CODES AND CIPHERS

GENERAL

Since ancient times man has used some form of secret communication to guard his written secrets from his enemy in business of war. The ancient Egyptians were reported to have invented hieroglyphics in order to secrete their wisdom from the vulgar. Historians allege that secret communications were held by means of firebrands at the siege of Troy, as early as 1184 B.C.; while Plutarch, in his life of Lysander, attributes the first use of secret writing to the Lacedemonians about 400 B.C.

Of course, these ancient means of secret writing were of the most simple types. They were sufficient, however, in that age to guard the secrets of the correspondents. With the improvement in means of communication, and particularly since the use of telegraph and radio has been developed, types of secret writing have become more complex, and naturally more difficult of deciphering by persons not provided with the keys. In modern times, systems of secret writing have been developed by the more powerful governments that surpass all comprehension of complexity by the average man.

We may well ask the question, "Why is a knowledge of codes and ciphers important to the CIC?" There are two answers to this question. First, the trained investigator must be familiar with the means which are available to him for the transmission of confidential messages pertaining to his own work that he may desire to send to his superiors or to fellow investigators. Second, he should have a knowledge of the various types of codes and ciphers which may be used by persons whom he is called upon to investigate.' It must be remembered that the principles set forth in this lecture are very elementary because time does not permit a thorough discussion of the subject. Further, it would take weeks to train investigators in the technique of solving cryptographic messages. Therefore, instruction in this matter is beyond the scope of this lecture, and we will confine ourselves, as the time allows, to a few fundamentals.

HANDLING OF SECRET MESSAGES BY INVESTIGATORS

While some secret messages that may come to the attention of military investigators will be of the simplest variety, and by those who have applied themselves to the study of cryptanalytics may be easily solved, all messages in any form of secret writing, whether visible or invisible, with all pertinent information concerning them, should be transmitted as rapidly as possible through military intelligence channels to the Military Intelligence Division, War Department, for examination and solution. Special care should be exercised not to mutilate in any way the paper containing the message, and where invisible writing is suspected the paper should be handled as little as possible.

The solution of some of the more complex types of codes and ciphers is very difficult and is accomplished only after the most careful analysis. Therefore, every available bit of information that may come to the attention of the investigator concerning the secret writing, must be transmitted with the message when it is forwarded to higher authority. Information of this type should include the following: When, where, and how the message came to the attention of the investigator; names of persons and places associated with the message; suspected nature of plain text, including subject and language; and, if intercepted by a radio transmitting station, frequency, nature of transmission, location of intercept station, etc.

While one message in even a relatively simple cipher system may resist solution of a trained cryptanalytic section, a much more complex system may be solved when there is an abundance of traffic. For this reason every effort should be made to obtain and forward as many messages as possible of any code or cipher system coming to an investigator's attention.

DEFINITIONS

Secret writing may be invisible or visible. In the field of invisible writing the characters are inscribed with certain chemicals called invisible, sympathetic, or secret inks, which have the property of either being initially invisible to the naked eye, or of becoming so after a short time. In order to make writing which has been inscribed by the use of secret inks visible, special processes must be applied. There are, in addition to the foregoing, certain methods of producing writing which is invisible because its characters are microscopic in size. These methods usually employ special photographic apparatus or very delicate mechanical instruments, called micropantographs, by means of which ordinary writing may be copied in extremely reduced size. In order to become visible to the naked eye, and hence before such writing can be read, magnifying lenses of high power must be used. Since this lecture is confined to codes and ciphers, invisible writing will not be further discussed.

In visible writing the characters are inscribed with ordinary writing materials and can be seen with the naked eye. The science which treats of visible secret writing is called cryptography, or, more popularly, codes and ciphers.

The term cryptogram is used to mean a communication in visible writing in secret language. To cryptograph is to convert a plain language message into a cryptogram by following certain rules mutually agreed upon in advance by the correspondents, or furnished them or their agents by higher authority. To decryptograph is to re-convert a cryptogram into the equivalent plain language message by a direct reversal of the cryptographing process. A person skilled in the art of cryptographing or decryptographing is called a cryptographer.

