the front of the stage and sings:

"I am the Master of the College,  
What I don't know ain't knowledge."



Insert for p. 23

REF ID: A62852

If ~~any~~ you are interested sufficiently  
to wish to learn ~~to~~ something about  
Poe's contributions to cryptology, I  
refer you to a very fine article by  
Prof W.K. Wimsatt, Jr., entitled "What  
Poe knew about cryptography", Publications  
of the Modern Language Association of  
America, New York, Vol LVIII, No. 3,  
September 1943, pp 754-79 In ~~it~~ it you'll  
find references to what I have published  
on the same subject.

Thus, Poe. What he couldn't solve <sup>he couldn't</sup> wasn't a real cipher--  
a very easy out for any cryptologist up against something  
tough.

*Just attached* → This completes the third lecture in this series.

In the next one we shall come to that interesting period  
in cryptologic history in which codes and ciphers were  
used in this country in the War of the Rebellion,  
the War Between the States, the Civil War--you use your  
own pet designation for that terrible and costly struggle.

*This was  
talked over  
the preliminary  
at Annapolis ca*

REF ID: A66639  
1929

7

In the brief time at my disposal this afternoon, it will be impossible to touch upon all phases of code work. Hence I shall confine myself chiefly to those phases which will probably at some future time concern most of those present; namely, the safeguards and precautions which must be observed in code or cipher operations in order to maintain the secrecy of the system of communication adopted.

A preliminary word of explanation with regard to the two terms "Code" and "Cipher" may be necessary. To most of you, the two words mean practically the same thing, but such is not the case. Modern cryptography draws a rather sharp distinction between the two terms.

A CIPHER, taken in a broad sense, is the name applied to any system of cryptography which involves the transformation of the individual letters of the original, intelligible text of a message into a secret or unintelligible form by means of previously established agreements which subsequently permit of the reconstruction of the original text from the secret text.

The original, intelligible text of the message is called the PLAIN TEXT. The resultant unintelligible or secret text is called the CIPHER TEXT.

The operation of transforming the Plain Text into the equivalent Cipher Text is called Enciphering; the reverse operation is called Deciphering.

A CODE is the name applied to a specialized system of cryptography which involves the transformation of the original, intelligible plain text of a message into a secret or unintelligible form by means of a book or a document which gives conventional words, or uniform, arbitrary combinations or numbers as the equivalents of not only the letters, but also the words, phrases, or entire sentences of the original text. It is obvious that identical copies of the Code or Code book must be in the possession of the correspondents. The operations which apply to this system are called ENCODING and DECODING.

While there are some ciphers which resemble code or tend to approach code, yet the distinction which exists and which should be made between cipher and code is this: in cipher one deals with the individual letters as units; in code, while one may deal occasionally with the individual letters, the operation is

-2-

principally concerned with the phrases or sentences taken as units.

When the code designations of the encoded words of a message are afterwards enciphered, or in other words, when a message is first encoded and then the code equivalents are enciphered, the result is called ENCIPHERED CODE. For example, if the code word for the phrase, "By order of the Commander-in-Chief" is POBAL, and if this code word is then enciphered into the form CITAX or into the number 17521, the latter is then known as enciphered code.

So far as I am aware, a system of secret communication which is absolutely impregnable against solution by the enemy and which at the same time is suited to the needs of naval, military, or diplomatic offices, is not known to the science of cryptography. I do not know how sufficiently to impress upon your minds the necessity for exercising the most rigid and painstaking care in the use of the codes or ciphers which may at some future time be entrusted to you. I have seen elaborate code and cipher systems rendered absolutely valueless through the carelessness and ignorance of one man. From the point of view of the Intelligence Department it seems to me that a man who flagrantly disregards or violates the rules and regulations laid down by the Code and Signal Section is as deserving of the extreme punishment for a breach of discipline resulting in the actual or potential loss of life of his comrades as is the man who consciously betrays them by furnishing information to the enemy. Let me tell you of one instance which to my knowledge had disastrous consequences.

You will recall that in March 1918 the Germans launched their last and greatest offensive on the Western front. Careful preparations and provision had been made for nearly everything. On the day of the opening of the offensive an absolutely new type of code went into effect in every sector simultaneously on the whole front. Months of work by the allied intelligence department upon the German trench code were rendered worthless at one stroke. We had to begin all over again and while the general situation on the whole battle front looked very dark, during those critical weeks, things looked especially dark to the members of the code and cipher section.

Among the very first messages, in the new code that were intercepted by our own Signal Corps was a set of three messages passing between two stations opposite the front held by the American forces. Here they are \*\*\*\*\*

This solution was of vastly greater importance than is apparent on the face of the decoded message. The message itself meant, for us, at least nothing. Even to this day I can only surmise what it meant. But the most important feature

\*  
See  
page  
133  
Elements  
of Cryptanalysis

of the message was that it at once gave definite clues with regard to the nature and mechanics of the new system. Certain features of the groups in this message led to the making of some assumptions which were tested upon other messages; they proved to be correct. At one blow the whole new system fell like a house of cards.

I have said that this message meant nothing to us; it may have meant but very little more to the Germans between whom the message was exchanged. But this message led to the breaking of the whole code. Certainly the German operator would not have committed this inexcusable blunder had the message been of great tactical importance. But for the code solver all messages are of equal importance - and most often the messages of least consequence as regards the tactical situation, yield the most far reaching results, and are therefore the most disastrous as far as maintaining the secrecy of the code is concerned. (Practice messages) *One of the German radio operators used to send regularly at 6:45 AM in code the proverb "Morgen stunde wie die rade in German service" - "The best time to get in your work is when it is first done."*

I might add that to complete the dramatic situation resultant upon the solution of this first message, the news, together with the date, was sent to the general head quarters of our allies by special aeroplane because at that time direct telegraphic communication between the American and the other code offices had not yet been established. *and called the worm; this gave us lots of clues when a new cipher was used.*

How many of his comrades lost their lives as a direct result of this one German's blunder, no one can say. He was guilty of violating one of the most important rules of code work, namely, a message once transmitted in code or cipher must NEVER be repeated in any other form whatsoever.

If it must be repeated because of mutilation or garbles, an exact duplicate of the original code or cipher text must be sent. If after several repetitions the message is still unintelligible, because of a failure on the part of the receiving station to be in possession of the necessary data for decodement, then it may be necessary to transmit the message in another form. Whatever this second form be, it should bear no resemblance whatsoever to the first message as regards internal form of the plain text which has been encoded or enciphered. In other words, the plain text of the original message must be altered in form to the greatest extent possible, consistent with the intent and meaning of the message. This process of altering the plain contents of a message for the purpose of changing its form, without material change in meaning, so that a close comparison between the plain text and its equivalent code or cipher text will be impossible, is called PARAPHRASING. I shall refer to it later. As far as possible no information should ever be given in any

plain text communication, code, or cipher message which may connect it in any way with a message previously sent. Of course, I need hardly add that a message once sent in code or cipher must never be repeated in plain text under any circumstances - there is no exception to this rule. The danger of such a procedure is so obvious that it is hard to conceive of any normal thinking person doing it. Yet, let me tell you of an actual instance.

(Case 2) *I can't recall it at the moment.*

It seems hardly necessary to say that the insertion of plain text in code or cipher text is so highly dangerous that it should never be done under any circumstances. Of course it is possible that in a long report, only one or two paragraphs might be secret, in which case, the rest of the report could be sent in plain text, providing that the plain text matter will give no clue whatever to the encoded or enciphered matter. However, the best plan of all would be to make them separate. The insertion of any signs, abbreviations, or punctuation should be absolutely prohibited. This would seem obvious but let me tell you of an instance in which the insertion of an abbreviation lead to the solution of a message. (Case 3).

The plain text and code or cipher messages should never appear on the same sheet of paper; in the event of the loss of the papers or their capture, there would be less likelihood of the two being compared. As soon as a message has been encoded or decoded, all the work sheets used in the process must be destroyed by burning in strict accordance with the regulations set forth. A waste basket in a code room is the most dangerous article of furniture in it. *Char-*  
*women* If it is necessary to keep an exact copy of the plain text, the same should be kept in the coding room and guarded with as much secrecy and care as the code itself. Where a plain text copy of the message must be furnished to departments whose files are not secret, the plain text must be carefully paraphrased.

The work of paraphrasing requires considerable skill and practice, and in the case of matters of very great importance, the paraphrasing should be done or supervised by the higher officers. In all cases the paraphrasing must be done before the message leaves the coding room.

To many of you, paraphrasing a message is more or less unfamiliar, and it might be advisable for me to give an illustration. It will do no good to change merely the order of a word or two in each sentence. The entire form of the message must undergo the change. The message should be altered by the substitution of

synonyms, the elaboration of phrases, the change from active to passive voice and vice versa, etc. all of which should be without essential change in the significance of the message. Then the sentences may be shifted about so that the final result bears very little resemblance to the original form of the message. The best way of approaching the task is first to read the message over very carefully in order to get a clear idea of its meaning. Once that is done the principal ideas are to be expressed in a form as different as possible from the original, without material alteration in the intent of the message. (Case 4)

With all these precautions, it hardly seems necessary to remind you that encoded or enciphered messages must never be filed with their equivalent plain text. I have personal knowledge of such an instance.

All the precautions that I have mentioned so far are of general nature, but I must add one more: NEVER SEND CODE OR CIPHER MESSAGES BY WIRELESS OR BY ANY MEANS SUSCEPTIBLE OR EASY INTERCEPTION WHEN A MORE SECRET MEANS IS AVAILABLE AND WHEN THE MATTER DOES NOT REQUIRE IMMEDIATE ATTENTION. If there are reports upon matters of no particular importance at the moment, they might better be sent by courier or through the regular channels rather than transmitting them by wireless. The reason for this is that the greater the amount of traffic an enemy can intercept, the greater his chances for breaking into the code. Furthermore, the enemy may in certain cases gain valuable information merely from the number of messages sent and their length, without being in a position to read a single one of them. That applies more to military affairs, I suppose, than naval. It may be interesting to you to learn a few facts bearing upon this phase of the question by giving you an instance from the recent war.

(Case 5)

*The Germans used to send  
their morning reports in code,  
in standardized paragraphs,  
numbered, etc.*

I should think that it would be wise to regulate the amount of traffic during an actual state of war so that the enemy can draw no conclusions from the number of messages. In regulating the amount of traffic, routine messages such as daily or weekly reports, especially if they are of set forms, must be sent by other means. They are highly dangerous because of the similarities of contents. There is a method of breaking into a code, called the Analogy Method, which makes use of just such messages.

(Case 6)

The sending of short messages should be avoided because the nature of such messages is rather limited and if they are apt to be very frequent they

constitute favorite points of attack. (Case 7.)

One way to eliminate this danger is to make good use of the dummy groups; but their use must be judicious. (Case 8.)

The use of dummies is to be emphasized, especially in phrases or between words likely to be repeated several times in the same messages or in several messages. They must be employed in the spelling of such words as are not present in the code.

Avoid the use of words and phrases not in the code when other words or phrases with the same significance are present, because it is absolutely necessary to avoid spelling out words or phrases as much as possible. There are <sup>no</sup> advantages in spelling out such words when it is unnecessary and moreover such procedure opens the way for an attack by the enemy because it has been found that the spelling groups in a code constitute ~~the~~ weakest elements. ~~of the code~~. The fewer spelling groups used the more secure will be the code. It may sound far-fetched to you if I tell you that the code man, after a careful study of the text of a considerable number of messages, is able to determine, for the majority of the groups that appear, which ones represent punctuation; which, spelling groups; which, military or naval units, etc. In the case of the spelling groups after a sufficient number of them have been classified as being spelling groups, there is involved only a more or less simple case of substitution cipher. Once a few of the spelling groups have been solved a great break has been made into the code. Remember then, use the spelling groups as little as possible, and when they must be used exercise caution and use your best judgment. (Cases 9 and 10)

Another rule, which seems almost too obvious to mention, is that all operations applying to the system of enciphering, or encoding, must be completed. If there are three operations necessary, it would be highly dangerous to leave off one of them, say the final one. I know of two cases in which an encipherer, either through carelessness or a foolish belief that one operation was sufficient, left off the final operation in enciphering. The results were ~~most~~ disastrous.

After a consideration of the general principles and rules that apply in the preparation of messages, we come to a discussion of some special and detailed features.

I suppose, if I were asked what is the most important of the minor rules with regard to all cryptographic processes, for the purposes of making them secure, I should say that it is the principle of random selection or use of anything pertaining to the system. I do not know how to impress upon you the importance of this



principle. One of the factors which most often led to a first break into the German systems, was the methodicalness of the German mind. The typical German mind is so fascinated with the idea of doing everything systemically and in accordance with a set form that everything he does must be done according to system; then when he has once adopted a system he never departs from it unless it is specifically called to his attention. It was his slavish adherence to set forms that most often gave the leading clues. And if he was told that he must vary his procedure, he varied it according to a system!

I must confess, however, that our own forces were not a great deal better in this respect than the German. Time and again we called attention to the flagrant violations of the rules by men in this regiment or that regiment. But the seriousness of the violations, I am sorry to say, was little appreciated by the superior officers of the men who were guilty. You know how difficult it is to get action on things like this through the usual channels. The men in action think that there are a lot of old fogies back at head quarters, who have nothing to do but amuse themselves getting up a lot of "fool rules and regulations" with which to pester them. They say to themselves "How the devil can the enemy get anything out of a code message that is nothing but a jumble of letters? If this thing were not safe they would not give it to us". It may be that it is psychologically impossible to make most men realize the seriousness of the hundred and one minute precautions that must be observed, except by actually letting them see how solutions are achieved from the most slender of threads and far fetched clues.

For example, in almost every code for secret communication, alternates or variants for the most frequently used groups are given. I cannot tell you how difficult it is to get operators to use these variants and use them at random. A systematic selection of those variants would be dangerous. For example, at first the German operators had the idea that if a word, or a spelling group, or a punctuation sign occurred several times in a message, the variants were to be used in succession, the first one the first time it was used, the second the second time, etc. Or if the group was only used once in a message, the first variant was to be used. Such a procedure as the latter does not accomplish the purpose for which the variants are intended. (Case 11)

Another source of danger is the repeated use of the same expression, whether it be in the beginning, middle, or end of message. I wonder how many of you realize

the danger involved in such important parts of a message as the address and signature. In cipher work especially, these two parts of a message are always the first to be attacked. Now if, as often happens, messages contain the same addresses and signatures many times, solution is particularly easy in certain forms of ciphers. For example, one of the safest ciphers I know can be solved if one has two ~~even short~~ messages in <sup>even though they be short messages</sup> the same key, in which the signature is the same. And recently we solved another cipher, which was heralded, even by other experts, as being absolutely indecipherable by taking advantage of the fact that the addresses of the messages were in cipher too, even though they were all different. It is not so much the fact that addresses or signatures are dangerous as the fact that the beginnings and ends of messages are always weak points. It is just as dangerous, if not more so, to have a more or less set form of beginning messages, such as "Acknowledging your message number so and so" or "Referring to your message number so and so". The only guiding point in such matters can be avoid all stereotyped expressions and adhere to no regular forms in doing anything in cryptographic work.

The use of punctuation in a code or cypher message, except where the sense would be ambiguous without it, should be avoided. I should say that one of the greatest sources of clues in our work on the German Trench Codes lay in the excessive use of all forms of punctuation by the German operators.

