Elementary Military Cryptography

William F. Friedman

February 18, 2019

Contents

Chapter 1

INTRODUCTION

I GENERAL

1 Scope

This manual consists of two parts as follows:

a. Part one is an introduction to the elementary principles of military cryptography. In this part a few typical examples of cipher systems and code systems are presented; the procedure in cryptographing and decryptographing by means of the systems is shown in detail; methods of preparing keys suitable for use in connection with them are illustrated; errors and their correction are discussed; and nally, a few of the most important precautions to be observed in safeguarding systems and cryptograms from enemy cryptanalysts are set forth. Only such considerations as apply to military cryptography are included.

b. Part two develops the principles established in part one and treats of the more advanced systems. Following the presentation sequence of part one, transposition systems are discussed rst, then substitution systems. Considerable attention is devoted to combined substitution and transposition methods. Following this is a description of a limited number of cipher devices and machines, together with a discussion of their present-day limitations. Finally, code systems are discussed briey with special emphasis upon enciphered code systems.

2 Developments in Cryptography

a. Cryptography is by no means a static art or science and viewpoints are always undergoing change; what is regarded as wholly impracticable today may, through some unforeseen improvement in technique, become feasible tomorrow, and it is unwise to condemn a system too hastily. For example, before World War I, and indeed for the rst 2 years of that conict, the use of codebooks in the theater of operations was regarded as wholly impracticable.[1] Colonel Hitt in

[1]See, in this connection, Friedman, William F., American Army Field Codes in the America Expeditionary Forces During the First World War, Signal Security Service Publication,

his Manual for the Solution of Military Ciphers, published in 1916, stated:

The necessity for exact expression of ideas practically excludes the use of cod. for military work, although it is possible that a special tactical code might be useful for preparation of tactical orders.

Also, in an ofcial British Army Manual of Cryptography prepared in 1914 is found the following statement:

Codes will rst be considered, but as they do not fulll the conditions required of a means of secret communication in the eld, they need not be dealt with here at length.

In the 1935 edition of this text the foregoing quotations were immediately succeeded by the following comment:

It need only he pointed out in this connection that today rode methods predominate in the secret communication systems of the military, naval, and diplomatic services of practically all the large nations cf the world. Nevertheless, it is likely that within the next decade or two the pendulum may once more swing over to the other position and cipher methods may again come to the fore, especially if mechanical and electrical cipher machines are perfected so that their operation becomes practicable for general use. It is for this reason, if for no other, that the cryptographer who desires to keep abreast of progress must devote considerable attention to the more complicated cipher methods of the past and present time, for with the introduction of mechanical and electrical devices the complexities and difculties of these handoperated methods may be eliminated.

In preparing the revision of this text in 1943, the author found it necessary to say that the forecast he made in 1935 in regard to the rebirth of cipher methods had been fully justied by the present trend, which is in a direction away from code and toward cipher methods, because of important advances made in the eld of mechanical and electrical cryptographic mechanisms.

b. Modern electrical communication methods and instrumentalities are nding an increasing need for applications of cryptographic theory and practice to their efcient operation. For example, in very recent years there has developed a distinct need for secure methods and means for distorting voice communications by telephone or radiophone, and for distorting facsimile transmissions by wire or radiotelegraphy. Teleprinter services permitting direct cryptographic intercommunication by machines operated from a typewriter keyboard make it desirable to have means whereby, although the keyboard is operated to correspond to plaintext characters, the latter are instantaneously and automatically enciphered in transmission and the received signals are instantaneously and automatically deciphered upon reception at the receiving end. Thus the printing mechanism at the receiving station records the original plain-text characters set up on the keyboard at the sending station but interception Of the signals passing over the line or by radio would yield only cipher text.

c. It is difficult to foresee the specic cryptographic methods which might some day be useful in connection with developments of the foregoing nature.

OCSigO, War Department, Washington, 1942

Progress in the electrical and electronic elds exercises an important effect upon developments in the cryptographic eld. Methods which today appear to yield a high degree of cryptographic security but which are impractical for hand operation a few years from now, may be readily mechanized and become highly practical. On the other hand, methods which today do provide a high degree of security may, a few years from now, become obsolete because high-speed electrical analytical machines have been devised for their rapid solution. Consequently, if among the many and more or less complex methods set forth herein certain ones appear to fall outside the realm of what is today considered practicable, it should be remembered that the purpose in describing them is to present various basic cryptographic principles, and not to set forth methods that may with a high degree of probability be encountered in military cryptography in the immediate future.