CODES AND CIPHERS

There are two main reasons for the use of Codes or Ciphers, (1) Secrecy and (2) Economy. In the business world, Codes and Ciphers are used mainly for economy, and the maintaining of trade secrets is generally of secondary importance. However, the main reason for the use of Codes or Ciphers in the military field is, naturally, Secrecy.

We have been speaking of "Codes and Ciphers". Now let us see exactly what we mean by these two word. Generally speaking, a cryptogram is said to be in cipher or a cipher system when the cryptographic treatment has been applied to the individual letters of the plain language message. A cryptogram is said to be in code or code system when the cryptogram was produced by applying the cryptographic treatment to entire words, phrases,and sentences of the plain text messages.

A cryptogram which has been produced by means of a cipher system is said to be in cipher and is called a cipher message, or some times simply a cipher. The text of the cryptogram is referred to as cipher text. The cryptographing process in this case is called enciphering, and the enciphered version of the plain language is often referred to as its encipherment. The corresponding terms applicable to the decryptographing process in the case of cipher systems are deciphering and decipherment.

A cryptogram which has been produced by means of a code system is said to be in code, and is called a code message,or some times simply a code. The text of the cryptogram is referred to as code text. The cryptographing process in this case is called encoding,and the encoded version of the plain language message is often referred to as its encodement. The corresponding terms applicable to the decryptographing process in the case of code systems are decoding and decodement.

Some times, for special purposes, the code text of a cryptogram subsequently undergoes encipherment, producing what is called a cryptogram in enciphered code,or an enciphered code message. Encoded cipher, where the cipher text of a cryptogram subsequently undergoes encodement, is also possible, but rare.

It may be stated that as a general rule all, or nearly all, cryptographic systems suitable for practical use can be broken down or solved, that is, properly-prepared cryptograms can be "translated" or read without a knowledge ~~or~~ possession ~~of~~ the general cryptographic system and the special key applying to the cryptogram. The science which deals with the principles, methods, and means employed in the solution or analysis of cryptograms is called cryptanalytics. The steps and operations performed in applying the principles of cryptanalytics constitute cryptanalysis.

CLASSES OF CRYPTOGRAPHIC SYSTEMS

Technically, there are two different types of treatment which may be applied to plain language to convert it into secret text, yielding two different classes of cryptograms. In the first, called TRANSPOSITION, the elements or units of the plain language, whether one is dealing with individual letters, groups of letters, syllables, whole words, phrases or sentences, retain their original identities but merely undergo some change in their relative positions or sequences, so that the message becomes unintelligible. In the second, called SUBSTITUTION, the elements of the plain language retain their original positions or sequences but are replaced by other elements with different values or meanings. A combination of the two treatments may be effected, but such combined transposition-substitution methods do not form a third category of methods. They are occasionally encountered but, due to their complexity, their use is restricted to correspondence between a limited number of individuals.

TRANSPOSITION CIPHERS

Transposition ciphers are roughly analagous to "jigsaw puzzles" in that all the pieces of which the whole original is composed are present but are merely disarranged. The pieces into which the picture forming the basis of the jigsaw puzzle may be divided are irregular in size and shape, but the pieces to which the plain language forming the basis of the transposition cipher may be divided must be much more regular in these messages for the sake of practicability. They must be either single letters or pairs of letters, or sets of letters in regular groupings, or finally, in an exceptional case, whole words. The majority of transposition methods, however, deal with individual letters.

It is impossible to describe here all the various means of enciphering a message by the transposition method. To clarify the method in your minds two of the best known types of transposition ciphers will be described.