There is one more caution that I might mention. Never give the enemy a chance to make any deductions with respect to the contents of any messages if it can possibly be avoided. Let us suppose for example that the units of a squadron are in maneuvers. A short message followed by a certain maneuver would enable a vigilant enemy to make certain deductions as to the contents of the message which dictated the movement. Similarly a message sent from A to B, followed by a short message from B to A, followed by a repetition of the first message by A would certainly indicate a request for repetition on the part of B. Or a long message sent by A, then a short message from B followed by a repetition of the first message from say the thirtieth group would certainly indicate a statement from B to A to the effect that the message was intelligible from the thirtieth group on. All such clues must be suppressed.

I have referred once before to the dangers of short messages. A short message from A to B followed by a longer message from B to A, say within ten or fifteen minutes, would indicate that possibly "question and answer" had been exchanged between the two stations. By watching these short messages the initial groups are apt to be easily solved

because questions most often begin with interrogatives such as "When" "Where" "How" or verbs such as "Is" "Are" "Have" etc.

Those responsible for the use of code books should regard it as part of their duties to send in to headquarters from time to time a list of words or phrases which are not present in the code and which are used sufficiently to warrant their being incorporated. In this connection I may tell you of the most peculiar anomaly of the German trench code. It had no word for code book. Consequently, every reference to it had to be spelled out. Now it was the regular practice to notify the stations, after a new code book went into effect, to return the old codes. Consequently, in the traffic the first day of the life of a new code one or more messages could always be found instructing the stations to send back the old code books. Since the word Code Book had to be spelled out, the finding and solving of such a message at once enabled us to make a great hole into every new code. If I were asked what word in all the German messages gave the most useful clues to solution, I should say it was this word "Satzbuch". This went on for over two years—all for the lack of a man with sufficient initiative and regard for his duty to inform the proper authorities. (Case 12)

I have told you about some of the things which helped us in our work on the German codes and ciphers used on the battle front, and have hinted at successes. Of our failures, I have told you nothing - and they were many. I am of the opinion and have good reason to suspect, that toward the end of the war the German intelligence department gave special courses of instruction in the use of code and cipher to the operators in charge of transmitting communications. The reason I suspect this is that as time went on the material became increasingly difficult to solve in spite of our continued experience with the material. The enemy evidently came to a realization of the importance of the correct use of their codes and ciphers and the result was that a most rigid discipline in communications came to be enforced. They even had inspectors whose duty it was to go from station to station and correct the errors being committed. One amusing incident in this connection may interest you. (Case 12.)

The idea of having an inspector or a sort of a "Security service" is fundamentally a very excellent one. The security service should be, it seems to me, a branch of the Code and Signal Section, because they are in a better position to realize all the mistakes and pitfalls and the seriousness of violations of the rules and they should also be able to keep a close watch over all the traffic. Such a department might seem superfluous but I believe that in the end it would more than

pay for itself. A poor code in the hands of experts can be used more safely than an excellent code in the hands of careless or ignorant operators. Finally, I might add that no code or cipher system known to me may be said to be "fool proof". Since the secrecy of operations is a fundamental prerequisite to success in warfare, it is hardly necessary to point out that the proper training of the personnel which is to be entrusted with the work of encoding and enciphering, and decoding and deciphering, is one of the most important factors in the realm of military or naval science.

MEMO ROUTING SLIP		NEVER USE FOR APPROVALS, CONCURRENCES, OR SIMILAR ACTIONS	
1 NAME OR TITLE	<i>Mr. W. F. Friedman</i>	INITIALS	CIRCULATE
ORGANIZATION AND LOCATION	<i>S/ASST</i>	DATE	COORDINATION
2	<i>Suspense</i>		FILE
			INFORMATION
3	<i>1 April 55</i>		NECESSARY ACTION
			NOTE AND RETURN
4	<i>1 May 55</i>		SEE ME
			SIGNATURE
REMARKS			
<p><i>This is the only edition thus far. However, Dr. Campaigne is working on a revision, and he expects to complete it in about two months.</i></p> <p style="text-align: center;"><i>5 August 1955</i></p> <p><i>Is in Dr. Campaigne's Office for typing then will have to be reproduced. Approximately 2 to 3 months before dissemination.</i></p> <p style="text-align: center;"><i>k</i></p>			

Declassified and approved for release by NSA on 11-06-2014 pursuant to E.O. 13526

FROM NAME OR TITLE	<i>ED Zallen</i>	DATE	<i>31 Dec 54</i>
ORGANIZATION AND LOCATION	<i>NSA-142</i>	TELEPHONE	<i>60317</i>

## MEMO ROUTING SLIP

REF ID: A59461

NEVER USE FOR APPROVALS, DISAPPROVALS,  
CONCURRENCES, OR SIMILAR ACTIONS

1 NAME OR TITLE <b>MR. CALLIMAHOS</b>	INITIALS	CIRCULATE
ORGANIZATION AND LOCATION <b>ING</b>	DATE	COORDINATION
2		FILE
		INFORMATION
3		NECESSARY ACTION
		NOTE AND RETURN
4		SEE ME
		SIGNATURE
REMARKS  Did we ever get out another edition of this? (This is marked "Preliminary")		
FROM NAME OR TITLE <i>J. [unclear]</i>		DATE <b>30 Dec 54</b>
ORGANIZATION AND LOCATION		TELEPHONE



Mr. Friedman's  
Appointments

1954 + 1955

12 APR 1955

In the Hospital



31 MAR 1955

Commander's Conference Cocktail Party

1 APR 1955

11:00 CWG mtg Poy's office

13:00 CWG mtg in Friedman's office

16:00 Mr. McPherson

4 APR 1955

In the Hospital

5 APR 1955

In the Hospital

6 APR 1955

In the Hospital

7 APR 1955

In the Hospital

8 APR 1955

In the Hospital

11 APR 1955

In the Hospital

14 MAR 1955

TDY Europe

15 MAR 1955

TDY Europe

16 MAR 1955

TDY Europe

18 MAR 1955

TDY Europe

21 thru 25 March 1955

TYD EUROPE

28 MAR 1955

Return to duty (first day)

2:00 Dr. Wright (Folger Library)

29 MAR 1955

No meetings

30 MAR 1955

10:00 Mr A.B. Clark

2 MAR 1955

TDY Europe

3 MAR 1955

TDY Europe

4 MAR 1955

TDY Europe

7 MAR 1955

TDY Europe

8 MAR 1955

TDY Europe

9 MAR 1955

TDY Europe

10 MAR 1955

TDY Europe

11 MAR 1955

TDY Europe

17 FEB 1955

10:00 Briefing in Gen Canine office by R/D

10:15 Collect long-distance call from Princeton

Dr. von Neumann, 4 mins. \$1.20 plus tax

2:00 Dr. Kullback

18 FEB 1955

TDY Europe

21 FEB 1955

TDY Europe

23 FEB 1955

TDY Europe

24 FEB 1955

TDY Europe

25 FEB 1955

TDY EUROPE

28 FEB 1955

TDY Europe

1 MAR 1955

TDY Europe

, 9 FEB 1955

10:00 Col Marcy's Office, AHS

3:00 Conf with Mr. Otis Wilson

Long Distance Call to Dr. Tukey (4 Mins.\$1.20 plus tax)

10 FEB 1955

Long distance call to Mr. McPherson

2:00 Classification Advisory Panel Mtg

11 FEB 1955

10:30 USCIB Mtg.

3:00 Bureau of Standards

14 FEB 1955

~~1:00 Briefing at AHS for Trip~~

15 FEB 1955

8:30 Gen's Staff Meeting

9:30 Mr. Corry and Dr. Stucky

3:00 Mr. McPherson, Gen Canine, Mr. Clark

16 FEB 1955

12-45 Mrs. BOGSON Gibson, AHS, PERS

1:00 Briefing for trip from PROD

1 FEB 1955

8:30 Gen's Staff Mtg

2:00 CWG

2 FEB 1955

10:00 CWG

Shots at Disp.

3:30 CWG

3 FEB 1955

10:00 CWG

4 FEB 1955

9:00 CWG

2:00 CWG

7 FEB 1955

10:00 CWG

Lunch with Mr. Friendly at Cosmos Club

3:00 mtg with Dr. Leibler, Mr. Clark, Dr.

Tompkins re SCAG

8 FEB 1955

8:30 General's Meeting

10:00 Technical Journal Meeting

**21 JAN 1955**

Sick Leave

**24 JAN 1955**

8:30 Dr. Tukey  
9:30 Ad Hoc Mtg of CWG  
10:30 CWG Mtg

**25 JAN 1955**

10:30 General's Staff Mtg (AHS)

**26 JAN 1955**

Lunch with Dr. Tukey at Cosmos Club

**27 JAN 1955**

AHS all morning  
4:00 CWG

**28 JAN 1955**

8:00 Technical Journal mtg  
9:30 CWG

**31 JAN 1955**

9:30 CWG Mtg, State Dept.  
4:00 CWG Mtg, State Dept.

<sup>12</sup>  
~~21~~ JAN 1955

9:00 Classification Meeting  
10:00 Mtg. in Mr. Polyozides office, State

**13 JAN 1955**

1330 Personal Development Board

**14 JAN 1955**

Dr. Wilks  
9:30 Mtg Mr. Polyizoides Office State  
2:00 Technical Journal Board

**17 JAN 1955**

9:30 Mtg Mr. Polyizoides Office - State  
2:00 Civilian Promotion Review Board

**18 JAN 1955**

8:30 Generals Staff Mtg  
1:30 Film "Mission"

**19 JAN 1955**

1:30 Members of SCAMP (introduced to Gen Canine)

**20 JAN 1955**

1:30 Length of Service Awards  
2:15 Ad Hoc Mtg Polyizoides Office State



**3 JAN 1955**

11:30 Dr. Tukey

**4 JAN 1955**

10:00 Meeting in Mr. Polyozides Office

**5 JAN 1955**

10:00 Meeting at Mr. Polyozides Office

2:00 Meeting with Mr. Hartstall

2:30 Meeting with Mrs. Crawford

**6 JAN 1955**

No Meetings scheduled

**7 JAN 1955**

1:30 Arlington Hall, Col. Marcy- SCAMP

**10 JAN 1955**

2:05 Called Dr. Sam Wilks, Princeton University

3 mins, 1 dollar plus tax

**11 JAN 1955**

8:30 General's Staff Meeting

9:30 Dr. Suits, talk with Capt Holtwick

11:45 Gen Canine's Office plus lunch (Cosmos Club)

2:00 Dental appointment

2 2 DEC 1954

Sick Leave

2 3 DEC 1954

Sick Leave

2 7 DEC 1954

Sick Leave

2 8 DEC 1954

4 hrs sick leave

2 9 DEC 1954

2 hours sick leave

3 0 DEC 1954

2 hours sick leave

1:30 Mr. McPherson

3 1 DEC 1954

19 DEC 1954

3:00 Reynolds and Leibler

10 DEC 1954

Lunch with General Canine, Mr. Crean

2:30 USCIB Meeting (110th mtg)

13 DEC 1954

1:30 - 4:00 General's Promotion Board

14 DEC 1954

8:30 The General's Staff Meeting

15 DEC 1954

4 hours sick leave

16 DEC 1954

11:00 Generals' Office Re: Dr. Pettengill

12:00 Lunch with Colonel Zeller

(10:00 Capt McDonald attended meeting in Pentagon  
with Mr. Bond)

17 DEC 1954

20 DEC 1954

Sick Leave

21 DEC 1954

Sick Leave

PL 86-36/50 USC 3605  
EO 3.3(h) (2)

80 NOV 1954

Attended lecture at AHS - invited by A.B. Clark -  
at 1330.

1 DEC 1954

Physical Exam

Luncheon of Armed Forces Communication  
Association - with Mr. Dingley and  
LT Col. Courtney

2 DEC 1954

No meetings

3 DEC 1954

3:35 Polyiozdes Office - State

4-6 DEC 1954

2:00 Cryptography Committee Meeting

7 DEC 1954

8:30 Director's Staff Meeting

9:30 Colonel Jacobs

1:00 Promotion Screening Board (GS 14 and above)

8 DEC 1954

1000 Generals Office

1300 USCIB Briefing in General's Office

15 NOV 1954

2:00 - 4:30 Civilian Promotion Review Board

16 NOV 1954

No meetings

17 NOV 1954

Lunch with "someone"  
at Cosmos Club. 1240-1440

18 NOV 1954

1300-1435 Personnel Development Board

19 NOV 1954

No meetings.

22 NOV 1954

Sick leave (8 hrs) ✓

23 NOV 1954

Lunch off the station with "someone"

24 NOV 1954

No meetings

25 NOV 1954

Holid. day

26 NOV 1954

Sick leave (8 hrs) ✓

29 NOV 1954

Lunch with daughter

~~1961 NOV 0 6~~

30 NOV 1954

Meeting (1030) at CIA [incl: Dingley, Parker, Erikson]  
for "demonstration":

1 NOV 1954

No Meetings

2 NOV 1954

9:00 General's Staff Meeting

3 NOV 1954

1:00 - 4:30 AHS

4 NOV 1954

Lunch with General Canine, Alexandria,  
Christi

5 NOV 1954

No meetings

8 NOV 1954

No meetings

9 NOV 1954

General's Staff Meeting

10 NOV 1954

9:30 RADAC Meeting

2:00 Briefing - USCIB Mtg.

Lunch with Mr. Pineau

12 NOV 1954

Annual Leave

20 OCT 1954

$\frac{1}{2}$  day at Justice Department

21 OCT 1954

Lunch with Thelma Pierce, May, and Kay and daughter

2:00 Miss Mary Jo Dunning

22 OCT 1954

Annual Leave

25 OCT 1954

2:00 - 4:30 USCIB Mtg.

26 OCT 1954

No meetings

27 OCT 1954

No meetings

28 OCT 1954

0830-1200 FBA Meeting

29 OCT 1954

No meetings

4 thru 8 October

At work

11 OCT 1954

Lunch with General Penny

12 OCT 1954

9:00 Staff Meeting

1:00 Gen Canine luncheon for Gen Sinclair

3:00 Gen Canine's Office - Al Friendly

13 OCT 1954

Meeting all day with Investigating Committee

14 OCT 1954

Met with Drs, Shaw, Shinn, Tordilla most of day  
Mr. Sidney Smith

15 OCT 1954

PL 86-36/50 USC 3605

EO 3.3(h)(2)

Justice Department

Lunch with General and Mrs. Penny

USCIB Meeting

13 OCT 1954

Justice Department

2:00 - 3:30 CivProBd

19 OCT 1954

Justice Department



23 SEP 1954

10:15 Mr Bane

24 September 1954

Annual Leave

27 SEP 1954

No meetings

28 SEP 1954

Gens Monthly Staff Meeting

Meetings at AHS 'til 3:00

29 SEP 1954

Spent most of day with Dr. Tukey and Mr. Weaver

30 SEP 1954

All morning spent at AHS

Dr. Tukey for short conference

Lunch with Dr. Sinkov

1 OCT 1954

4 hours annual leave

10 September 1954

No meetings

13 September 1954

No meetings

14 September 1954

Annual Leave

15 September 1954

Annual Leave

16 September 1954

Annual Leave

17 September 1954

No meetings

20 September 1954

Annual Leave

21 September 1954

Director Meeting 1½ hours

22 September 1954

Gen Ackerman's Office 9:00 - 10:30

Lunch with Mr. McPherson

EXSAB NSASAB - 1:00 3:00

30 Augsut

8:15 Colonel Herrelko

31 AUG 1954

8:30 Directors Staff Meeting

10:00 Dr. Kullback

10:30 Mr Hogan, B/D

1 SEP 1954

9:00 Brief - Holtwick - General Canine

10:00 Ad Hoc Committee

4:00 CIA - Briefing SAC

2 SEP 1954

Annual Leave

3 SEP 1954

Annual Leave

7 SEP 1954

Annual Leave

8 SEP 1954

Annual Leave

9 SEP 1954

No meetings

July 8 - August 19

TDY in London with five (5) days annual leave

**20 AUG 1954**

First day at work

**23 AUG 1954**

9:30 11:30 [REDACTED]

2:00 3:30 Mr Callimahos

**24 AUG 1954**

8:00 1:30 Arlington Hall (Generals Monthly Meeting)

1:30 4:30 [REDACTED]

**25 AUG 1954**

8:30 Classification Advisory Panel

10:00 General Canine

**26 AUG 1954**PL 86-36/50 USC 3605  
EO 3.3(h) (2)

No meetings

**27 AUG 1954**

Ad Hoc [REDACTED] 10:00 - 1:00

Mr. F. Rupp 1:30 - 2:00

Mr. Darby and Miss Church 3:00 - 3:30

28 June

10:30-12:00 State Dept.