II TERMINOLOGY

3 Basic Definitions

In a study of military cryptography as employed in the U. S. Army, the following denitions will be useful:

a. SIGNAL COMMUNICATIONS. Any means of transmitting messages in plain or encrypted text other than by direct conversation or mail. A commander uses signal communications to receive reports of hostile dispositions and activities, to receive reports of the progress and needs of subordinate and neighboring friendly units, to send orders to subordinate units, to receive orders from superior units, and to send to higher and adjacent units information necessary for the coordinated action of the whole command.

b. AGENCY 0F SIGNAL COMMUNICATION. The organization, teams, and personnel necessary to perform operational duties pertaining to signal communications.

c. MESSAGE. Used in its broadest sense in Department of the Army and other Ofcial publications, the term message includes all instruc- tions, reports, orders, documents, photographs, maps, or other information, transmitted by means of signal communication. In this manual, however, the term message implies instructions, reports, orders, and similar communications usually transmitted by electrical means.

d. MEANS OF SIGNAL COMMUNICATION. A medium (including equipment) used by an agency for transmitting messages. There are two dozen or more different means; the most important, so far as this manna is concerned, are

(1). *Wire*:

Telephone.

Telegraph.

Teletypewriter.

Facsimile (picture or photo transmission).

(2). *Radio*:

Radiotelephone.

Radiotelegraph.

Radio teletypewriter.

Radio facsimile.

e. WRITER. The person who actually prepares and signs the message blank. The writer may be the originator or his ofcially designated representative.

f. ORIGINATOR. The authority who orders the message written and sent. The commander may delegate this authority to one or more subor- dinates. Ofcers assigned as members of a units general staff are

assumed to have been so designated. .

g. TIME or ORIGIN. The time shown on a message by the writer to indicate the hour and minute when he completed its writing

h. ADDRESSEE. The authority (organization, ofce, or person) to whom a message is directed by the originator.

i. MESSAGE CENTER. That signal communication agency of a head- quarters, or echelon thereof, which is charged with the receipt, routing and delivery of all ofcial messages except: those which are transmitted directly from the originator to the addressee by means of a personal agent, or telephone or teletypewriter provided for his personal use; mail handled by military or civil postal services, and purely local messages.

j. COMMUNICATIONS CENTER. One or more agencies of signal communication equipped to receive, route, and transmit ofcial messages. A communications center may be established at a point xed or mobile.

4 Cryptology and Secret Communication

a. Secrecy of intercommunication in military operations is of the utmost importance. Need for it has been recognized from the earliest days of organized warfare. That branch of knowledge which treats the production, use and solution of the means and methods. of secret[2] communications is called cryptology.

b. Intercommunication may be conducted by any means susceptible of ultimate interpretation by one of the ve senses, but those most com- monly used are visual or auditory. Aside from the use of simple visual and auditory signals for intercommunication over relatively short dis- tances, the usual method of intercommunication involves, at one stage or another, the act of writing, speaking over a telephone, or of drawing or taking a picture.

[2]Throughout this manual the term "secret" will be used in its ordinary sense as given in the dictionary. Whmever the designation is used in the more restricted sense of the security classication as dened in AR 3805, it will be so indicated. There are in current use the classications, Restricted, Condential, Secret, and Top Secret, listed in ascending order of degree.

c. To preserve secrecy of intercommunication by telephone, there are means and methods of disguising the electrical currents in telephony so that the messages or conversations can be understood only by persons provided with the proper equipment. The same thing is true of secrecy in the electrical transmission of pictures, drawings, maps, etc. However, this manual is concerned only with secrecy of intercommunication by means of messages conveying in written words the thoughts, orders, reports, etc., of the originator to the addressee.

d. 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 is done with certain chemicals called invisible, sympathetic, or secret inks which have the property of either being initially invisible to the naked eye or becoming so after a short time. In order to make writing done with secret inks visible, special processes must usually be applied. There are also methods of producing writings which is invisible because the characters are of microscopic size. These methods usually require either special photographic apparatus or very delicate mechanical instruments called micropantographs, by means of which ordinary writing may be copied in extremely reduced size. Magnifying lenses must be used to make such writing visible to the naked eye.

e. Invisible writing and visible writing prepared in a form unintel- ligible in the language in which it is written, constitute secret writing. Both of these forms of secret writing have their uses in military com munications, but this manual deals only with visible secret writing.

