Please Note: These FOLLOWING historical documents are PDF images of formerly classified carbon paper and letters that have been declassified. Due to the age and poor quality of some of the PDF 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.

## MASSACHUSETTS INSTITUTE OF TECHNOLOGY

236

CAMBRIDGE 39. MASS.

DEPARTMENT OF MATHEMATICS

Deor Major Grosjean, I have weitter RAND concerning the machine description. This was hand written and was sent to NSA late last spring, I believe, or sent to someone there. Essentially the same machine description was once sent to a Navy communication in the description to the termine center in Washington, I think. Center in Washington, I think. I have discussed the machine and theory general machine and theory general exponential conjecture with R.C. Blanchfield and A.M. Gleasen Who have worked for NSA. Recently a conversation with Prof. Hoffman here indicated that he has recently been working objectives. Since he will be consulting for NSA I shall

discuss my ideas with him. He has developed minimal redundancy coding methods. I hope my handwaiting, etc. do not give the impression I am just a crank of circle-squares. My position here is Assist. Rolf. of math. My best known work the is In game theory (reprint sent. separately). I mention these things only in the interest of securing a most careful consideration of the machine and ideas by your most competent associates. does not torn up. I will prepare another. Also I shall be happy to provide any additional information or aswer any queries to the best of my ability. queries With many thanks for your Sincerely Yours, John Hoah

## MASSACHUSETTS INSTITUTE OF TECHNOLOGY

CAMBRIDGE 39, MASS.

DEPARTMENT OF MATHEMATICS

letter concerns ENCIPHERING

Dear Sires: An enciphering-deciphering machine Cin general outline) of my invention has been sent to your asgonization by way of the RAND corporation. In this letter I make some remarks on a general principle relevant to encipheing in general and to my machine in posticulos. This pronciple seems quite impostant to me and I have some reason to believe you may not be fully aware of it. with a finite "key", operationing on binary messages . Specifically, we can assure the process described by a function Y: = t(x, d2, .... Xr; X:, Xi-1, Xi-2,.... Xi-n) where the d's, X's, and y's are mod 2 and where if xis is changed, with the other x's and is left fixed then Yi is changed.

The l's denote the "key". 12 Containing & bits of information. n is the spon maximum spon of the "memory" of the process. If n were the asguments given below would not be basically altered. To consider the resistance sham enciphering process to being broken we should assure that at same times the enemy knows everything but the key being used and to break it need only discorry the key from this information. We see immediately that in principle the enemy needs very little information to begin to break down the process. Essentially, as soon as n bits of enciptived message have been toons mitted the key is about determined. This is no security, for a practical key should not be too long. But this does not consider how easy it is for the energy to make the computation determining the key. If this computation

, although possible in principle, were 13 sufficiently long at best then the process could still be secure in a partit practical sense. The most direct computation proceedure would be for the energy to try all 25 possible keys, one by one. Obviously this is easily made impractical for the enemy by simply choosing & bage enough. In many cruder types of enciptering particulosy those which are not auto-coding," such as substitution ciphers [ letter for letter, letter pair for letter pair, toiple for triple.] shorts means for computing the key are feasible, essentially because the key can be determined piece meal, one substitution at a time. So the a logical way to dassify enciphering processes is by the way In which the computation tength Tength for the computation of the key Increases with increasing tength length of the key. This is at best exponential

and at worst probably a relatively small power of r, ar2 or ar3, 4 as in substitution ciphers. Now my general conjecture is as follows: For almost all sufficiently complex types of enciphering, especially the where the mformation instructions given by different portions of the key interact complexly with each other in the determination of their ultimate effects on the entry enciphening, the man key computation length increases exponentially with the length of the key, or in other words, with the mormation content of the key. The significance of this general conjecture, assuming its touth, is easy to see. It means that it is quite feasible to design ciphers that are effectively inbreakable As ciphers, became more sophisticated the game of cipher breaking by skilled teams, etc., should became a thing of the past.