29 June

10:30 General Monthly Staff  
Meeting (A.H.S.) Council  
2 hours Annual leave

30 June

Annual Leave

1 July

Annual Leave

PL 86-36/50 USC 3605

EO 3.3(h)(2)

2 July

9:30 General Council

2:30 State 

6 July

8:30 General Staff Meeting

10:00 Dr. Pittenzill + Major

7 July

no meetings

17 JUN 1954

1030 PBA - Conference Room

18 JUN 1954

830 PBA - Conf. Room (12:00)

21 JUN 1954

1100-1200 Ad Hoc mtg of CWG  
2:00 Civ. Perm. Bd.

22 JUN 1954

PL 86-36/50 USC 3605  
EO 3.3(h) (2)8:30-9:00 Staff Conference  
1030-1:00 CWG (State)

23 JUN 1954

9:30-12:00 RADAC mtg.  
2:30-3:30 GEN AOKERMAN

24 JUN 1954

9:00-10:00 Mr. With Dr. Ludell, Dr. Rogers  
10:30-12:00

25 JUN 1954

10:30-12:00 State Dept.

8 JUN 1954

● Prog. Bd. Adv. Com. Sec 10:30  
 Civ. Prom. Bd 1:30

9 JUN 1954

Prog. Bd. Adv. PROA 10:30

10 June

1000 Ad. Hqd to CWG  
 1045 CWG Mtg. Poly  
 2:30 Mr. Zister

11 June 1954

8:30 PBA mtg.  
 XXX 1:30 Briefing for USCIB

14 June 1954

2:20 USCIB Meeting, CIA.

15 JUN 1954

no meetings.

16 JUN 1954

● Mr. Christi, General Jordan  
 9:00 - 2:30  
 2:30 MR. CLARK's office (mtg)



26 may

Sick June

27 may

none

28 may

none

29-31 may Vacation

1 June

2:00

meeting w CONSULTANTS in C/S office

2 June  
Lunch at Cosmos Club

3 June

none

4 June

none

5-7 JUN 1954

none



11 MAY 1954

● 1100 CWG - STATE

2:00-4:30 DR SINKOV OFFICE

12 MAY 1954

3:00 Mr. Rowlett + 

4:00 Dr. Hilber - Counsel

13 MAY 1954

9:00 Visit w/Col Campbell of JEC.

2:30 Ex Group USA - affairs

14 MAY 1954

● 2:30 USCIB Meeting (103rd)

17, 18, 19 May Annual Leave

20 May

NSA Scientific Advisory Board

21 May

NSA Scientific Advisory Board

24 May

None

25 May

1000 General's Staff Meeting RAS

1:45 Mr. Bucher

27 APR 1954

● Monthly Staff Meeting at AHS

28 APR 1954

29 APR 1954

1100 Brig Gen Jiltman (said Dodge)

30 APR 1954

1145 Gen Thompson

4 May 54

● 0930 CW Prom. Bd - Gen Canine's Office

1300 Mr. McPherson - Gen. Canine

5 MAY 1954

9:30 Mr. Lea - Rosen

2:00 Rosen - Austin

2:30 Ad hoc Group - State

6 MAY 1954

1230 A.C. Friendly - Cosman

7 MAY 1954

● 8:30 Pettingill - Wallenfly

10:00 Working Com - Colf. Room

12 APR 1954

*None*

13 APR 1954

10:30 Mr. Bayne

14 APR 1954

12:30 Luncheon Cosmos Club

15 APR 1954

10:00

12:00 Luncheon Capitol Hill Club.

16 APR 1954

PL 86-36/50 USC 3605  
EO 3.3(h) (2)

10:00 - 12:00

*meeting*

19 APR 1954

2:00 Ad. Civ. Prom. Mtg. Postponed

6:30 CIA Party Met. Club.

20 APR 1954

0930 Working Committee + 

1000-1700 Scientific Advisory Board

21 APR 1954

0900-1700 Scientific Advisory Board

26 APR 1954

1100 - Mr. Sheldon (CIA)

1330 - 1630 Prog. + 3rd. An. Bl. Conf.

24 MAR 1954

25 MAR 1954

26 MAR 1954

ANNUAL LEAVE

29 MAR 1954

0900 Program &amp; Budget Advisors

30 MAR 1954

Maxwell AFB

31 MAR 1954

Maxwell AFB

1 APR 1954

~~Mr. Petty~~

12 APR 1954

Mr. McPherson here  
Called Mr. J. J. Cairns

15 APR 1954

16 APR 1954

17 APR 1954

annual  
leave

18 APR 1954

Lunch. with Scott

19 APR 1954

0900 Programs

12 MAR 1954

0830 NSA - Project & Budget Advisor  
Bldg 19

230 USCIB Meeting

15 MAR 1954

200 Civilian Promotion Board

16 MAR 1954

8:30 Staff Meeting

17 MAR 1954

1000 Capt. Supac  
200 Mr. Rupp

18 MAR 1954

1100 Class Adv. Panel

19 MAR 1954

1100 Walker - Austin

22 MAR 1954

Lunch - [redacted] [redacted]  
with Silber & Albert

23 MAR 1954

1000 Ad Hoc State Dept

1 MAR 1954

~~none~~

2 MAR 1954

0830 Staff Meeting

1005 Ad Hoc - Polyzoides

1030 Ad Hoc -  
136 class spec. (did not attend - Edna FB)  
P. Ware

3 MAR 1954

0900 Budget Advisory Meeting

400 Ad Hoc State

4 MAR 1954

~~none~~

5 MAR 1954

8 MAR 1954

9 MAR 1954

0830 Staff Meeting

9 MAR 1954

0930 Mr. Harton

1:00 Princeton Dr. Von Neumann

10 MAR 1954

Horton left ~~none~~ on leave

11 MAR 1954

1100 State-Comb. Working Group  
Ad Hoc Polyzoides

17 FEB 1954

1:30 AFSAC Meeting (Pentagon)

18 FEB 1954

8:30 Classification

1000 Briefing Gen. Canine *and depth*

2:00 Historian - w/Capt Frost

19 FEB 1954

900 A.B. Clark - Director's Off.

23 FEB 1954

1000 AHS. Staff Conf.

24 Feb

0930 RADAC Meeting (WF.)  
20202 NSS

25 Feb 1954

0830 Class. Adv. Bd. Panel

26 Feb 1954

1230 Army Navy Club (ANCC)  
w/ Polygides (CWS)  
Lunch

Leave 12:30 16:30

8 FEB 1954

NONE

9 FEB 1954

0830

Staff Meeting

10 FEB 1954

1230 LUNCH, Big Siltman, Polygraph  
(Westchester)

2:30 Briefing

11 FEB 1954

2:30

Board Meeting

12 FEB 1954

NONE

15 FEB 1954

200

Classification Board Meeting

1145

AA Albert

16 FEB 1954

0830

Staff Meeting

1000

Ad Hoc Polygraph

130

NSA Specialist AHS



28 JAN

9:15 to 11:30 Ad Hon &amp; CWS.

State Mr. Palygoides

12:30 Mr. Becker - Cosmos Club

29 JAN

8:30 Class Ad Panel - Conf Rm

10:00 Capt Naltunick AHS

12:00 Dr. Petty

2:30 Mr Palygoides Office

1 Feb

0800 Mrs. Feleraki

2 Feb

0830 Staff Meeting

4:00 Dr. Waterman, (Dr. Cairns also)

1520 H St N.W. Rm - M-24

(old Cosmos Club Bldg)

3 Feb

0930 State Dept. Palygoides

4 Feb

none

5 Feb

none

14 JAN

3:00 Frank Lewis

15 JAN

9:00 Mrs. Barlow

18 JAN

12:00 Sta. Cafeteria Mr. Crean

2:00 Civ. Promotion Rev. Board  
Conf. Rm. 1

20 JAN

10:00 Nelson

1:00 Athenhalt to plane

Gen. Canine's office

21 JAN

12:15 Lunch - Crean, Welkin, Canine

22 JAN

9:15 Gen. Canine re - Peterson

10:30 Gen. Canine re - Peterson

26 JAN

10:30 Monthly Staff Meeting AHS

27 JAN

10:30 R+D Presentation

4 JAN 1954

None

5 JAN 1954

8:30 - Weekly Staff Meeting - Conf. Rm.

10:00 - Operations Analysis Briefing - Capt. Holtwick  
- Conf. Rm.

1:30 - Meeting w/Dr. Engstrom and DIR in DIR's  
office.

6 JAN 1954

None

7 JAN 1954

PL 86-36/50 USC 3605

EO 3.3(h)(2)

8:45 Miss Dunning

9:15 Miss Fox

11:30 USCIB Meeting - CIA

8 JAN 54

9:00 Smith (Secret is in the letter)

10:30 State Mr. Paleroides

12 JAN

8:30 Staff Meeting

LONG DISTANCE PHONE CALLS  
Placed by Mr. Friedman

(as of 15 February 1954)

DATE	TIME	PERSON	COST
15 FEB	1105	Col. ROBT. W. GRIFFIN AIR CMD + STAFF Sch. MAXWELL AFB, ALA. (X 3212) spoke to his acct. Maxwell No. 7341	
3 Mar	1210	Prof. John von Neumann, Princeton (chg to home phone -)	
4 Mar	1:25	Prof. John von Neumann Princeton 1.00 + tax \$1.25	
29 Mar	2:20	Same as 15 Feb Col. Robt. W. Griffin +	
2 Apr	245	Called S.S. Cairns Mr. McPherson here ect	
16 APR 1954	2:00	Mr. Stephen Dearthell Saratoga 2-5826 home ect Office Plaza 3-1900 Ext. 579 call made to Plaza # \$1.10	
16 Apr 54	4:30	Dr. Claude Shannon \$1.10	

19 APR 1954

19 Apr. 1000 Van Neumann \$1.10  
Princeton, N. J.  
"COLLECT FROM"

(R)  
19 Apr. 1309 Dr. Baker (Baker's expense)  
Seymour N. Y.

27 Apr 3:35 (C) Mr. McPherson, New York

30 Apr  
Mr. Leo Rosen, Boston  
3 minutes \$1.55 plus 10% tax  
CF. made call

8 June  
Received no expense call from  
Mr. J. Howard (P. Allen)

18 Aug  
Dr. S. S. Wilks 9:30  
Princeton University  
5 mins - \$1.40 plus tax

21 Sept  
Dr. S. S. Wilks. 10:30  
Princeton University  
6 mins \$1.60 plus tax

10 Jan

Projector University  
Sam Wilks -

~~TOP SECRET - ULTRA~~

File

HEADQUARTERS  
ARMY SECURITY AGENCY  
WASHINGTON 25, D. C.

WDGSS-14

1 October 1945

**SUBJECT:** Report on Temporary Duty, ETO

**TO:** Commanding General  
Army Security Agency

1. Pursuant to attached orders (Enclosure 1), I left Arlington Hall Station at 0900 hours on 14 July 1945 and returned to that station at 0900 hours on 14 September 1945. Although the temporary duty was originally scheduled to be of three months' duration, Colonel Cook and I both felt that the work for which SID asked that I be sent to the ETO had been completed at the end of two months and there seemed to be no reason for staying any longer. Attached hereto (Enclosure 2) is a detailed account of my movements and duty on this trip.

2. a. A great deal of useful and important information was accumulated by participation in the work of TICOM. In my opinion the results of the TICOM operation have been extremely fruitful and it will take considerable time to assess and properly evaluate the mass of data gained thereby. It is believed that the innermost secrets of German cryptography and cryptanalysis have been laid bare and we are already in excellent position to give an overall picture of the results the Germans achieved, their successes, and their failures. In a separate paper to be prepared I hope to give a detailed report thereon, but at this moment I think it warranted to state that the British and American achievements in both main fields far surpass those of the Germans.

b. In the cryptographic field the Germans made progress -- but never so rapidly or in so coordinated and integrated manner as to prevent or delay for any considerable length of time the continued reading, by the Allies, of the innermost secrets of German military, naval, air force, or diplomatic high- and low-grade communications. Attempts to improve their cryptographic machinery were nearly always obstructed by jealousies, bickerings, and administrative incompetence on the part of those concerned in the research

~~TOP SECRET - ULTRA~~

WDGSS-14 (1 Oct 45)

~~TOP SECRET - ULTRA~~

and development work involved. For example, they started in 1939 to improve on the Enigma machine and by May 1945 had produced but a single complete model; in another case, they started work on an all-mechanical machine, an improvement on the Hagelin, in 1941; by May 1945 only a few machines had been produced and saw very little service. They produced a half-dozen different variations of a teletype encipherment machine, each of which except the very last was solved on a daily basis by the British. The early models of these machines were put into service without any serious attempt to study their security. German efforts to produce secure speech secrecy devices were dismal failures.

c. In the cryptanalytic field, they had but a mere half-dozen first-rate technicians and they failed to make even a dent in the high-grade cryptographic machines of the British or the United States. Their greatest achievements were the solution (up to the end of 1943) of the British Naval Cipher No. 3, British Naval Code, and American Strip Cipher using 30 strips regularly. When the channel interruption system was introduced in the last-mentioned system, they could do nothing further with it. They were completely baffled by our Sigaba traffic; they apparently did not even attempt a serious study of our SIGCUM or SIGTOT traffic, possibly because they were not too successful in intercepting it; they were apparently absolutely oblivious to or unaware of our SIGSALY transmissions. Their cryptanalytic deficiencies may, in part, be attributed to faulty organization and internecine warfare: there were at least half-dozen different, uncoordinated and competing cryptanalytic establishments, each one jealous of its own secrets and unwilling to cooperate except in a sporadic and faltering manner with any one of the other establishments. If there was a high-level coordinating agency, TICOM has failed to uncover it thus far. However, it does appear that the Germans had considerable, if not almost complete success with Russian military and naval cryptography--because it presented in most cases only the most elementary of cryptanalytic and traffic analysis problems.

d. It must also be stated that while the Germans had very little success, judged by our own standards, with British and United States high- and medium-grade material, they did not lack for certain important information gleaned from traffic analysis. The latter success was only possible because of our own shortcomings in radio procedures, practices, and security doctrine. A wide field for improvement in this respect remains for us to explore and to propagandize, with the hope of bringing about changes in attitude on the part of signal operating personnel.