5 Plain Text and Encrypted Text

a. A visible message which conveys an intelligible meaning in the language in which it is written, with no hidden meaning, is said to be in plain text. A message in plain text is called a plain-text message, a clear text message, or a message in clear.

b. A visible message which conveys no intelligible meaning in any language is said to be in encrypted text. Such a message is termed a cryptogram.

c. A visible message may convey an intelligible meaning which may not be the real meaning intended. To quote a simple example of a mes- sage containing a secret or hidden meaning, prepared with the intention of escaping suppression by censors in war time, the sentence Son born today" may mean Three transports left today. Messages of this type are in encrypted text and are said to be in open code. Although occa- sionally useful in espionage and counter-espionage, secret communication systems of this sort are impractical for eld military use, and will not be dealt with further in this manual.

d. The term correspondents is used in this manual to designate per- sons who exchange messages with each other. Between the originator and the addressee there may be persons who actually write and handle the messages, who convert the plain texts into cryptograms, or who reconvert the cryptograms into plain texts. The originator and the addressee may also do this work but in the U. S.

Army such work is usually done by special personnel who act as agents of the correspondents.

e. The term enemy is used in this manual to designate all persons who obtain messages or copies of messages not intended for them.

6 Cryptography, Cryptographing. and Decryptographing

a. Cryptography is that branch of cryptology which treats of various means and methods for rendering plain text unintelligible and recon- verting unintelligible text into plain text or the application thereof.

b. To cryptograph[3] (encrypt) is to convert a plain-text message into a cryptogram by following certain rules agreed upon in advance by correspondents, or furnished them or their agents by higher authority. The process of cryptographing a message produces a cryptogram.

c. To decryptogroph (decrypt) is to reconvert a cryptogram into the equivalent plain-text message by a direct reversal of the cryptographing process; that is, by applying to the cryptogram the key used in crypto- graphing the plain text.

d. A person skilled in the art of cryptographing and decryptographing, or one who has a part in making a cryptographic system is called a cryptographer; a clerk who cryptographs and decryptographs, or who assists in such work, is called a cryptographic clerk.

7 Codes, Ciphers, and Enciphered Code

a. Cryptographing and decryptographing are accomplished by means collectively designated as code: and ciphers. Such means are used for either or both of two purposes: (1) secrecy, and (2) economy or brevity. Secrecy usually is far more important in military cryptography than economy or brevity. In ciphers or cipher systems cryptograms are pro- duced by applying the cryptographic treatment to individual letters of the plaintext messages, whereas in codes or code systems cryptograms are produced by applying the cryptographic treatment to entire words, phrases, and sentences of the plaintext messages. The specialized mean. ings of the terms code and cipher are explained in detail later.

b. 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. Such act or operation of cryptographing 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. The cryptographic clerk who performs the process serves as an encipherer. The corresponding terms applicable to the decryptographing of cipher messages are deciphering, decipherment, and decipherer. A clerk who serves both as an encipherer and decipherer of messages is called a cipher clerk.

c. A cipher device is an apparatus or a simple mechanism for literal encipherment and decipherment, usually manually powered; a cipher machine is an

[3]Compare the terms "cryptography," "cryptogram," and "cryptograph" with the terms telegraphy, "telegram," and "telegraph."

apparatus or complex mechanism for literal encipherment and decipherment, usually requiring an external power source.

d. A cryptogram produced by means of a code system is said to be in code and is called a code message, or sometimes simply a code. The text of the cryptogram is referred to as code text. This act or operation of cryptographing 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 corres- ponding terms applicable to the decryptographing of code messages are decoding, decodement, and decoder. A cryptographic clerk who serves both as an encoder and decoder of messages is called a code clerk.

e. Sometimes, for special purposes, the code text of a cryptogram undergoes a further step in concealment involving an enciphering process, thus producing what is called a cryptogram in enciphered code, or an enciphered-code message. Encoded cipher, the cipher text of a crypto- gram which subsequently undergoes encodement, is also possible but rare.

f. In U. S. Army tables of organization and other publications, cipher clerks and code clerks are cryptographic technicians. They are specically trained to encipher, decipher, encode, and decode messages, using authorized means, equipment, and procedures.