One of the most common types of transposition is that called columnar transposition. In this type the letters are usually written in a geometric design, most often a rectangle, by inscribing them in the ordinary manner, that is, in horizontal lengths from left to right, and from the top downwards, and then the letters are transcribed by "reading" the columns in a sequence, known as the numerical key, which has been previously arranged between the correspondents. An example of cryptographing by this method follows:

NUMERICAL KEY: 5 -2 - 1 - 4 - 3 -6 -

J	O	E	H	A	S
E	N	L	I	S	T
E	D	I	N	T	H
E	I	N	F	A	N
T	R	Y	A	T	N
E	W	Y	O	R	K

CRYPTOGRAM: ELINY YONDI RWAST ATRHI NFAOJ EEETE STHNN K

To decryptograph such a cryptogram a rectangle with the proper number of cells as determined by the length of the message and the length of the pre-arranged sequence must first be prepared. In the foregoing example, since the cipher text consists of 36 letters and the sequence consists of six numbers, the rectangle (a) is prepared and the columns are filled in numerical order. An early stage in the decryptographing is reproduced in (b). It is only after the process has been finished that the complete message reappears as shown in the rectangle (c) below:

5	2	1	4	3	6

(a)

5	2	1	4	3	6
	O	E			
	N	L			
	D	I			
	I	N			
		Y			
		Y			

(b)

5	2	1	4	3	6
J	O	E	H	A	S
E	N	L	I	S	T
E	D	I	N	T	H
E	I	N	F	A	N
T	R	Y	A	T	N
E	W	Y	O	R	K

(c)

The method indicated above is susceptible of considerable variation, consisting in (1) changing the length and order of the numerical sequence, and (2) changing the direction of inscribing the letters of the plain language or in transcribing them to form the cipher text. By effecting frequent changes in the former a greater security may be obtained for the cryptographed message; as to the second factor, while numerous methods of inscription may be used, only the more simple combinations ~~are suitable~~ for military use. However, individual correspondents may devise and use any type, and the investigator should not expect the ciphers that come to his attention to be in the simplest form.

The degree of cryptographic security of columnar transposition methods is much increased if the rectangle is not completely filled in. The reason for this increased security can be shown only by demonstrating solution, which is beyond the scope of this lecture.

Another common transposition method of some practical importance is that known under the general name of "grille." This is usually made of a square sheet of cross-section paper, from which cells have been cut in definite but apparently irregular positions. The grille is superimposed on another sheet of cross-section paper of the same dimensions, and the letters of the message are written in the cells exposed by the perforations. Usually the grille is then given 90° turn clockwise or counterclockwise, as agreed, and the fresh cells exposed by the perforations are filled with the next letters of the message. If the grille has been prepared properly, it is possible to give it four turns of 90° each, at the end of which all the cells on the under-sheet of cross-section paper are filled with letters. The grille is then removed and the letters of the sheet underneath it are transcribed in accordance with some prearranged method to form the cipher text. Naturally, the correspondents must have identical grilles, and every step must be definitely prearranged. Although it is possible to construct grilles with many different arrangements of perforations, the necessity for carrying the device on the person and the many agreements and understandings necessary for its successful operation make the method hardly suitable for wide use. However, it may be used by individuals engaged in subversive activity.

It should be noted that all transposition methods are susceptible of one, two, or more transpositions, that is, the letters resulting from the first transposition may be again transposed, those resulting therefrom again transposed, etc. The resulting cryptograms present a very great degree of security, but methods involving more than two transpositions are seldom used because of their complexity.

While transposition methods vary greatly as regards cryptographic security, as a general rule all of them present important advantages as regards speed and simplicity. In only a few types are written memoranda required, and very often the entire cryptographic process may be easily memorized by persons of good intelligence, such as secret agents. For these reasons transposition systems are often used in espionage activities.

Transposition methods, however, present three very serious disadvantages. Any errors occurring in cryptographing or transmission may make decryptographing impossible. Secondly, if two or more messages prepared in the same key and of exactly the same length are available for study, no matter how complicated the method employed the cryptograms can be solved. Finally, in certain oases where a double-transposition process is used inevitably a careless person will fail to perform both steps correctly, thereby laying not only that particular message open to solution, but all other messages prepared in the same key.

SUBSTITUTION CIPHERS

Substitution ciphers differ from transposition ciphers in that the elements or textual units composing the original plain language retain their relative positions but do not retain their identities, being replaced by other elements or textual units so that the external form of the writing is cryptographic in appearance. They may deal with individual letters, set of letters in regular groups, syllables, whole words, phrases, or sentences. Broadly speaking when the cryptographic process involves, as a general rule, the treatment on individual letters or pairs of letters, and only exceptionally the treatment of syllables or whole words, the method is referred to as a substitution cipher; and when the process involves, as a general rule, the treatment of whole words, phrases, or sentences, and only exceptionally the treatment of individual letters, groups of letters, or syllables, the method is known as a code system, because it usually necessitates the use of a code book.