~~TOP SECRET - ULTRA~~



~~TOP SECRET - ULTRA~~

WDGSS-14 (1 Oct 45)

3. My second visit to GC & OS can hardly be said to have been as interesting as my first: V-E Day and the imminence of V-J Day had diminished activities and operations to but a mere shadow of their former stature. An air of the graveyard and tomb hung over each of the "huts" and buildings. Gone was the bustle, hurry, sense of urgency, and hum of wheels turning; every day fever faces were seen. However, I found the visit interesting nevertheless and was glad of an opportunity to renew acquaintance with many old friends, all of whom endeavored to impress me with their earnest desire to continue our collaboration during the peace and to cement further the cordial relations that existed at the end of the war.

2 Incls:

1. Copy of orders
2. Account of movements & duty on trip

WILLIAM F. FRIEDMAN  
Director of  
Communications Research

~~TOP SECRET - ULTRA~~

~~RESTRICTED~~

*1945*  
WAR DEPARTMENT  
The Adjutant General's Office  
Washington 25, D. C.

*14 July*  
*14 Sept.*

AG 201 Friedman, William F.  
(10 Jul 45)OB-S-B

hak - 2B-939 Pentagon

11 July 1945.

SUBJECT: Travel Orders, Shipment IJ-Paris-YC.

TO: The Commanding General,  
Air Transport Command;  
The Chief of Transportation,  
Army Service Forces.

1. Mr. William F. Friedman, P-8, is hereby directed to proceed from Arlington, Virginia, to Washington, D. C., for further movement by air, on or about 14 July 1945, to Paris, France, and to such other places within the European Theater as may be directed by the Commanding General, United States Army Forces there on temporary duty for a period of approximately ninety (90) days, and upon completion of this temporary duty to return to Arlington, Virginia. UST-3-10975-WDP-JUL.

2. Prior to departure from the continental United States, he will be required to have completed the prescribed immunizations in conformity with current War Department instructions.

3. Regulations governing the procurement of military clothing and equipment in the United States are published in Section I, Circular 399, WD, 1944. Mr. Friedman is in Group 6. A uniform is required by the overseas commander. (Note Tab A, attached.)

4. Just prior to departure for port of aerial embarkation, he will advise correspondents that all mail will be addressed to him at APO 24441, c/o Postmaster, New York, New York. Upon arrival at destination overseas, he will contact the nearest Army Post Office to arrange for receipt and dispatch of official and personal mail. Civilian personnel using an APO mailing address are not entitled to the free mailing privilege.

5. Baggage to accompany the individual will be marked with the owner's full name, will be limited to sixty-five (65) pounds, and will accompany the individual to the port of aerial embarkation. Baggage will not be marked so as to disclose the overseas destination.

~~RESTRICTED~~

*Incl 1*

## Travel Orders, Shipment IJ-Paris-YC. (Cont'd.)

6. Travel by military, naval or commercial aircraft and common carrier is directed as necessary in the military service for the accomplishment of an emergency war mission and is chargeable to 601-3 P 432-02 212/60425 S 99-999.

7. In lieu of subsistence, a flat per diem of \$6.00 while within and \$7.00 while outside the continental limits of the United States is authorized in accordance with existing law and regulations while traveling and absent from permanent station. No per diem is authorized while traveling on board ships where the cost of passage includes meals.

8. The Chief of Transportation, Army Service Forces, Washington, D. C., will issue Certificate of Identification, WD, AGO Form No. 65-11 to Mr. Friedman with assimilated rank of Field Grade Officer. Upon the return of Mr. Friedman to the United States, Certificate of Identification will be surrendered to the Commanding General, Port of Entry.

9. Mr. Friedman is designated as official courier for the purpose of transporting official documents. Each package or envelope containing official matter which is to be exempt from examination will be sealed and will bear on its exterior cover the inscription "Official United States Army Communication, Exempt from Censorship", followed by the signature and official title of the authority dispatching the documents, who will furnish the courier with a letter addressed to the Collector, United States Bureau of Customs, Port of Aerial Embarkation, Washington, D. C., so describing the exterior cover or covers of the communications to be exempt from censorship as to enable the Customs Collector to identify them.

10. He is authorized to carry a camera, film and equipment and, subject to the restrictions of the theater commander, to take such photographs as may be necessary for the accomplishment of his mission.

11. In the interest of security there should be no discussion with unauthorized persons of the overseas destination involved herein.

12. The Commanding General, Air Transport Command, and the Chief of Transportation, Army Service Forces, will each furnish the transportation for which he is responsible and coordinate with all concerned.

~~RESTRICTED~~

Travel Orders, Shipment IJ-Paris-YC. (Cont'd.)

13. Mr. Friedman may be contacted thru Captain Robert S. Travis, Military Intelligence Service, War Department, Washington, D. C., telephone REpublic 6700, extension 72468.

By order of the Secretary of War:

/s/ Donald M. Davis  
Adjutant General

1 Incl.  
TAB A.

## COPIES FURNISHED:

CG, ETO (8); CO, PoAE, Wash., D. C. (2);  
OPD, WDGS (1); APS, AGO (2); Mr. Friedman, THRU:  
Capt. Travis (10); Capt. Travis, MIS (2);  
Ch/Transp., ASF (Maj. Warker) (1).

I certify that this is a true copy:

  
THURMAN R. HAMMAN  
Major, Signal Corps

~~TOP SECRET - ULTRA~~

## DETAILED MOVEMENTS

1945

- 14 July -- Left Washington Airport at 1130 hours (ATC terminal) by C-54 airplane. Stops at Newfoundland and Azores.
- 15 July -- Arrived Orly Field, Paris, France, at 2340, local time. Billsted at Hotel Franklin.
- 16 July -- Reported in at ETO HQ; OCSigO; SID HQ. Preliminary conference with Colonels Bicher and Cook.
- 17 July -- Continued conference with Colonel Bicher and Cook; review of SID current operations and situation; conference with Captain Wilkins, in charge of historical projects, SID.
- 18 July -- Continued conference with Colonels Bicher and Cook; conference with them and with Lieutenant Colonel Hilles, MIS representative in ETO, in regard to SIGTOT installation at Bletchley Park in British area. Formal call on and luncheon guest of General Rumbough, CSigO of ETO.
- 19 July to 25 July, inclusive -- Began one week's motor trip into U. S. Occupation Zone in Germany, with Colonel Bicher and Lieutenant Colonel Allen, on inspection tour of SID installations in Germany, including the following: (a) The Vierling Laboratory (an important TICOM target); (b) SID Advanced HQ (Detachment D), at Rüsselsheim; (c) 116th Signal R. I. Company at Scheuern; (d) 118th Signal R. I. Company at Rosenheim; (e) fixed intercept station at Grosse Geran. Visited Berchtesgaden en route.
- 26 July -- SID HQ in Paris. Continued conference with Captain Wilkins on historical project; conference with Colonels Bicher and Cook on TICOM matters; review of new TICOM documents; discussions with regard to new ETO security document; discussion with regard to box of OKW/Chi documents recovered from Lake Schliersee.
- 27 July -- En route to London with Colonel Bicher, by ATC; reported SID HQ at Weymouth Street. Review of TICOM situation and matters with Lieutenant Colonel Johnson.

1

~~TOP SECRET - ULTRA~~

Incl 2

~~TOP SECRET - ULTRA~~

- 28 July -- To Bletchley Park with Colonel Bicher; lunch and conference with Commander Travis; formal TICOM meeting in afternoon; tour of TICOM HQ and informal discussions with TICOM representatives.
- 29 July -- Visit to CSDIC HQ at Beaconsfield, to listen in on interrogation of an important German P/W (Mettig). Conference with Captain Ginsburg of CSDIC.
- 30 July to  
7 August inclusive -- TICOM HQ; study of TICOM documents and preparation of special questions to be put to P/Ws; discussions with TICOM members on current matters; conferences with Major Seaman, Mr. Lewis, Brigadier Tiltman, Captain Hastings, Paymaster Cmdr. Dudley-Smith, Mr. Hinsley. Tour through Bourbon section with Colonel Pritchard. Conferences with Mr. Ben Shute, chief MIS representative on Combined Historical Project, and with Mr. Birch (GO & CS), Editor in Chief of the Project.
- 8 August -- Spent day in London, visiting Berkeley Street. Conference (and lunch) with Captain Hastings and Major Stone (MIS representative at Berkeley Street); conference with Mr. Kendrick, technical head; conference with Lieutenant Colonel Johnson on TICOM matters. Courtesy call on Brigadier General Van Voorst, Assistant U. S. Military Attache.
- 9 August to  
14 August inclusive -- Continued work at Bletchley Park. Study of new TICOM documents; TICOM meetings and discussions; conferences with Major Seaman and Mr. Lewis on Bourbon project; conferences with Mr. Shute and Captain McCown (SSA representative on historical project).
- 15 August -- Official V-J Day. Trip to Cambridge with Cmdr. Travis to tour Cavendish Laboratory and visit Professor Vincent.
- 16 August to  
24 August inclusive -- Continued work and conferences as per 9-14 August cited above; conferences with Brigadier Tiltman and Cmdr. Travis; conferences with Mr. G. L. S. Williams on intercept and intercept control for Berkeley Street traffic; conferences with Dudley-Smith on questions arising from TICOM operations.
- 25 August -- Second visit to CSDIC HQ to listen in on further interrogations of German P/Ws (Huettenhain, Fricke, et al).

~~TOP SECRET - ULTRA~~

~~TOP SECRET - ULTRA~~

- 26 August -- In London, second visit to Berkeley Street; continued discussions with Mr. Williams and conferences with Messrs. Catty, Rees, Kendrick.
- 27 August -- Continued conferences at Berkeley Street; lunch  
and with Captain Hastings; visit to Queens Gate House  
28 August to tour special Berkeley Street tape-reading operation; conferences with Lieutenant Colonel Johnson on TICOM and SID matters.
- 29 August -- To Frankfurt, by air, via Paris.
- 30 August -- Conferences with Colonel Cook on TICOM matters;  
to second visit to Detachment D (HARN) and to Inter-  
2 Sept cept Station at Grosse Gerau; formal call on and  
inclusive luncheon guest of Major General Lanahan, OSigO, USFET; tour through Signal Corps installations at USFET HQ with General Lanahan; continued conferences with Captain Wilkins on historical project.
- 3 Sept -- To London with Colonel Cook, by air.
- 4 Sept -- To Bletchley Park with Colonel Cook for last formal TICOM meeting.
- 5 Sept -- Completion of TICOM work; final farewells to  
to GC & OS people, etc.  
7 Sept
- 8 Sept -- Return to London; made arrangements for return to U. S. by air.
- 9 Sept -- Final visits to Berkeley Street; conferences with  
and Captain Hastings, Messrs. Williams, Kendrick,  
10 Sept Catty, etc.
- 11 Sept -- Left London for Prestwick, by air; to Iceland;  
to return to Prestwick on account of bad weather;  
14 Sept to Azores, thence Bermuda and New York, where  
inclusive arrived at 0300 hours, 14 Sept; then by rail to Washington, arriving at 0830.
- 14 Sept -- Reported in at SSA, HQ, 0900.

~~TOP SECRET - ULTRA~~

~~TOP SECRET~~~~TOP SECRET~~31 May 1951  
AFSA-OOT

MEMORANDUM FOR: Distribution

SUBJECT: SCAG Conference

Enclosures: (A) Draft agenda  
(B) Notes to accompany draft agenda

1. The enclosures are forwarded for telephonic concurrence and/or comments (Ext. 60240).

2. It is proposed to distribute copies of the agenda to SCAG members at the opening session. Enclosure (B) is intended only for AFSA personnel.

## Distribution:

Adm. Stone - 1 copy  
Col. Collins - 1 copy  
Capt. Wenger - 1 copy  
Col. Hetherington - 1 copy  
Capt. Holtwick - 4 copies  
Capt. Harper - 4 copies

*William F. Friedman*  
WILLIAM F. FRIEDMAN  
Technical Consultant

This letter may be reduced to CONFIDENTIAL when enclosures are removed.

~~APPENDED DOCUMENT CONTAINS  
CODE WORD MATERIAL~~

~~TOP SECRET~~



~~TOP SECRET~~

SPECIAL CRYPTOLOGIC ADVISORY GROUP  
(SCAG)

Agenda  
for  
First Conference of SCAG  
4-5 June 1951

~~TOP SECRET~~

DRAFT

This sheet of paper and all of its contents must be safeguarded with the greatest care. Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.

SPECIAL CRYPTOLOGIC ADVISORY GROUP (SCAG)

Agenda

for

First Conference of SCAG

4-5 June 1951

—  
OPENING SESSION

Morning of 4 June 1951

Time: 10:00 A.M.

Place: Office of the Director, Armed Forces Security Agency, Room 118,  
Building 19, Naval Security Station, 3801 Nebraska Avenue, North West,  
Washington.

- Time
- 10:00 1. Address of welcome:  
  
Dr. William Webster, Chairman, Research and Development Board (RDB)
- 10:05 2. a. Presentation regarding the Armed Forces Security Agency (AFSA):  
  
Organization of AFSA; position in Department of Defense and Armed Forces; relationships with other U.S. agencies and bodies such as the United States Communications Intelligence Board (USCIB), and the Armed Forces Security Agency Council (AFSAC).  
  
Rear Admiral Earl E. Stone, USN, Director, AFSA
- b. Question and discussion period.
- 10:30 3. a. Presentation regarding the use and value of communications intelligence (COMINT) in national defense:  
  
Capt. J.N. Wenger, USN, Deputy Director, AFSA
- b. Question and discussion period.
- 11:00 4. a. Presentation on procedural matters in connection with the functioning of SCAG as an agency of RDB and a consultative body of AFSA:  
  
Mr. Edwin A. Speakman, Executive Director, Committee on Electronics, RDB
- b. Question and discussion period.
- 11:30 5. Outline of program for technical sessions:  
  
Mr. William F. Friedman, Technical Consultant, AFSA
- 11:35 6. Indoctrination of SCAG members not already indoctrinated:  
  
Capt. J.N. Wenger, USN, Deputy Director, AFSA
- 12:00 Luncheon: Conference Room, adjoining Admiral Stone's Office, Room 19-125.  
ARMED FORCES SECURITY AGENCY

This sheet of paper and all of its contents must be safeguarded with the greatest care.  
Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.

TECHNICAL SESSIONS

Commencing after lunch on 4 June 1951

Time: 1:00 P.M.

Place: Room 202, Building 20, Naval Security Station

Time:  
1:00

1. a. Presentation to illustrate how a complex COMINT problem was successfully handled in World War II:

LCDR Andrew M. Gleason, USNR

I. The cryptographers' point of view

- A. Requirements
- B. Codes and ciphers
- C. Mechanics of a cipher system

II. Single-letter substitution ciphers

- A. General description
- B. Machine systems
- C. Pad systems; additives

III. Wired-wheel machines and the German Enigma

- A. General description
- B. The commercial Enigma
- C. The steckered Enigma
- D. The Bombe
- E. Duenna

2:00            b. Question and discussion period.

3:00            2. a. Tour of special cryptanalytic machines at the Naval Security Station:

Dr. H. Campaigne and Dr. J.J. Eachus

I. Atlas

Presentation regarding AFSA's position and program in the field of electronic computers

II. Demon I and Demon II

III. Goldberg

IV. World War II Bombe for Enigma solution

4:00            b. Question and discussion period.