The nature of this conjecture is Les such that I cannot prove it, even for a grecial type of cipbe. Nor do I expect it to be prover. But this does not destroy its signifiance. The probability of the touth of the conjecture can be guessed at on the basis of experience, with enciphering and deaphring believe in the exponential conjecture the I think we (the U.S.) can not afford not to make use of it. Also we should try to keep track of the progess of foregen nations towards inbreakable" types of ciphers. Since the U.S. presumably does not want other nations to use ciphers we cannot expect to break, this general principle should probably be studied but the kept secret. I believe the enciptering deciphring

machine. I more the enclosering deciphring machine. I more and had too smithed to the N.S.A. via RAND has this "inbreakable" property. In addition it has several other advantages in that

the some physical machine would function both for ciptering and deciptering and that it is auto-synchronizing and recovers after isolated errors in tomsmission These properties are not typical of enciphering systems which are auto-coding. Also it is suitable for all electronic , ultra rapid, enbodyment.

I do not expect any informative answer to this letter, yet it would be nice to have some sort of answer. I would be happy to explain more fully any thing which is not clear in my letter, or to amplify on it. I have been treating my ideas as information deserving some secrecy precautions, yet I feel it is important to communicate them to the right people. I hope the material in this letter can obtain prompt consideration by very highly competent men, versed in the field.

Sincerely, Jehn Mash John Nash Asst. Prof. Math.

531 Serial: 25 JAN 1955

Mr. John Nash Department of Mathematics Massachusetts Institute of Technology Cambridge 39, Massachusetts

Dear Mr. Nash:

Your recent letter, received January 1955, is noted. Technicans at this Agency recall a very interesting discussion with you which took place approximately four years ago, and will welcome the opportunity to examine your ideas on the subject of cryptography.

A check within this Agency has, unfortunately, disclosed no information on your machine. A description of the principles involved will be appreciated.

Sincerely,

AG cc: C/S COMSEC (3) 412

E.M. Gibson Lt.Col., AGC Assistant Adi. Gen.

M/R: In Jan 1955, Mr. Nash offered general remarks on cryptography and requested evaluation of descriptive material which he had forwarded through Rand Corp. NSA Ser 236, 12 Jan 55 informed Mr. Nash that the material had not arrived. Mr. Nash in letter rec'd 18 Jan 55 states the material was sent to NSA and to a Navy Communication Center in Wash. late last spring. A check of Agency records and discussions with various individuals (R/D mathematicians and persons who might have had contact with Rand Corp.) within the Agency has undovered nothing concerning the system. This correspondence requests a description of the machine.

In 1950 Mr. Nash submitted material, in interview, which was evaluated by NSA as not suitable.

Lyons, 4128, 60372, in

Serial: 236

Mr. John Nash Department of Mathematics Massachusetts Institute of Technology Cambridge 39, Massachusetts

Dear Mr. Nash:

Reference is made to your recent letter concerning enciphering processes. The information regarding the general principles has been noted with interest. It will be considered fully, and particularly in connection with your enciphering-deciphering machine.

The description of your machine has not yet been received from the Rand Corporation. As soon as details are received, the machine will be studied to determine whether it is of interest to the Government.

The presentation for appraisal of your ideas for safeguarding communications security is very much appreciated.

Sincerely,

cc: AG

C/S

412

COMSEC (3)

D.M. GROSJEAN MAJOR WAC Actg. Asst. Adjutant General

M/R: Mr. Nash offers remarks on a general principle relevant to enciphering in general and to his machine in particular. The machine, which he is sending via the Rand Corporation, has not yet been received.

This letter informs Mr. Nash that his remarks are being noted and that the machine will be studied as soon as details are received. This reply coordinated with Mr. M. M. Mathews, NSA-31. This is an interim reply. M. A. Lynes M. A. Lyons, 4128, 60372, in

C/SEC 2-2

MASSACHUSETTS INSTITUTE OF TECHNOLOGY CAMBRIDGE 39, MASS.

D Los

DEPARTMENT OF MATHEMATICS E.M. Gibson, Lt. Col., AGC, Asst. Adj. Gren. DEOF SIT: mput Here is a description of my enciphering deciphering machine. ( cla (Cipi 25 martatics - Permuter-Reverser Adder mod 2 CLOOSA Transmitting Arrangement Retosdas R D P A output designed Receiving Arrangement & In the receiving arrangement the some components are used except for the addition of the retorder, which is a one-onit delay. The messages are

to be sequences of binosy digits (numbers mod 2). The machines work on a cycling basis, performing cretain operations during each cycle.

During each cycle the adder A, takes in two digits and adds them and sends on the sum obtained from the previous addition. The delay in this addition necessitates the retorder R in the receiving circuit.