The simplest kind of substitution cipher is that which is known in literature as "Julius Caesar's cipher," but which, as a matter of fact, was a favorite long before his day. In this cipher each letter of the text of a message is replaced by the letter standing the third to the right of it in the ordinary alphabet; the letter "A" is replaced by "D", the letter "B" is replaced by "E", etc.; the word "CAB" becomes converted into "EDE." The substitution effected in this system may be shown by using a cipher alphabet, as follows:

```
Plain:  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

Cipher: D 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
```

"A" of the plain language is to be replaced by "D", "B" of the plain language is to be replaced by "E", etc. It is obvious that message can be enciphered in this manner using any type of cipher alphabets. They may be standard alphabets in the direct or reversed orders, or mixed alphabets that have been disarranged in a regular or random order. For example:

(1) DIRECT STANDARD

```
Plain:  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

Cipher: Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
```

(2) REVERSED STANDARD

```
Plain:  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
Cipher: Q P O N M L K J I H G F E D C B A Z Y X W V U  T S R
```

(3) MIXED

```
Plain:  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
Cipher: D N E O F P J Q K R L S A T B U C V G W H X I Z M Y
```

The process of enciphering a message by means of a single cipher alphabet is simple. The letters of the plain language are consistently replaced by their equivalents as shown in the cipher alphabet selected or agreed upon. For example, if the correspondents agreed to employ the cipher alphabet (1) Direct Standard, above with the relative positions of the two components of the alphabet as shown, a message may be enciphered as follows:

Message: WHEN WILL YOU ARRIVE

Encipherment: MXUD MYBB OEK QHHYLU

Should it be desired to send the message by telegraph or radio, the cipher text may then be grouped in fives and would read as follows:

MXUDM YBBOE KQHHY LUXXX

(X's are added to complete the last group)

The procedure in decipherment is merely the reverse of that in encipherment. The relative positions of the two components of the cipher alphabet must be the same as when enciphering. The message deciphers thus:

Message: MXUDM YBBOE KQHHY LU

Decipherment: WHENW ILLYO UARRI VE

The plain language is then written in word lengths:

WHEN WILL YOU ARRIVE

It is well known that the individual letters composing ordinary intelligible plain language are employed with varying frequency. Some, such as (in English) E, T, R, I, and N, are used much more often then others, such as J, K, Q, X, and Z. In fact, each letter has a characteristic frequency, by means of which definite clues are established in the solution of simple substitution ciphers. This has led cryptographers to devise methods for disguising, suppressing, or eliminating the characteristic frequencies manifested by the letters of cryptograms produced by simple substitution. One of such methods is that in which the letters of the plain component of the cipher alphabet are assigned two or more equivalents. An example of this type of cipher is one using figures as substitution equivalents, as shown in the tabulation which follows:

Plain:	A	B	C	D	E	F	G	H	I—J	K	L	M	N
Cipher:	08	09	10	11	12	13	14	15	16	17	18	19	20
	35	36	37	38	39	40	41	42	43	44	45	46	47
	68	69	70	71	72	73	74	75	51	52	53	54	55
	87	88	89	90	91	92	93	94	95	96	97	98	99

Plain:	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher:	21	22	23	24	25	01	02	03	04	05	06	07
	48	49	50	26	27	28	29	30	31	32	33	34
	56	57	58	59	60	61	62	63	64	65	66	67
	00	76	77	78	79	80	81	82	83	84	85	86

The plain language letter A may be represented by any one of four numbers, 08, 35, 68, and 87; the letter B by 09, 36, 69, and 88, etc. The equivalent used in any particular instance is merely selected at random, so that the word "CAB" may be represented in cipher by any one of a total of 64 combinations, such as 10-08-09, 70-35-09, 37-08-69, etc. In the final cryptogram the figures may be run together in groups of five. The cipher group 10080 on deciphering would be split up into 10-08-0. Another means of suppressing the characteristic frequency of the letters of the alphabet is to assign each letter a set of numbers in accordance with its relative frequency in ordinary English, so that each of the most frequently used letters will have perhaps 7 or 8 different equivalents, while letters of low frequency will have but one equivalent. The obvious disadvantage of all such methods is that the cryptographic text is exactly twice as long as the original plain language, thus increasing the cost of transmission.