ARMED FORCES SECURITY AGENCY

This sheet of paper and all of its contents must be safeguarded with the greatest care.  
Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.

TECHNICAL SESSIONS, Cont'd

Morning of 5 June 1951

Time: 9:00 A.M.

Place: Room 202, Building 20, Naval Security Station

PRESENTATIONS REGARDING A CURRENT HIGH-PRIORITY AFSA PROBLEM

Time  
9:00

1. a. Introduction to Albatross

I. Background of the Albatross problem

II. What is known about the machine

III. Present indicator system

IV. The Round Robin machine

To be presented by Mr. F.A. Raven and Mr. D.H. Shepard

10:00

b. Question and discussion period.

11:00

2. Isomorphism and wheel recovery

I. Discussion of isomorphism

II. A sample problem in wheel recovery

To be presented by Mr. A.N. Levenson and Mr. E.D. Marston

12:00

Luncheon: Executive dining room, Naval Security Station Cafeteria

This sheet of paper and all of its contents must be safeguarded with the greatest care.  
Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.

Afternoon of 5 June 1951

Time: 1:30 P.M.

Assembly point: Room 1082, Building "A", Arlington Hall Station, 4000 Lee Boulevard, Arlington, Virginia. (Transportation from Naval Security Station to Arlington Hall Station will be provided for SCAG members)

Time  
1:30

1. Tour of AFSA machines, to be conducted by Mr. Frank B. Rowlett, assisted by Dr. A.E. Highley and Mr. William J. Lawless.

I. The IBM installation

II. RAM equipment

- A. Abner
- B. Robin
- C. ASAF-1

- 2:30 2. a. Discussion period on isomorphism and wheel recovery.

To be held in Room 2010, Building "B", AHS

b. Coffee will be served during this period.

- 3:30 3. a. Presentation regarding AFSA project S EATER: Matrix projection (Room 2032, Bldg. "B")

Mr. Albert E. Roberts

This presentation is of interest primarily to those members of SCAG who are specialists in the field of mathematics.

- 3:30 b. Presentation regarding electronic representation of rotors (Room 2010, Bldg. "B")

Dr. Eachus, assisted by Mr. Ray L. Bowman and Mr. Roger Moulton

This presentation is of interest primarily to those members of SCAG who are specialists in the field of electronics and electrical engineering.

- 4:30 4. Final discussion.

To be held in Army Security Agency Conference Room (Room 117), Headquarters Building, Arlington Hall Station.

5. Closing remarks.

Rear Admiral Earl E. Stone, USN, Director, AFSA

ARMED FORCES SECURITY AGENCY

~~TOP SECRET~~

OPENING SESSION  
Morning of 4 June 1951

Time: 10:00 A.M.

Place: Office of the Director, Armed Forces Security Agency, Room 118,  
Building 19, Naval Security Station, 3801 Nebraska Avenue, North  
West, Washington

- Time  
10:00
1. Indoctrination of SCAG members not already indoctrinated:  
     Capt. J.N. Wenger, USN, Deputy Director, AFSA
- 10:15
2. a. Presentation regarding the Armed Forces Security Agency (AFSA):  
     Organization of AFSA; position in Department of Defense and Armed  
     Forces; relationships with other U.S. agencies and bodies such as  
     the United States Communications Intelligence Board (USCIB),  
     and the Armed Forces Security Agency Council (AFSAC);  
     Mission for SCAG:  
     Rear Admiral Earl E. Stone, USN, Director, AFSA
- b. Question and discussion period.
- 10:40
3. Remarks on behalf of Lieut. General Walter B. Smith, USA, Director  
     of Central Intelligence:  
     Mr. Kingman Douglass, Assistant Director, CIA
- 10:45
4. Address of welcome:  
     Mr. William Webster, Chairman, Research and Development Board (RDB)
- 10:50
5. a. Presentation regarding the use and value of communications intelligence  
     (COMINT) in national defense:  
     Capt. J.N. Wenger, USN, Deputy Director, AFSA
- b. Question and discussion period.
- 11:20
6. a. Presentation on procedural matters in connection with the functioning  
     of SCAG as an agency of RDB and a consultative body of AFSA:  
     Mr. Edwin A Speakman, Executive Director, Committee on Electronics, RDB
- b. Question and discussion period.
- 11:50
7. Outline of program for technical sessions  
     Mr. William F. Friedman, Technical Consultant, AFSA
- 12:00
- Luncheon for SCAG members: Director's Office, Room 19-118.

~~TOP SECRET~~

~~TOP SECRET~~

## TECHNICAL SESSIONS

Commencing after lunch on 4 June 1951

Time: 1:00 P.M.

Place: Room 202, Building 20, Naval Security Station

Time:  
1:00

1. a. Presentation to illustrate how a complex COMINT problem was successfully handled in World War II:

LCDR Andrew M. Gleason, USNR

- 2:00 b. Question and discussion period.

- 3:00 2. a. Tour of special cryptanalytic machines at the Naval Security Station:

Dr. H. Campaigne and Dr. J.J. Eachus

## I. Atlas

Presentation regarding AFSA's position and program in the field of electronic computers

## II. Demon I and Demon II

## III. Goldberg

## IV. World War II Bombe

- 4:00 b. Question and discussion period.

~~TOP SECRET~~





~~TOP SECRET~~TECHNICAL SESSIONS, Cont'd  
Afternoon of 5 June 1951

Time: 1:30 P.M.

Assembly point: Room 1062, Building "A", Arlington Hall Station, 4000 Lee Boulevard, Arlington, Virginia. (Transportation from Naval Security Station to Arlington Hall Station will be provided for SCAG members)

Time

1:30

1. a. Tour of AFSA machines, to be conducted by Mr. Frank B. Rowlett, assisted by Dr. A. E. Highley and Mr. William J. Lawless.

- I. The IBM installation  
II. RAM equipment

- b. Tour of AFSA machines under development, to be conducted by Dr. Eachus, assisted by Mr. C.J. Schierlmann.

2:30

2. a. Discussion period on isomorphism and wheel recovery.

To be held in Room 2010, Building "B", AHS.

- b. Coffee will be served during this period.

3:30

3. a. Presentation regarding AFSA project SWEATER: (Room 2032, Bldg. "B")

Mr. Albert E. Roberts

This presentation is of interest primarily to those members of SCAG who are specialists in the field of mathematics.

3:30

- b. Presentation regarding electronic representation of rotors (Room 2010, Bldg. "B")

Dr. Eachus, assisted by Mr. Ray L. Bowman, Mr. Roger Moulton, Mr. Robert E. Gordon and Mr. Arthur Moulton.

This presentation is of interest primarily to those members of SCAG who are specialists in the field of electronics and electrical engineering.

4:30

4. Final discussion.

To be held in Army Security Agency Conference Room (Room 117), Headquarters Building, Arlington Hall Station.

5. Closing remarks.

Rear Admiral Earl E. Stone, USN, Director, AFSA

~~TOP SECRET~~

~~TOP SECRET~~

NOTES

(for AFSA personnel)

TO ACCOMPANY AGENDA FOR FIRST SCAG CONFERENCE

~~TOP SECRET~~

Notes (for AFSA personnel) to accompany Agenda for First SCAG Conference

4-5 June 1951

1. a. Arrangements have been made to issue "Conference Badges" to all SCAG members (except in the case of Dr. Engstrom, who already has a "White A" Badge).

b. The badges will be available by 0830 hours on 4 June, and will be picked up by Captain Mary C. Lane, who will deliver them as follows:

<u>Badge for:</u>	<u>To be delivered to:</u>
Dr. William Webster	Capt. Hazard
Mr. Edwin A. Speakman	Capt. Hazard
Dr. John von Neuman ✓	ICDR Gleason
Dr. Stewart S. Cairns ✓	ICDR Hall
Dr. Charles B. Tompkins ✓	ICDR Hall
Dr. R.K. Potter	Dr. Kullback
Dr. Claude E. Shannon	Dr. Campaigne
Mr. John Howard	Dr. Campaigne
Mr. Joseph Desch	Dr. Eachus
Mr. John C. McPherson	Dr. Eachus

2. a. The indicated AFSA personnel will act as "guides" for the following SCAG members:

<u>SCAG member:</u>	<u>"Guide"</u>
Dr. von Neuman	ICDR Gleason
Dr. Cairns	ICDR Hall
Dr. Potter	Dr. Kullback
Dr. Shannon	Dr. Campaigne
Mr. Desch	Dr. Eachus
Mr. McPherson	Dr. Eachus

b. It is assumed that the other members of SCAG (Dr. Tompkins, Dr. Engstrom, and Mr. Howard) are sufficiently acquainted with AFSA and Washington as to make it unnecessary to assign specific "guides" for them; however, AFSA personnel should make every effort to assist those members whenever appropriate.

~~TOP SECRET~~

3. a. In addition to SCAG members, only the following will be present at the opening session of the Conference at 1000 hours, 4 June, in the office of DIRAFSA, Bldg. 19, NSS (See page 1 of Agenda):

Adm. Stone  
 Mr. Webster  
 Mr. Speakman  
 Mr. Douglass  
 Capt. Wenger  
 Col. Hetherington  
 Capt. Harper  
 Capt. Holtwick  
 Mr. Friedman

b. Luncheon for SCAG members, Mr. Speakman, Mr. Douglass, DIRAFSA, the Deputies and Mr. Friedman will be served in the Director's Office after 1200 hours.

4. a. In addition to the SCAG members, the following will be present at the first technical session, 1300 hours, 4 June, in Room 20-202, NSS (See page 2 of Agenda):

AFSA-02:

Capt. Holtwick  
 Mr. Rowlett  
 Mr. Raven  
 Mr. Shepard  
 Mr. Levenson  
 Mr. Harston

AFSA-03:

Capt. Harper  
 Dr. Kullback  
 Dr. Campaigne  
 Dr. Eachus  
 LCDR Gleason  
 LCDR Hall

Mr. Speakman, RDB  
 Mr. Friedman, AFSA-OOT

b. Coffee will be served at about 1500 hours.

c. At the close of this session AFSA participants will endeavor to see that SCAG members have transportation to their hotels.

~~TOP SECRET~~

~~TOP SECRET~~

5. a. In addition to the SCAG members, the following personnel will be present at the morning session, 5 June, in Room 20-202, NSS (See page 3 of Agenda):

AFSA-02:

Capt. Holtwick  
 Mr. Rowlett  
 Mr. Raven  
 Mr. Shepard  
 Mr. Levenson  
 Mr. Marston  
 Capt. Dennis  
 Mr. Highley  
 Mr. Lawless  
 Mr. Kirby  
 Mr. Reimers  
 Mr. Schmitt  
 Mr. Shinn  
 Mr. Hesse

AFSA-03:

Capt. Harper  
 Dr. Kullback  
 Dr. Campaigne  
 Dr. Eachus  
 LCDR Gleason  
 LCDR Hall

Mr. Speakman, RDB

Mr. Friedman, AFSA-00T

b. Coffee will be served at about 1030 hours.

c. A special luncheon costing about \$1.00 will be served in the Executive Dining Room, Naval Security Station Cafeteria. In view of the limited facilities, only the following can be readily accommodated:

SCAG members  
 Mr. Speakman  
 Col. Collins  
 Capt. Fonger  
 Col. Hetherington  
 Capt. L.S. Howeth, Op-202  
 Capt. W.M. Gullett, CO, NSS  
 Capt. Harper  
 Capt. Holtwick  
 Capt. Dennis  
 Mr. Rowlett  
 Dr. Kullback  
 Dr. Campaigne  
 Dr. Eachus  
 LCDR Gleason  
 LCDR Hall  
 Mr. Friedman

(Total: 25)

~~TOP SECRET~~

~~TOP SECRET~~

d. AFSA personnel will endeavor to insure that SCAG members requiring transportation from NSS to AHS for the afternoon technical session at AHS will be provided therewith. This should be taken care of before or during the luncheon period.

6. In addition to the SCAG members, the following personnel will participate in the tour of machine installations at AHS (See para. 1, page 4 of Agenda). (The assembly point will be Room 1082. Building "A", at 1330 hours):

AFSA-02

Mr. Rowlett  
Mr. Highley  
Mr. Lawless

AFSA-03:

Capt. Harper  
Dr. Kullback  
Dr. Campaigne  
Dr. Eachus  
LCDR Gleason  
LCDR Hall  
Mr. Schiefelmann

Mr. Speakman, RDB  
Mr. Friedman, AFSA-COT

7. a. The personnel to be present at the discussion period indicated to follow the tour (see para. 2, page 4 of Agenda), beginning at 1430 hours, in Room 2010, Building "B", AHS, will be the same as in attendance at the session indicated in Paragraph 5.a. above.

b. Coffee will be served during this period.

8. a. For the presentation regarding AFSA project S'EATER (see para. 3 a., page 4 of Agenda), at 1530 hours in Room 2032, Bldg. "B", the following will be present:

SCAG members:

Dr. von Neumann  
Dr. Cairns  
Dr. Shannon  
Dr. Engstrom  
Dr. Tompkins

~~TOP SECRET~~

~~TOP SECRET~~AFSA personnel:AFSA-02:

Mr. Levenson  
 Mr. Shepard  
 Mr. Schmitt

AFSA-03:

Dr. Kullback  
 Dr. Campaigne  
 LCDR Gleason  
 LCDR Hall

Mr. Albert E. Roberts

b. For the presentation regarding electronic representation of rotors (see para. 3.b., page 4 of Agenda), also scheduled for 1530 hours in Room 2010, Bldg. "B", the following will be present:

SCAG members:

Dr. Potter  
 Mr. Desch  
 Mr. McPherson

AFSA personnel:AFSA-02:

Mr. Highley  
 Mr. Lawless  
 Mr. Marston

AFSA-03:

Capt. Harper  
 Dr. Eachus  
 Mr. Rosen  
 Mr. Dumey  
 Mr. R.E. Gordon  
 Mr. R. Moulton  
 Mr. Bowman  
 Mr. A. Moulton

Mr. Speakman, RDB

Mr. Friedman, AFSA-OOT

9. In addition to all SCAG members, the following persons will attend the final session at 1630 hours, 5 June 1951, in the ASA Conference Room, Hq Bldg., AHS (see paras. 4 and 5, page 4 of Agenda):

Adm. Stone  
 Mr. Speakman  
 Capt. Holtwick  
 Mr. Rowlett  
 Capt. Harper  
 Dr. Kullback  
 Dr. Campaigne  
 Mr. Friedman

10. Record of proceedings will be kept by Dr. Campaigne, assisted by LCDRs Gleason and Hall.

~~TOP SECRET~~

# THE INFLUENCE OF C-POWER\* ON HISTORY.

## LECTURE NO. 3

### MAKING THE MOST OF A CRYPTOLOGIC OPPORTUNITY.

#### ← [ PART 1 - INTRODUCTION

Introduction to the Walter Cronkite Television Story Entitled

"The Secret Message that Plunged America into War!" —

one of the episodes of his "You Are There" <sup>Series</sup> ~~Program~~  
Columbia Broadcasting System  
presented over the TV network

on  
23 October 1955, repeated on 4 August 1957.