The permutes will be described in more detail below. It takes in a digit from D during each cycle and also puts out a number. What it does, which is the choice between two permutations is determined by what digit (1 or 0) is in D at the time. The permutes always hog a time. The permutes always hog a time. The permutes always hog a the number of digits remembered within it. Each cycle it shuffles them oround, changing some I's to zeros, sends one digit on, and takes in a digit from D.

In operation the input of the receiver is the output of the transmitter. So the input to R is the some as the input to D in the transmitter. Hence the output of P in the receiver is the same as the out-put of P in the transmitter, except for a onemit lag.

So the addres A in the receiver gets: (1) the out put of A in the toansmitter, and (2) the previous input from Perons.) to A(trons). Now Since binory addition is the same as binary subtraction (i.e. + + - mad) ore the same) the output of Afreceiv, will be the previous input to A(trans.) From the input to the toans mitter, i.e., It will be the clear or inciphered message. the permuter, P, and "decider", D work as follows, illustrated by example:  $O_{+1}$ >0-60-E O blue permit 6 P

The cilles represent places where (4) a digit can be stored. During each cycle either the red permutation of digits or the blue takes place. This is decided by the digit in D at the beginning of the cycle. The D dgit moves to the first sciencle or storage place in P during the cycle after it has determined the choice of the permitation. Both premutations should cycle through all the places in P, so that a digit would be corried tot through all of them and out inder its action alone. In addition to moving digits around the permutations can change and 1's to O's and v.v. For example represents a shift of the digit in the left circle to the right with this change  $= 1 \rightarrow 0$ (For II 2->1)

The "key" for the enciphering (5) machine is the choice of the permutations. If there are n Storage points MP, not counting the first one, which receives the digit from D, then there are [n! 2"+172 possible teys. people to check on the possession of this machine of the various properties I clarmed for it in a previous, letter. I hope the correspondence I have sent in receives, cooeful affention from the most qualified people, because I think the basic points involved are very important. Sincerely P.S. Various devices Jehn Mosh could be added to the machine, but I think it would dereally be better to enloge the permuter than to add anything. Of course Assist. Rot. Math. error correcting boding could occasinally be a useful adjunct.

Serial:

1358 3 MAR 1955

Mr. John Nash Department of Mathematics Massachusetts Institute of Technology Cambridge 39, Massachusetts

Dear Mr. Nash:

Reference is made to your letter received in this Agency on 17 February 1955.

The system which you describe has been very carefully examined for possible application to military and other government use. It has been found that the cryptographic principles involved in your system, although ingenious, do not meet the necessary security requirements for official application.

Unfortunately it is impossible to discuss any details in this letter. Perhaps in the future another opportunity will arise for discussion of your ideas on the subject of cryptography.

Although your system cannot be adopted, its presentation for appraisal and your generosity in offering it for official use are very much appreciated.

It is regretted that a more favorable reply cannot be given.

Sincerely,

E.M. Gibson Lt. Col., AGC Assistant Adj. Gen.

cc: AG

C/S COMSEC (3) 412

(M/R ATTACHED)

M/R: In Jan 55 Mr. Nash offered general remarks on cryptography and requested evaluation of descriptive material which he had forwarded through Rand Corp. The Material was not received from Rand Corp. Dr. Campaigne received a letter from Mr. Nash inclosing a copy of the letter (5 Apr 54) from Rand which transmitted this material to NSA. This material was found in R/D files. In the meantime Mr. Nash sent a handwritten description of his enciphering-deciphering machine.

Mr. Nash proposes a permuting cipher-text auto-key principle which has many of the desirable features of a good auto-key system; but it affords only limited security, and requires a comparatively large amount of equipment. The principle would not be used alone in its present form and suitable modification or extension is considered unlikely, unless it could be used in conjunction with other good autokey principles.

This correspondence informs Mr. Nash that his system does not meet necessary security requirements; and expresses pleasure at the thought of an opportunity to discuss Mr. Nash's ideas on cryptography again. Such a discussion took place in 1950 when Mr. Nash submitted material, in interview, which was evaluated by NSA as unsuitable.

An interesting pamphlet on Non-Cooperative Games, written by Mr. Nash was also sent to this Agency by the author for our information.

Dr. Campaigne has been informed that the reply has been written and is not interested in further coordination.

Malyons, 4128/60372/rwb