In the substitution methods thus far mentioned, only one cipher alphabet is employed in the encipherment of a message. In order to provide greater security two or more cipher alphabets are often used in accordance with an agreed upon procedure. The number of such systems is quite large and it will not be possible to describe the many common methods. An example of the simplest form follows: Suppose two correspondents agree upon a numerical key, for example, 47203046, each digit of which means that the plain text letter to which the digit applies as a key number is to be replaced by the letter that stands a corresponding number of places to the right of it in the normal alphabet. For example, if R is to be enciphered by the key letter 4 it should be replaced by V; the numerical key is written under the letters of the plain language message, letter for letter, and is repeated until the whole message is provided for. Let the message be WHERE IS THE MONEY. The encipherment of the message would be as follows:

```
Plain W H E R E I S T H E M O N E Y
      4 7 2 0 3 0 4 6 4 7 2 0 3 0 4

Encipherment:  A O G R H I W Z L L O O Q E C
```

The text is then transmitted in five-letter groups: AOGRH IWZLL OOQEC. Of course, as in a simple substitution, the alphabets used may be either standard alphabets in normal or reversed order, or may be mixed by prearrangement. Also, it is possible to use different alphabets for each separate unit of the key. Such procedure adds greatly to the security of the system and the difficulty of its solution.

CIPHER DEVICES AND CIPHER MACHINES

Only a little practical experience with any of the methods so far described is necessary to convince one that on a whole they are slow, more or less cumbersome, and subject to errors that often delay or make impossible the decryptographing of messages. Furthermore, from the point of view of cryptographic security, when employed in regular voluminous traffic they leave much to be desired. Consequently, cryptographers, both experienced and inexperienced, have been let to devise apparatus which will not only facilitate cryptographing and decryptographing, but will also increase the degree of cryptographic security. Small devices constructed for this purpose, operated by hand, are often called cryptographs. Scores of them have been devised, of which only a few are of sufficient practicability for general use, and still fewer are of such construction that they produce cryptograms of unusual security. Among the better examples of such cryptographs is that employed in our Army under the name of Cipher Device, Type M-94. The degree of cryptographic security of the device, however, is not especially great, particularly when employed under circumstances where the enemy is in a position to assume with a fair degree of probability the presence in message of such words as "enemy"; "battalion"; "artillery"; etc.

There are larger cryptographic machines which are much more automatic, and can therefore be operated at a much greater rate of speed. These are usually equipped with typewriter keyboards which can be manipulated with considerable speed. The machine may also print the enciphered and deciphered text, and sometimes they are equipped with electrical transmitters and can thus serve not only to encipher and decipher messages but also to transmit them automatically. A mechanism of the latter nature is usually in the form of a modified printing telegraph apparatus. One of the cipher systems adopted for wartime use in the Army is of this type and is known as the "Printing Telegraph Cipher System." It can only be used between the larger headquarters where traffic is very great.

DISADVANTAGES OF CIPHER SYSTEMS

Aside from certain cipher machines that are operated electrically or mechanically in conjunction with a typewriter keyboard, all cryptographic methods employing cipher systems are comparatively slow, cumbersome, and subject to error. Practically all of them are open to solution by enemy cryptanalysts, and such as are suitable for use in a theater of operations can by the very nature of the limitations imposed by such use offer fewer obstacles to solution than can systems suitable for use in the zone of the interior. Furthermore, cipher systems are not economical as regards the number of time units required in electrical transmission, since the best they can do in this respect is to produce cryptograms no longer than the original plain text. When it is considered that there are other cryptographic methods which offer more advantages in respect to speed, simplicity, and economy, and at the same time afford as great, or even greater degrees of cryptographic security, it is not surprising to find that the latter methods predominate over cipher methods in those fields in which these factors are essential.