*Insert attached* →

I imagine that, for many of ~~those present this evening~~ the name Alfred

Zimmermann, German Minister of Foreign Affairs in Berlin in the years 1914-1916, <sup>at</sup>

*these days;*

is not one that arouses much interest; in fact, I doubt that the name means

*a great many*

anything to ~~most~~ of you. Yet, this gentleman, of whom I find it difficult to

say "may his soul rest in peace", was the diplomat whose ~~stony~~ and unimaginative

*constituted a fine example of how not to make friends and*

conduct of German foreign affairs in the three critical years I've mentioned

*Here Zimmermann's culminating cap in a career of ~~stony~~ unimaginative characteristics*

brought the United States of America into World War I as an active belligerent

*(This); within a month after it had become known to the Americans. The military*  
on the side of the Allies; ~~and the~~ ~~side of the United States~~ could easily have been

*it was wrong for our country, that is, on the side*

thrown to the other side--during the critical months of the year 1916--had the Germans

*and particularly* I lived through that period and I know from first-hand  
Zimmermann been more astute. The consequences of such an event can hardly be

*gauged;*  
~~measured;~~ *It would be an understatement to say that possibly* the course of

*not*  
history would have been changed in a <sup>most</sup> spectacular manner.

\*"C-power" = Cryptologic power.

*experience that there were several occasions when it wouldn't have tilted in much to the balance in favor of Germany.*

*influence people; in fact, it can out have been paid by many historians that:*



What did Herr Zimmermann do or fail to do to merit so strong a statement

What did he do or fail to do that tipped the balance suddenly in favor of Britain?  
as the one I've just made? What he did was to send a telegram on 16 January 1917

to the German Ambassador in Washington--a telegram which was in German <sup>a German office</sup> enciphered

code and which was intercepted and solved by the British cryptanalytic unit in <sup>first, to realize that Americans might react if they learned the contents of his message;</sup> London. <sup>What he failed to do was to see to it that the cryptosystem that had to</sup>  
<sup>Now Zimmermann</sup>

be used to encrypt his message was technically sound enough to protect its

<sup>In the aftermath of the discovery of his diplomatic dumbness he</sup>  
contents. <sup>He</sup> did and failed to do something else in connection with his now

famous message--but of that, more later.

In order to prepare a proper background for the Zimmermann Telegram of

16 January 1917--that's what it's called in history--I <sup>will</sup> give you a brief

~~with~~ picture of the situation from the outbreak of the war, on 1 August 1914, up

<sup>about the time</sup>  
to ~~the~~ the telegram was sent. ~~The picture I'm going to depict is a~~ condensation

~~of the excellent story set forth on pages 22 and 23 of Admiral Sir~~

~~William James' book entitled The Eyes of the Navy, published in Boston in 1955.~~

By 1914 England had become so dependent on sea-borne imports that her people couldn't live, let alone wage war, for more than four or five weeks after her sea-routes were broken. Keeping these routes open was therefore the principal task of the British Navy. On the other hand, her principal enemy, Germany, was

Let's see what the telegram says. I show slide of 1917 version.

not dependent on sea-borne imports, so that the British Navy's historic function of arresting an enemy's sea-borne trade lapsed after German shipping had found refuge in neutral ports.

There were, then, the British Grand Fleet and her hardly much inferior protagonist, the German High Seas Fleet, ~~glaring~~ <sup>glaring</sup> at each other at a distance, and, although the Grand Fleet was becoming impatient and spoiling for a fight, the Germans didn't dare risk their fleet in major battle, <sup>They</sup> confined their attacks to sporadic forays by fast units and to minelaying.

German hopes of quick victory were shattered when trench warfare in France

brought ~~things~~ <sup>the war</sup> to a stalemate, ~~and~~ <sup>each</sup> with the passing ~~of each~~ month it became clear

that there could be no victory ~~for Germany~~ <sup>German</sup> unless British overseas trade was cut

Even in 1915 <sup>in certain German circles</sup>, there were those who had off. ~~Some high up in the Government~~ <sup>thought</sup> that what appeared to be a good idea, <sup>very</sup>

<sup>these people thought that the</sup> ~~inherent~~ success of the German small sub Flotilla of 1914 pointed the way out

without risking the <sup>eyes</sup> High Seas fleet, <sup>But the time was not yet ripe for such violent</sup> and the good idea was to give highest

priority to building submarines and use them to destroy British <sup>if necessary,</sup> and all other

shipping to ~~and~~ <sup>the</sup> British Isles.

<sup>The time wasn't ripe because</sup>

~~Now it happened that~~ civilized rules of maritime warfare required that no merchant ship be sunk without warning; <sup>and before the crew could take to life</sup>

boats. ~~Observance of~~ <sup>these rules had hitherto been required</sup> ~~by both belligerents~~ <sup>were being respected</sup>

but for <sup>the</sup> Germany <sup>S</sup> this ~~of course~~ <sup>severely</sup> reduced the destructive power of <sup>their</sup> ~~the~~ submarines and from time to time their commanders <sup>either on their own initiative ignored or they</sup> were ordered to ignore them, <sup>That this was especially true</sup> in

the case of the British merchantmen. <sup>goes almost without saying,</sup> But there were bound to be mistakes and <sup>Sometimes</sup> the ships of neutrals were <sup>with the result that</sup> ~~sunk,~~ <sup>also</sup> ~~that~~ <sup>the</sup> German unrestricted submarine warfare, as it came to be called,

Government, ~~and there were~~ <sup>Many bitter and</sup> ~~there were~~ <sup>were sent</sup> acrimonious notes <sup>by our</sup> to that government, especially from ~~the~~

~~American~~ Government, when <sup>our</sup> ~~our~~ ships were sunk and specious excuses were given for <sup>it couldn't pay the price of</sup> Germany ~~decided that~~ <sup>unrestricted</sup> submarine warfare in the form of universal condemnation, <sup>and</sup> such sinkings. <sup>from some up the practice. But as regards American shipping</sup> American antagonism was heightened by the discovery of plots and sabotage activities of German agents in America. <sup>Had continued to be terrible and</sup>

The powerful German submarine offensive in 1916, <sup>even though unrestricted,</sup> soon began to take a dreadful

turn for the British. <sup>Soon</sup> ~~with~~ the daily toll of ~~the~~ shipping losses <sup>became</sup> ~~was~~ so heavy that it began to be obvious <sup>that</sup> unless some new tide set in -- or unless <sup>the</sup> United States of America could be

drawn into the war on the Allied side -- there could be only one end to <sup>the war,</sup> ~~it,~~ and that end would come soon.

Britain's <sup>First,</sup> ~~the~~ problem then was two-fold: (1) To labor prodigiously to gain mastery over

the German submarines; but this, it was recognized, would be a slow, a very slow,

<sup>Second,</sup> process (2) <sup>to</sup> try not to irritate or antagonize the United States, and certainly

not to exasperate America <sup>were</sup> as the Germans <sup>was, of course,</sup> ~~were~~ <sup>The</sup> hope that the letter would <sup>of Germans</sup>

"Were serious doubts being cast in America on the genuineness of the instructions to the German Minister in Mexico the authorities here might reconsider their position, but as Zimmermann has admitted their genuineness in the Reichstag this can hardly be the case."

7  
That is what Hall greatly feared would happen--but his fears turned out  
to be groundless.

sooner or later, the sooner the better, good ~~the~~ <sup>the</sup> ~~Americans~~ into joining the war on the English side:

*later* ~~against Germany~~. The British were fortunate in both respects. It turned out that

thanks to the tremendous exertions of <sup>their</sup> British shipbuilders, ~~scientists~~, and sailors,

mastery over the submarines was attained, but <sup>that didn't come</sup> ~~not~~ until early in 1918. With this

phase of the British problem as I've just stated it, we shall not concern ourselves

today. It is with the other phase of it that my talk will deal.

Let's see how the Germans behaved so as to outrage <sup>nearly</sup> practically all Americans and <sup>to</sup> make President Wilson ask Congress to declare war on <sup>the</sup> ~~them~~ <sup>Germans</sup>.

*As I've already related,*

During the first <sup>two</sup> years of submarine warfare the German Government respected and followed the rules of civilized warfare. the rights of neutral nations, <sup>but</sup> when faced with the prospect of losing the war

<sup>Germany felt forced to</sup> unless all imports to the British Isles were cut off, ~~it~~ <sup>it</sup> made a fateful decision.

*on* 1 February 1917, <sup>Germany</sup> ~~it~~ announced that as of that date ~~German~~ <sup>its</sup> submarines would

sink at sight ALL ships met on the high seas; in short, <sup>the German Government officially</sup> ~~it~~ proclaimed that unrestricted submarine warfare was being resumed. And it was <sup>without further</sup> ~~it~~ <sup>add.</sup>

What did President Wilson do on receipt of the German proclamation? Why,

*two days later,* on 3 February, he informed German Ambassador von Bernstorff that ~~his career in the~~

United States was at an end <sup>was cutting</sup> ~~and~~ the United States ~~had severed~~ diplomatic relations

with Germany. Von Bernstorff's <sup>career in the United States was over;</sup> ~~wasn't~~ given much time to pack his belongings and

go home. And <sup>of course, American</sup> Ambassador Gerard <sup>in Berlin</sup> was called home. But note that severing diplomatic relations doesn't mean war — and it didn't in this case.

P L E A S E   N O T E ! ! !

Advance Registrations MUST BE RECEIVED IN SECRETARY'S OFFICE PRIOR  
TO SEPTEMBER 30TH. THEREAFTER THEY WILL BE RECEIVED BY

RICHARD D. HIGGINS  
Archivist of the Commonwealth of Massachusetts  
Chairman Local Arrangements Committee, SAA  
State House, Boston 33, Massachusetts

Fredman Chief AS... 12 - J. Lee King script 49  
then 11.5

Ray Apple

4146

Handwritten signature

It was only natural if Britain to hope that we <sup>her in</sup>  
~~of course, Britain had hoped that the United States would now join the war~~  
~~but, as to say we held back -~~ To many of us our  
against Germany ~~The American position was quite humiliating because it was clear~~

we were unable to <sup>it seemed that</sup>  
that ~~she could~~ not give our own merchantmen any protection whatever, that is, <sup>the just</sup>  
provide protection <sup>that was something not to do; he said he was going</sup>  
couldn't without going to war, and President Wilson had promised <sup>(to keep</sup>

But nothing he hadn't promised <sup>was</sup> to keep our ~~own~~ merchantmen sailing on the high seas <sup>from fear of being pulled to the</sup>  
out of the war. Hence, after the German declaration of unrestricted submarine

there was nothing <sup>our</sup> could do except keep  
warfare ~~American~~ ships ~~kept~~ within American harbors, <sup>because</sup> they were afraid to

because they would certainly  
leave ~~and~~ become helpless victims of submarine torpedoes--with large losses in

This situation was unbearable but, as <sup>us</sup>  
life to be expected. ~~I've~~ I've said, President Wilson was determined to keep <sup>us</sup> America

out of war, just <sup>as</sup> ~~like~~ the Scandinavian and certain other countries in Europe were

keeping out of it. <sup>But</sup> ~~his~~ position was a very difficult one; his own ambassador

in London wrote in his diary:

"I predict that the President cannot be made to lift a finger  
for war--until the Germans should actually bombard one of our ports. It's  
cowardice or pacifism that holds him back every time" <sup>defferentialism,</sup>

On the whole, <sup>our</sup> ~~American~~ sympathies were with the Allies but the feelings of  
a large German-American population had to be taken into account, especially when  
British high-handed action, every once in a while, severely prejudiced their case.

Still, the President held back. <sup>So</sup>  
~~So the U.S. official attitude and position was, as I've indicated, very difficult,~~

One writer, commenting on President Wilson's conduct, said that he "was hesitating  
on the brink of war, reluctant to plunge into it, clinging painfully to the idea

How  
down  
to  
p. 7  
insert

from fear of being pulled to the



<sup>Solve an enemy's cryptosystem and as a result</sup>

It's a nice thing to ~~have solved the~~ code, or cipher, or enciphered code, gain information which in pretty nearly all cases is indubitably authentic because it comes ~~not to have as a result some~~ information right out of the horse's mouth; but the information without arousing the enemy's suspicion as to its origin if you can't use ~~it~~, what good is it except, perhaps, for historical purposes?

in the COMINT business we try our best to eat our cake and still have it, and we try this hard

In other words, it's one thing to have COMINT—and another, to use it properly,

that is, so as ~~not to try up the source of the COMINT~~ to continue to receive

the blessings which flow from your crypto-astuteness and good security. Another way of putting the matter I'm going to discuss at some length <sup>today</sup> is to say that ~~it's~~ pretty nearly every day. Our record hasn't been too bad and now ~~this afternoon~~ we're going to observe an excellent case illustrative of

an enduring cryptologic two phenomena <sup>so</sup> these ~~points~~ which are often hard to join in marriage, viz, using the COMINT to its utmost advantage and at the same time protecting its ~~source~~ <sup>source</sup> so as not to dry it up at its source.

of strict neutrality which seemed to be almost a part of his religion."

But maybe a bit of politics got mixed up with the religion because, as some of you may remember, the Democratic slogan for President Wilson's campaign for a second term was: "he kept us out of war". And let's not forget the other famous explanation he gave for keeping out of war; his statement that "there is such a thing as being too proud to fight!" *I would try to defend that.*

There was another factor we must keep in mind. For a large part of the United States, especially the Middle and Far West, the war in Europe was 3,000 miles across the Atlantic. ~~It~~ *It* might as well have been on another planet so far as

the people who lived in those parts of our country were concerned.

*Insert 1 from p. 6 suggest attached*

*which involved what I've termed "a"*

~~What came the "cryptologic opportunity" which formed the principal part of~~

*It was an event (almost*

~~in the title of my talk, this morning, and which, overnight, it seems, the episode~~

~~of the interception and solution by the British of the Zimmermann Telegram.~~

entirely changed the picture. What was this opportunity? It was the disclosure  
*event and the*

Now, historians may disagree as to why the United States became a belligerent

~~in World War I; some of them~~ *even* ~~still~~ *still* believe ~~that~~ we went in on the wrong side. But I

think that most historians would now agree that it was the *interception and* solution of the Zimmermann

Telegram and the brilliant way in which the British used it, that brought ~~the~~ *us* United

~~into the war~~ *just in the nick of time, and on the right side —* when she was brought in, and brought ~~to~~ *us* the side of the Allies."

*could now be no doubt whatever as to the outcome of the war.*

*Insert 2 attached*

<sup>most</sup> 2/ After severing diplomatic relations with  
Germany something had to be done, of course,  
to try to give our merchant ships some  
protection and the question of arming them  
to protect themselves was discussed.  
The idea was to let the Navy provide  
guns and trained gunners to handle them.  
And on 26 February, President Wilson

addressed Congress in joint session to advocate that course of action. A bill known as the Armed Ship Bill was introduced in both Houses of Congress, and on 1 March it passed the House by a vote of 403 to 13. In the Senate it was less fortunate; it became the subject of acrimonious debate which finally developed into a filibuster led by (2)

Senator Fa Follette of Wisconsin. The filibuster was successful and succeeded in preventing passage of the bill Wilson wanted. But the President still had a way open to him to do what he wished done - his constitutional powers to direct the Navy to furnish the guns and gunners for American ships that had to pass through the German-declared war zones.

"While the Armed Ship Bill was under discussion in Congress another ... ~~an~~ event occurred, <sup>which</sup> caused the greatest excitement throughout the country and aroused the people of the United States even more; Secretary of State Lansing wrote, "than the announced policy of submarine ruthlessness." What was the event? It was the one

(4)

is for the most part a strictly authentic and truthful account. J.  
 The Cronkite film hardly needs comment to indicate the importance which  
 that it ~~will~~ portrays

the ~~publication of the~~ Zimmermann Telegram exercised upon history, ~~and the~~ because what  
 almost immediately followed the disclosure of its contents  
 publication must inevitably be considered in any study of the causes which

led to ~~the~~ <sup>our</sup> entry of the United States ~~of America~~ into ~~the~~ World War I and the role played  
~~Incidentally~~ by our country.

The whole episode is replete with drama, <sup>found</sup> and ~~it~~ has been reported in a really <sup>of the</sup> dramatic manner on a recently presented TV program that was one <sup>of the series</sup> of historical episodes recounted on Walter Cronkite's "You are There!" <sup>series.</sup> Some of you

may have seen it when the program was presented "live" <sup>over WTOP-TV</sup>; some of you may have seen it as recorded on motion-picture film, a copy of which <sup>is owned by NSA and which</sup> I've borrowed from the Office

of Training, <sup>sound-track</sup> ~~and~~ that film we now are about to see and hear. I'd like to add that

the Zimmermann Telegram of 16 January 1917 was the subject of a radio broadcast

by the British Broadcasting Corporation ~~and~~ <sup>on</sup> as recently as 26 May 1958. I'm

trying to get a transcript of that broadcast. I mention this to show you that

the <sup>subject</sup> Zimmermann Telegram is <sup>still</sup> quite a live <sup>one</sup> subject <sup>more than</sup> today -- 40 years later!

Now let's have Walter Cronkite's <sup>film</sup> "You are There!" ~~account of the Zimmermann~~

Telegram episode which he presented under the title "The secret message that

~~plunged America into war.~~ <sup>After that I'll take up the background and detailed</sup> ~~account of this spectacular and fateful cryptologic episode of World War I.~~ \* \* \* \* \*



careful study by <sup>cryptologists</sup> ~~historians~~ as well as <sup>historians</sup> ~~cryptologists~~. It is a story replete with lessons on the disastrous consequences of weakness in "C-power", <sup>as well as</sup> ~~and with~~ lessons on the opportunities attendant upon ~~great~~ strength in "C-power". ~~And,~~ ~~in passing, I may add that the story as it now appears in the history books and popular accounts of the Zimmermann Telegram episode <sup>contains</sup> ~~contains~~ errors, in ~~time,~~ ~~some of which will be pointed ~~out~~ ~~later~~.~~~~

I think it correct to say that history attributes <sup>our</sup> ~~U.S.~~ ~~entry~~ <sup>on</sup> 6 April 1917 ~~into~~ <sup>World War I</sup> ~~WWI~~ as a belligerent on the side of the Allied Powers. to the disclosure of the contents of the Zimmermann Telegram. Note that this statement is qualified

Just before the film Starting started I said I'd get into it after showing you the background, <sup>of this episode and give you a</sup> ~~and~~ detailed account of this, the most spectacular and fateful, <sup>single</sup> cryptologic episode of World War II, <sup>or of World War II, for that matter. I think that</sup> cryptologic history <sup>throughout</sup> ~~throughout~~ <sup>the</sup> episode of World War I, <sup>an episode of such importance in</sup> ~~the~~ <sup>war</sup>.

You will recall that in the Cronkite story question was raised as to <sup>the reasons for</sup> the delay between the date the Zimmerman Telegram was sent, ~~16~~ <sup>10</sup> January 1917, and the date its contents were communicated to the American Ambassador, 24 February, ~~or~~ <sup>a</sup> period of almost six weeks. Why did it take so long? <sup>This was a question</sup> many persons asked. Wasn't that suspicious? What kind of British skullduggery was being covered up? Walter Cronkite <sup>tried to</sup> give an explanation. He said, <sup>or rather hinted</sup> that the story was held back <sup>until</sup> the Germans changed their code. Then the Zimmerman Telegram could be published without harm to British intelligence. Well, let's see. At this point perhaps I should say that <sup>the</sup> ~~the~~ <sup>principal</sup> idea behind my talk is to account for <sup>this</sup> ~~the~~ <sup>delay</sup>.

by a date, viz, 6 April 1917. Perhaps that would have come about without the

and ~~I think it would~~  
 Zimmermann Telegram, sooner or later, for one reason or another, ~~the~~ most

because probably ~~as a result~~ of German ruthlessness in the conduct of submarine warfare.

But "later" might have been too late, because after ~~February 1917~~ when

unrestricted submarine warfare started there wasn't much time left to help

Britain, ~~and her Allies, because England was being starved for food and munitions,~~

And if ~~America~~ <sup>we</sup> had waited until England had been starved into starvation and capitulation, it is <sup>of course</sup> possible that ~~America~~ <sup>we might</sup> would never have entered ~~into the war.~~ <sup>the war.</sup>

Or, if ~~it was~~ <sup>we were later</sup> forced to ~~enter~~ <sup>fight</sup> because of ~~German~~ <sup>we</sup> arrogance, ~~it~~ <sup>we</sup> might have been left to ~~face~~ <sup>had</sup> a powerful and jubilant Germany all alone. Who knows?

The fact is, however, that the Zimmermann Telegram was <sup>sent on 16 January 1917, its decrypted plain text was</sup> published on

March 1st, and within a little over one month, <sup>after publication</sup> on April 6th, ~~we~~ declared war on

Germany. <sup>According to practically all historians</sup> There seems to be little doubt, ~~therefore~~, that ~~America~~ <sup>we</sup> entered the

war when ~~we~~ <sup>Perhaps we in the cryptologic</sup> did because of the Zimmermann Telegram, ~~or shall we say~~, rather, <sup>field should be a bit more specific and say that we entered</sup> as a consequence, on the one hand, of German obtuseness in affairs diplomatic

and naivete in affairs cryptologic; and, on the other hand, <sup>we should add, that we entered into it</sup> first because of <sup>second, because of their</sup>

British astuteness in affairs diplomatic, and brilliance in affairs cryptologic. Or, should these two reasons be interchanged in their order. I'll let you be the judges.

impact that disclosing the

The Cronkite film has, <sup>in some</sup> dramatic, portrayed the contents of the Zimmermann Telegram had on Congress. It was only to be expected that question and doubt should be raised as to its

authenticity, of the Zimmermann Telegram. The newspapers were full of denunciations and discussions of what many people regarded <sup>at first</sup> a complete hoax, a patent fraud. In the Congressional Record the debate on March 1st takes up 22 whole pages--all devoted to the question of the authenticity of the Zimmermann Telegram,

which had so far nothing to back it except the word of the Washington Correspondent of the Associated Press, <sup>for</sup> ~~you~~ <sup>made</sup> the disclosure.

The publication had not been made on the authority of the State Department. <sup>Charge as it may seem, it had</sup> ~~Associated Press~~ at all. It had strangely appeared merely as a dispatch, ~~sent~~ <sup>sent</sup> broad

<sup>What was widely distributed</sup> ~~and~~ apparently upon its own responsibility. <sup>You will recall this point in the</sup> ~~Cronkite Film~~ <sup>Congressional</sup>

~~It is certain that for so many years should the Zimmermann Telegram in a~~

But now let's lift ~~the secrecy veil a bit.~~ <sup>It will be of interest to</sup> ~~lift~~ <sup>lift</sup> tight veil of secrecy. Let's begin with a brief

~~start~~ <sup>start</sup> in with a brief story about how the British cryptologic organization got

started. I should tell you that according to the historical accounts, and I know they're true, the British Government had no crypt-

Read from Ewing lecture at Edinburgh 14 December 1927.

analytic organization in being within World War I, <sup>be</sup> ~~out~~ Oh!

Read from Ewing Room 49, page 173-4.

<sup>previously</sup> I know there had been a long, long tradition of code and cipher solving by British Intelligence agencies

and this is true. <sup>But</sup> ~~that's~~ another story and I don't

<sup>wish</sup> to go into it at this time. <sup>all</sup> I want to say at <sup>being</sup> ~~is~~ that there was <sup>no</sup> cryptanalytic organization <sup>in</sup> the British Government when war came in 1914. <sup>Just</sup> as

19

official crypt REF aid 463374 in Washington

There was no ~~in the American Government~~ when we entered World War I as a belligerent in April 1917. In both cases there had to be improvisation with amateurs taking the leading roles, not professionals. Let me read from a letter dated - mark this well - August 23, 1958 written to me by Cmdr A.G. Denniston, who was for a number of years before World War II, and for a couple of years during that war the head of the British crypt-analytic organization.

copy from HTR

See marked portion beginning "But do remember"

Cmdr. Denniston's mention of Sir Alfred Ewing requires a bit of elaboration. You'll find a good deal of information about him in a book by his son, published in 1939, after some clearance bouts with the authorities. The book is entitled The Man of Room 40: The life of Sir Alfred Ewing (Hutchinson & Co, London, 1939). Has mentioned in several other books, and in particular a book published in 1955 by Admiral Sir William James, entitled Eyes of the Navy. ~~Admiral James~~ James devotes a good deal of space to the part played by Ewing in World War I. Let me quote from that book which is primarily about Admiral Sir William ~~James~~ Spencer Hall.

p. 24 - 1st par.

After follows a few paragraphs on codes and ciphers, there follows this paragraph:

bottom of p. 25 + top 3 on p. 26

\* \* \* \* \*

p. 28 - 3 paras specifically for intercepting enemy radio signals

A radio receiving station was set up - by amateurs, too, but we won't go into that - and this first station was eventually expanded into 14 stations in the British Isles. Later three overseas stations were established.

James p. 29 - 3 paras + top par on p. 30

Believe it or not, ~~according to some~~ Ewing's work for a number of months was entirely a private enterprise effort. It is not clear whether he and his small band of amateurs were paid. - I must assume, somehow or other, <sup>Ewing's</sup> they were, ~~perhaps~~ ~~what James meant~~ and he says ~~no, was that~~ the small organization did not come under any Director or Sea Lord. This situation was changed when Ewing's ~~the~~ group became a section of ~~the~~ Naval Intelligence under the overall direction of <sup>a man who soon after the war</sup> gained a great deal of publicity as a result of the work of the people under him, Admiral Sir W. Reginald Hall. Ewing continued to be <sup>technical</sup> the head of the group until he became Chancellor of Edinburgh University two years later.

Ewing and his small team were University men - not naval officers; as a result their translations of German naval signals were strange things in the eyes of the very few men in the Naval Operations staff to whom the translations went. And, of course, the gifted ~~of the~~ <sup>cryptanalysts</sup> amateurs became the butt of jokes and it was a long time before Admiral Hall was able to break down the prejudice against their work. The amusing thing to note is that Hall had assigned a Navy Captain to put the translations into proper naval

until 6 November 1914, when he not only was allowed in Room 40 but "became Hall's representative in charge of the staff of cryptographers."

language - but that officer wasn't permitted to have access to the room where the cryptanalysts worked or to have any personal contact with them. It is also reminiscent of certain <sup>early</sup> days in the history of our own cryptanalytic organization to learn that ~~it~~ for a good ~~while~~ many months <sup>one and</sup> only one person <sup>was permitted to</sup> receive the translations - the Chief of Staff, to whom they were personally handed in a locked book! But now it's high time I got down to the real cryptologic details, which had been <sup>of the Zimmerman Telegram, details</sup> ~~completely~~ shrouded in mystery for almost ten years before the ~~certain amount of information began to leak out~~ <sup>veil of secrecy was lifted a bit by a story in the</sup> November issue of a now defunct American magazine called World's Work, <sup>in which was</sup> published the final installment of a book by Burton J. Hendrick, entitled The Life and Letters of Walter H. Page. <sup>Since then other accounts</sup> have appeared, perhaps the best and certainly the latest one being that in <sup>late 1914</sup> Admiral Sir William James' <sup>entitled</sup> book, The Eyes of the Navy, which I've <sup>already</sup> mentioned. But let's begin with the version given in the Hendrick account, <sup>not only</sup> because it's pretty accurate, having been based upon certain telegrams exchanged between our ambassador in London and the State Department in Washington but also because it's quite dramatic.

Insert

I think Walter Cronkites story <sup>used a lot</sup> ~~was based~~ of information that appeared first in this Hendrick account. And in passing I might quote ~~it~~ from an <sup>address</sup> ~~speech~~ delivered on 6 November 1925 by Lord Balfour who, speaking at a luncheon given at Edinburgh University said, as reported in The Scotsman of 7 November 1925:

see me  
p. 240 Ewing

Soon we shall learn the part Balfour played in our story of the Zimmermann Telegram.

22

22



Here copy <sup>material in</sup> p. 23 & 24 to end of Telegram <sup>indicated</sup> Page, 2d col p. 24.

World's Work and from time to time make comments.

*indent quote*

at the moment

We shall not concern ourselves with the steps taken by President Wilson and Secretary Lansing, culminating in the publication by the Associated Press and Secretary Lansing, culminating in the publication by the A.P. of the text of the Zimmermann Telegram. Our attention will be concentrated upon the minute details of the manner in which the message was intercepted and solved.

*first*

Copy part of p. 24 1st para p. 25 to point indicated 8th line, ending with

*indent*

(Continue reading from Hendrick, p. 24 "manner in which" . . . etc to

"the most fateful message sent to America during the war." Go on with following

~~from p. 26, 1st col~~ "In the British Admiralty this Nauen-Sayville thoroughfare was known as "the main line"; it was the most direct and consequently the one most used for sending German dispatches to the United States."

Hendrick cites no authority for the statement that the Zimmermann Telegram was transmitted by radio from Nauen to Sayville. There is very good reason to doubt it.

A few hours after outbreak of war the British, who've always recognized the importance of control of communication channels as well as sea lanes took immediate steps to isolate Germany from the rest of the World that lay beyond the

oceans, by cutting and diverting to her own service the two German cables across the Atlantic, leaving only indirect channels of communication with her ambassador at Washington. These were four in number.

- (1) <sup>Best</sup> Radio <sup>From Germany, to</sup> <sup>London, New York,</sup> <sup>and Tuckerton, New Jersey.</sup> <sup>Both routes were</sup> <sup>(supervised</sup>

by the U.S. <sup>and</sup> <sup>were</sup> <sup>well supervised to protect our neutrality.</sup>

- (2) <sup>For</sup> Cable from Germany via Berlin-Stockholm-Buenos Aires, Washington--

but this route was secret from <sup>the United States Government,</sup> U.S. although there is positive evidence that it was quite

<sup>You see,</sup> well-known to the British from the first days of its use, <sup>for</sup> the cable from Stockholm to Buenos Aires passed through England; <sup>as</sup> "the Swedish Roundabout." <sup>and</sup> the route was jocularly called by <sup>Room 40</sup>

- (3) <sup>Another cable route</sup> <sup>to</sup> <sup>Via Berlin, Copenhagen,</sup> Washington, <sup>and</sup> this cable also touched

English soil. This was a very unusual channel for the Germans because it could be used only with the knowledge and cooperation of the U.S. <sup>United States Government.</sup> <sup>more about that</sup> <sup>channel</sup> <sup>later,</sup>

- (4) <sup>The last route</sup> <sup>Involves inserting</sup> <sup>secret text in ordinary news dispatches</sup>

<sup>we learned about it</sup> <sup>when this method</sup> <sup>(this was what we may call a "concealment method")</sup> and was disclosed <sup>only</sup> after the war by Berjstorff himself.