CODE SYSTEMS

We come now to a disucssion of the nature, uses and types of code systems used in communication. Considered in its broadest aspect, a code system is merely only a specialized type of substitution cipher, and, in fact, there are some systems of code which so closely approach cipher systems that no sharp line of demarcation can be established to separate code and cipher systems. As has been previously explained, the essontial difference between the two systems lies in the fact that in ciphor systems we deal with units of equal length (single letters, pairs of letters, or groups of definite length), applying some form of transposition or substitution, or a combination of the two principles, to these units. In code systems we deal with units of unequal lengths (ranging from letters to entire sentences), for which there is substituted arbitrary equal length combinations of letters or figures provided by a codebook. The cipher system may necessitate the use of no apparatus whatsoever other than pencil and paper. The code system requires the possession of identical copies of a codebook by all the correspondents.

The simplicity of code as a system of communication is one of its chief advantages. In encoding it is necessary merely to replace the various words, phrases, sentences, etc., by the letter or figure groups as provided by the codebook. In the case of words or names which are not already in the vocabulary provision is made for building up the word by means of syllables and individual letters. It is usually the case that the encoded message is somewhat shorter than the original plain text message on account of the abbreviating nature of code; sometimes a single code group will represent a long phrase of perhaps five times as many letters. This feature, of course, constitutes one of the most important advantages of code from a commercial point of view. The process of decoding is, of course, merely the reverse of encoding, and where the errors in transmission are few, it is fairly rapid. It is obvious, however, that even a small number of errors in a message may obscure the meaning or render it extremely difficult to decode.

There are various types of codebooks, depending upon their uses. Many of you are more or less familiar with the ordinary kinds of commercial and business codes used extensively for the purpose of economy, such as the ABC code, Lieber's code, Bentley's code, Western Union code, and the like. They are usually fairly large codes adapted for general commercial correspondence. Most large business firms have their private codes, constructed especially for their use and containing a more or less highly specialized vocabulary. If its use is very limited such a code may also constitute a secret code. There are also many commercial codes which are adapted to a particular industry, for example, the rubber or the sugar industry, and can be purchased by the general public from the publishers. Such codes usually have a highly specialized technical vocabulary, in addition to the general vocabulary. The principal purpose of a code in commercial practice is to effect economy in transmission, secrecy being usually of secondary importance. This is just the opposite of the case in government codes where secrecy is of primary importance and economy, while an additional desirable feature, is relatively unimportant. In investigative work commercial codes will probably come to your attention due to their widespread use. Solution of messages in these systems may be readily achieved by the use of code libraries where all of the commercial codes are available. Such a code library is maintained in the War Department.

TYPES OF CODE GROUPS

As regards the types of code groups used in codes there are two general classes: (a) letter groups; (b) figure groups. Both possess advantages and disadvantages. In those parts of the world where italic or Roman letters are used for writing, letters possess greater advantages as regards accuracy in reading by telegraph operators, this being the prerequisite to correct transmission and reception. But the Arabic digits are almost universally recognized and used, so that for communications between obscure ports and cities in certain foreign countries, figure groups are preferred over letter groups. Most codebooks contain both figure groups and letter groups, so that either may be used at the discretion of the correspondents.

The length of code groups used, that is, whether they are groups consisting of two, three, four, or five letters or figures, often depends upon the size of the code. This, however, applies almost entirely to military or naval codes, where transmission is through a government agency; for in commercial messages or in governmental communications transmitted over privately owned and operated lines five letter or five figure groups are used almost exclusively on account of regulations adopted by the commercial telegraph and cable companies. In international communications if the letter groups are pronounceable according to the common usage of any one of the following languages: English, French, Spanish, Italian, German, Portuguese, Dutch or Latin, a special tariff rate approximately 6/10 the full rate is charged. If the group is not pronounceable then each group of five letters counts as one word and is charged for at the full rate, whereupon it is seen that the cost of cablegrams using non-pronounceable groups is about double that of pronounceable groups. All governments and all commercial firms take advantage of this regulation whenever possible. Within the United States ordinary land line transmission of either code or cipher messages each group of five letters, whether pronounceable or not, is charged for as one word.