<sup>Now</sup> <sup>As to the first method,</sup> the use of the radio channel <sup>from Nauen to Sayville or Tuckerton; its use</sup> was prohibited except <sup>and effective.</sup> and I am glad to say that the supervision <sup>under American supervision/exercised by American authorities was very detailed,</sup>

Hendriek is absolutely wrong when he says (p. 25, 1st column) ". . . how little this

prohibition interfered with the Germans is shown by the use they made of

the Long Island station for this, the most fateful message sent to America

during the war." I have very carefully searched every available record and

have found not the slightest evidence that this channel was actually used,

*for the Zimmermann Telegram*

*by me* *the* *accounts of yours*  
The German accounts have been examined as well as American.

*in learning just how the* I suggest you study his brochure on the Zimmermann  
supervision was exercised, *Eng. Chiffre 9072* *Read from p. 7 and 8 of*

*brochure, paras checked*  
Telegram (pages 7 and 8). I think you'd agree that great care  
was taken by the authorities who had the responsibility of seeing  
to it that ~~we~~ lived up to our international obligations *which strict neutrality*  
No, the Zimmermann Telegram wasn't sent via that route, although

Hendrik's account makes it plausible by saying:

*Hendrik p. 25, col 2 beginning*

*col 25, col 2* "On the 16th of January, 1917 . . . etc. whole

column to 1st 2 lines p. 26). *II* Does Hendrik want to imply Berystorff

*this lure which the Mexican President Carranza was to swallow?*

added this precious bit of enticement? No, Hendrik's explanation is quite

*wrong; it is, in fact, misleading and perhaps intentionally*  
~~flat~~ and disingenuous. We shall soon learn the real explanation for the

gaps and doubtful points in the text of the message as first intercepted.  
*It will go a long way to explaining the 6-weeks' delay we've been trying*  
*to explain.*

We come now to the second communication channel used by the German

Government etc. . . . bottom p. 8 of brochure *to end of line at top p. 9*

*see me*



German Foreign Office Communications.

more than one route was routine procedure with <sup>in</sup> Derystorff. But Hendrik

says:

indent quote

see me

Hendrick. P. 26, Col. 1 - two <sup>two</sup> ~~marked~~

Read from p. 26 of Hendrik, Column 1. Hendrik's statement "In many

capitals German messages were frequently put in Swedish cipher and sent to Swedish Ministers...

implies that the British read Swedish codes, too. Now it would be easy to believe

etc. p. 10 of brochure - 4 paras + to point on p. 11 marked stop at end of top

Read from p. 18 of brochure - Now it would be easy to believe

One of these two pieces of evidence is going to stick over with the memo statement that it involves the publication by our State Department on 8 September 1917 of certain messages known as the German "Sturlei veranlet" or "sent without trace" messages.

We come now to the third and most interesting of the Zimmermann

Telegram routings--the one used with cooperation of the State Department. I quote from the Hendrick narrative:

see me

Page 11 of Brochure, this small type indent matter beg. "The German..." and continue on p. 12, 13 to point marked stop at line.

Hendrik makes it appear that obtaining permission to use State Department

facilities was a rather simple matter p. 12 brochure--all the page to

end place p. 13 marked "stop here".

I am in a position to say categorically that the State Department was indeed careful in placing its communication

facilities at the disposal of the Germans. Mr. Lansing not only realized etc.

see me

Continue with matter in 2d para on p. 14

(Read from p. 14 brochure - one para only.)

That story, too, is very interesting but of course it is not... The British read Swedish codes, too. Now it would be easy to believe... One of these two pieces of evidence is going to stick over with the memo statement that it involves the publication by our State Department on 8 September 1917 of certain messages known as the German "Sturlei veranlet" or "sent without trace" messages. We come now to the third and most interesting of the Zimmermann Telegram routings--the one used with cooperation of the State Department. I quote from the Hendrick narrative: see me Page 11 of Brochure, this small type indent matter beg. "The German..." and continue on p. 12, 13 to point marked stop at line. Hendrik makes it appear that obtaining permission to use State Department facilities was a rather simple matter p. 12 brochure--all the page to end place p. 13 marked "stop here". I am in a position to say categorically that the State Department was indeed careful in placing its communication facilities at the disposal of the Germans. Mr. Lansing not only realized etc. see me Continue with matter in 2d para on p. 14 (Read from p. 14 brochure - one para only.)

... or codes

We come now to a study of the code used for the Zimmermann Telegram. Note the plural - "Codes" - that's very important in this case, as you shall see. and, first, its passage from Berlin to Washington: there can be no question that the message, <sup>as the code used for</sup> which carried the Zimmermann Telegram (it bore the No. 158) was the one which had

been appended to Berlin-Washington <sup>message</sup> No. 157, and which <sup>was</sup> had been sent via State Department channels. As I've already said, the British Government

has officially never published any account of the interception and solution of the Zimmermann Telegram by its ~~cryptologic~~ <sup>cryptanalysts in Room 40,</sup> agency commonly referred to as

~~Room 40.~~ <sup>the</sup> But when we study very intently telegrams that passed between the British and American Governments dealing with the Zimmermann Telegram

as related in the Hendrik account - and more especially now, the account contained in ~~the book published only three years ago by a close~~

The Author's Foreword to Admiral James' book,

~~associate and war-time colleague of Admiral Hall,~~ <sup>we can see certain things</sup> ~~This is the book, Eyes~~ that illuminate the dark or dubious points in the story. of the Navy, by Admiral Sir William James.

Admiral James in his forward says:

Read from p. xi and xii to point marked

But Admiral James was careful. Even though, as he says, he had no access to unreleased official papers and there <sup>fore</sup> ~~as he says~~, it wasn't

I'm fortunate to be able to show you what Mr. de Grey looked like. In my many talks with him not once did he mention the role he played in the reading of the Zimmerman Telegram - not did anyone else in the organization (over)

in which he was ~~the~~ Deputy ~~Chief~~  
to Sir Edward Travis, the Chief.  
I have no photograph of the  
Reverend Montgomery to show you.  
But Nigel de Grey was and looked  
the part of a character in Dickens or in  
a spine-chilling mystery ~~encountered~~  
in book or on stage.



necessary for him to obtain official approval for publishing his book, he

did submit it for some sort of blessing, if not approval, ~~as this memo to~~

*report* *1955* *This I learned in a*  
~~dated~~ 15 December from our ~~then Deputy Senior~~ Liaison Officer ~~to GCHQ~~ *in London,*  
who said: " : :"  
~~clearly shows.~~

~~Read from~~ Larkin memo.

"A" attached

~~And perhaps it's not strange to say~~ *PP* *Apparently* Admiral James himself *didn't* ~~doesn't~~

know the delicate and interesting technical points about the Zimmermann

Telegram which ~~remained~~ *in my own mind at least, if not, in the* ~~remained~~ obscure or in doubt until he published his book. *minds of others -*

*the same* *said of :* And ~~it is~~ can be ~~about~~ his clarification, --unintentional, I'm sure, of

other dubious points about the history and operations of Room 40. ~~But we~~ *can't go into these except as they deal with or impinge upon* ~~But we shall have to confine ourselves to the verifiable facts about~~

*involved in* the cryptology of the Zimmermann Telegram.

Let's begin by quoting from Admiral James' account. (James, p. 136 --

*See me.*

"Then early in the New Year (read p. 136 and 137 to point indicated and comment

re the truth of what James says about the source of the DeGrey-Montgomery

message. ~~(Incidentally, describe DeGrey).~~ *#space*

*Doesn't interested* There are reasons to believe that the version *of the Zimmermann Telegram you've* ~~that we have~~ just seen

came from the ~~British~~ copy of the State Department message containing Berlin's

Nos. 157 and 158 to Washington--but I don't think it would ~~have~~<sup>be</sup> been polite

~~at the time~~ or even now to ~~say~~<sup>impute</sup> intimate ~~was~~ that the British were also

intercepting and studying messages of the U.S. Government! I wouldn't ~~even~~<sup>had to</sup> mention such an idea were it not a fact that soon after we came into the war our ally Britain ~~officially~~<sup>officially</sup> told us that our codes weren't safe!  
(Then go on with last paragraph p. 137 and continue with p. 138 and 139)

to point indicated, ~~at~~<sup>in</sup> middle of p. 137.

Berjstorff tried desperately to have Berlin change its decision about unrestricted sub<sup>marine</sup> warfare--to no avail.

On 1 February, Berjstorff ~~presented~~<sup>officially handed in his government's announcement</sup> the declaration re sub-warfare which that unrestricted submarine warfare would begin that day. President Wilson broke off relations two days later, on 3 Feb.  
As we have already noted, sets continue with the story as Admiral James tells it: Resume reading James, p. 140, middle paragraph only. See me

Hall then took steps to obtain the additional evidence that he required ~~in the~~<sup>event of an exposure</sup> circumstances and telegraphed to his secret agent in Mexico City, to

get all copies of Berjstorff's telegrams to Eckhardt since 18 January. These ~~were~~<sup>to be</sup> the British military in were sent to Washington and forwarded by cable to London in British cipher. No hitch developed in ~~his~~<sup>his</sup> nice arrangement. <sup>^</sup> were then to be

James goes on: "So much progress with the reconstruction of the code had

been made that by February 19 Hall had in his hands an almost perfect trans-

cript, and James then gives the text of the Zimmermann Telegram as <sup>generally</sup> published in the history books.

At this point I want to tell you about the "M.T." referred to in what I've just said. [Continue with what's attached]

Mr. "T" was a British operative or secret agent in Mexico City. In a rather old way <sup>and quite by accident</sup> he turned out to be a most useful character in the drama of the Zimmermann Telegram.

Copy portions marked on p. 134-135

When "H" was replaced by secret agent "T" <sup>of James</sup> the good work went on, and that's how Hall in London was able to get a copy of the Zimmermann Telegram in the form <sup>in which</sup> it was sent <sup>Bernstorff in</sup> from Washington to Eckhardt in Mexico City. <sup>possession of that version of the message</sup> He turned out to be of crucial importance! As Admiral James says (p. 141):

*one-part code known as Code 13040*  
*10,000*  
*newly*

But James is throwing a little dust in our eyes. The version of the Zimmermann Telegram that was finally published was not the version that

was in the telegram from Zimmermann to Berystorff, <sup>the latter was in a comparison</sup> which ~~was~~ in code 7500.

Whereas

but the equivalent version that was in the telegram from Berystorff to

Eckhardt, <sup>although quite similar in content,</sup> ~~and that~~ was in the older and much simpler, <sup>a much</sup> ~~13040~~ <sup>one-part code known as Code</sup> code.

*Here's the message in its -13040 clothing:*

*Read the message entire as given on p. 141 James.*

*message as on p. 141 if omitted continue*

*Continue with p. 142 down to stop. Omit next paragraph and continue*

as follows:

But by this time Hall had information that the German-Americans in the U.S. <sup>had</sup> were extremely active in their endeavors to stay the President's

hand. He felt that the time had come for immediate action and formally <sup>as regards bringing the Zimmermann Telegram to the attention of President</sup> pressed for a decision. <sup>Wilson</sup> On 20 February he received Balfour's authority

to handle the whole matter as he saw fit. *James continues the story:*

*"Prolonged discussion with De Page etc."*

*Continue with p. 143 James--whole page, and ~~top lines~~ on pp. 144, then*

*and 145 to end of 3rd para. on p. 145*

We've already heard <sup>and seen</sup> the contents of the message from Page, the American Ambassador, in London, to the President and Secretary of State, so I won't repeat it now. You'll recall that in that telegram Page stated:

*P. 144 215*

that "early in the war the British Government etc. read extracted and marked paragraphs on p. 144, James.

But now listen to James: (p. 145) "It was not the case etc -- just that

p. 18 of brochure beginning "When Ambassador Page paragraph and the next one and then continue from p. 16 of F-M brochure and

2<sup>nd</sup> page

read all the way to bottom of page 16 of brochure ]

place around the cryptanalytic feet every security safeguard he could devise. If necessary Nobody can blame Hall for trying to put everyone including Page, the he would put off on the wrong trail anybody ~~that~~ he thought might jeopardize security so as President, the Secretary of State, off on the wrong trail and to cover the

tracks of Room 40. At the time this brochure [hold up F-M brochure] was

written we didn't know all the facts -- we were <sup>using</sup> making inferences and <sup>making</sup> deductions.

We said:

2 marked paras of brochure

Read two marked paragraphs on p. 17 of brochure.

We felt that "cipher book" cryptographic The statement that a codebook -- or at least some sort of code document --

or captured must have contained but we didn't know just how was found must contain an element of truth, because here is what the Ewing <sup>turned over to us</sup> <sup>copy of their</sup> <sup>13040 code</sup> <sup>didn't pay anything about it</sup> <sup>having</sup> <sup>been constructed upon the basis of</sup> <sup>Jan's code that they'd</sup> <sup>But that's exactly what they'd done, as I have since there got able that.</sup> <sup>For instance, in Ewing (p. 18) we read the following:</sup>

Note the illuminating statement

Ewing says that the captured material enabled the workers in Room 40 to

read much enemy dip correspondence, "thus providing a starting-point from

which to penetrate, one after another, the German Foreign Office Ciphers."

all the Ewing p. 187 - When the p. 188 - "psychology"

~~On the other hand,~~ <sup>Admiral</sup> James <sup>too,</sup> gives us much more specific and valuable

information on this point. ~~add I think it is accurate.~~ (James, pp. 69-70)

James pp. 69-70 In April etc

~~Read James p. 69 to top p. 70. In April (1915) something~~

With the aid of our able archivists I've been able to dig out of the old  
~~if I'd had more time to prepare for these talks before coming out~~

files of World War I.

here it is.

~~I would have sent~~ German Code 13040; ~~put with my slides, etc.~~ It's

an interesting document. ~~as also is~~ Englecher Chiffre 9972 and Code 7500--

~~these are all in our archives now.~~

But to get back to the Zimmermann Telegram itself again, you will recall

that I said it was published in all the important newspapers of the world

In pro-German circles the telegram was immediately denounced as a forgery  
on March 1st, 1917. After acrimonious debate a resolution was passed by

the Congress that the President be asked to state the source of the informa-

tion. He replied the same evening through his Secretary of State as follows:

~~Read James, p. 147 -- Lansing and next paragraph: marked beginning of sentence~~  
~~on p. 148 to end~~

Zimmermann in a statement before the Reichstag made a long, involved

and foolish apology for his inept conduct, ~~making up with this~~  
made and foolish apology for his inept conduct, ~~making up with this~~ and he

gave error because if he'd [insert matter on next page]

~~Read James p. 148, marked paragraph.~~

How naive! How could such a naive man, <sup>as Herr Zimmermann was</sup> rise to be head of the Foreign

Office of a great and powerful state? It will hardly astonish you that  
Zimmermann continued to use Code 13040 -- and that he soon  
lost his job as Foreign Minister.

Continue with James, p. 149 and 150 to end of quoted matter at top of

p. 150.

*\* insert to preceding page*

If ~~Zimmermann~~ had been really smart he would have denounced the telegram as a forgery, <sup>a</sup> fraud, <sup>the</sup> and product of British duplicity and chicanery-- even if only to smoke the British out and make them prove the authenticity of the telegram by disclosing exactly how the message and the information contained <sup>had been</sup> in it ~~was~~ obtained.

*(Quote from James, p. 148 "American reaction..." and p. 154...)*

That is what Hall greatly feared would happen--but his fears turned out to be groundless. Zimmermann was too dumb, too slow, too inept, <sup>It was hardly actual you know. It</sup> and he soon... ~~lost his job.~~

Now go back to F-M brochure, p. 17 to end of 2d para.