As regards their construction or arrangement, codes may be of two types: (1) "One-part" or "alphabetical" codes, in which the plain language groups are arranged in alphabetical order accompanied by their code groups, which are also arranged in alphabetical order, or numerical order. Such a code serves for decoding as well as for encoding. (2) "Two-part" or "randomized" codes, in which the plain text groups are arranged in alphabetical order, accompanied by their code groups arranged in non-alphabetical order or random order, the code groups being assigned to the plain language groups in an absolutely arbitrary and random manner, by drawing the code groups out of a box in which they have been thoroughly mixed up or by some other manner in which the element of chance operates in assigning the code groups of the plain language groups. It follows, therefore, that such a list can serve only for encoding, and for the decoding another list must be provided, in which the code groups are arranged in alphabetical or numerical order, accompanied by their meanings as given in the encoding section. The following brief extracts from typical one-part and two-part codes will serve to illustrate the difference between them:

One part code				Two part code	
		Encoding		Decoding	
ABABD	A	GAJVY	A	ABABD	Obstructed
ABACF	Abaft	TOGTY	Abaft	ABACF	Term
ABAHK	Abandon	FEHIL	Abamdon	ABAHK	Enemy
ABAJL	--------it	BAYLT	--------it	ABAJL	If it has not
ABALN	Abandoned	WITYH	Abandoned	ABALN	Building
ABAMP	----------by	NYSYX	----------by	ABAMP	Please advise
ABAWZ	Abandoning	IFWUZ	Abandoning	ABAWZ	Acceding
ABPAD	Abandonment	RUMGO	Abandonment	ABBAD	Do not attempt

The two-part code is a comparatively recent development in code systems. Its purposes are two-fold--greater secrecy and greater accuracy. For these reasons they are used by large governments for their secret diplomatic, military, and naval communications, although the cost of compiling such codes is more than three times that of compiling the ordinary one-part code.

Sometimes the code groups of a code message undergo a further process of encipherment, in which case the resulting cryptogram constitutes an enciphered code message. There are two circumstances in which enciphered code is employed, first, if the codebook is not secret and it is desirable to transmit a secret message in this code, it becomes necesaary to encipher the code groups; secondly, even if the codebook is kept secret it is desirable in the case of highly secret communications to encipher the message in order to increase the degree of security by delaying as long as possible the solution of the code by the enemy cryptanalysts. In those codes which employ pronounceable groups for the sake of economy it is obvious that the resulting enciphered code must remain pronounceable in order to take advantage of the reduced cost of cable messages, as previously explained. Hence the systems of enciphering to produce this result are rather limited, but where the resultant form of the code groups is of no importance almost any type of encipherment may be applied. The increased degree of secrecy due to the encipherment depends entirely upon the nature of the system applied.

INVESTIGATORS' CODE

At the present time any confidential or secret messages to be transmitted by investigators will be cryptographed by means of War Department systems now available in Service Commands and posts, camps, and stations. These messages will be referred to the intelligence officers of the nearest Service Command or post, who will arrange for their cryptographing and transmission. In case a need for an additional cryptographic system for use by the Counter Intelligence Corps alone becomes essential, a system will be prepared in the War Department and distributed to all intelligence agents requiring it. Instructions for its use will be issued with the system.

BIBLIOGRAPHY

For those interested in a study of the subject of codes and ciphers the following modern books in English are suggested:

Gaines, Helen Fouche - Elementary Cryptanalysis, Boston, 1939.

Hitt, Parker - The ABC of Secret Writing, New York, 1935.

Langie, Andre, Cryptography, Translated from the French by J. C. H. Macbeth, New York, 1922.

Mansfield, Louis C. S., Solution of Codes and Ciphers, London, 1936.

O'Haver, M.E., Cryptogram Solving, Columbus, Ohio, 1933.

Pratt, Fletcher, Secret and Urgent, The story of Codes and Ciphers, Indianapolis, 1939.

Thomas, Paul B., Secret Messages, New York, 1928.

Yardley, Herbert Osborne, The American Black Chamber, Indianapolis, 1931.