8 General System and Specic Key

a. The total of all the basic, invariable rules followed in cryptograph ing a message according to a given method, together with all the agree ments, conventions or private understandings drawn up between the correspondents or their authorized agents or furnished them by higher authority, constitute the general cryptographic system.

b. In the general cryptographic system usually a number, a group of letters selected at random, a word, a phrase, or a sentence, is used as a key. The element selected governs the manner in which a cipher device Or a cipher machine is prepared for the encipherment or decipherment of a specic message, or it controls the steps followed in cryptographing a specific message. This elementusually of a variable nature and changeable at the will of the correspondents, or prearranged for them or for their agents by higher authorityis the specic key. The specic key may also involve the use of a set of specially prepared tables, a special document, or even a book.

c. Hereafter, the general cryptographic system will be referred to as the system, and the specic key, as the key.

9 Cryptanalytics and Cryptanalysis

a. In theory, any cryptographic system except one can be broken down if enough time and skill are devoted to it, and if the volume of trafc is large enough. This can be done even if the general cryptographic system and the specic key are unknown at the start. The exception is the one time system in which the key is

used only once and in itself must have no systematic construction, derivation, or meaning. In military operations theoretical rules must usually give way to practical considerations. How the theoretical rule in this case is affected by practical considerations will be taken up in subsequent portions of this manual.

b. That branch of cryptology which deals with the principles, methods, and means employed in the solution or analysis of cryptograms is called cryptanalytics.

c. The steps and operations performed in applying the principles of cryptanalytics constitute cryptanalysis. To cryptanalyze a cryptogram is to solve it by cryptanalysis.

d. A person skilled in the art of cryptanalysis is called a cryptanalyst, and a clerk who assists in such works is called a cryptanalytic technician.

III TWO CLASSES OF CRYPTOGRAPHIC SYSTEMS

10 Transposition and Substitution

a. Technically there are only two distinct types of treatment which may be applied to plain text to convert it into secret text, yielding two different classes of cryptograms. In the rst, called transposition, the elements or units of the plain text, whether one is dealing with individual letters or groups of letters, syllables, whole words, phrases and sentences, retain their original identities and 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 tex retain their original positions or sequences but are replaced by other elements with dierent values or meanings.

b. It is possible to cryptograph a message by a substitution method and then to apply a tran5position method to the substitution text, or vice versa. Such combined transposition-substitution methods do not form a third category of methods. They are occasionally encountered in military cryptography, but the types of combinations that are sufciently simple to ,be practicable for eld use are very restricted.

11 Letter, Syllable, and Word Methods

Under each of the two principal classes of cryptograms as outlined in the preceding paragraph, a further classication can be made with respect to the nature of the textual elements or units with which the crypto- graphic process deals. These textual units are (1) individual letters, or groups of letters in regular sets, and (2) complete words. Methods which deal with the rst type of units are called letter methods, including, when such is the case, syllable methods; those which deal with the second type of units are called word methods.

12 Cipher Systems and Code Systems

It is necessary to indicate that the classication into letter, syllable, and word methods is more or less arbitrary or articial in nature, and is established for purpose of convenience only. No sharp line of demarca- tion can be drawn in every case, for occasionally a given system may combine methods of treating single letters, groups of letters, syllables, whole words, phrases and sentences. When in a single system the cryptographic treatment is applied to textual units of regular length, usually single letters or pairs, and is only exceptionally applied to textual units of irregular length, the system is called a cipher system. Likewise, when in asingle system the cryptographic treatment is applied to textual unit-s of irregular length, usually whole words, phrases, and sentences, and is only exceptionally applied to single letters, pairs, or groups of letters and syllables, the method is called a code system because it generally involves the use of a code book. i

IV SECURITY AND TIME ELEMENTS IN CRYPTOGRAPHIC SYSTEMS

13 Interception, Radio Direction Finding, and Radio Position Finding

a. Messages transmitted by electrical means can be heard and copied by persons who are not the correspondents or their authorized agents. Messages transmitted by radio can be manually copied or automatically recorded by suitably adjusted radio apparatus located within range of the transmitter. Some messages transmitted over wire lines can likewise be manually copied or automatically recorded by special apparatus suited for the purpose. Correspondents have no way of knowing whether or not radio transmissions are being copied by the enemy, since the unauthorized copying does not interfere in the slightest degree with signals being transmitted. Interception of wire trafc is much more difficult than of radio, mainly because the equipment must be located very near the wire line, or connected directly to it. The act of listening-in and copying or recording electrically-transmitted messages by persons other than the cor- respondents or their authorized agents is called interception. The pur- pose of interception is to obtain copies of messages transmitted and, by studying them, to obtain information. In time of war, it must be assumed that the enemy will intercept all messages transmitted by any signal communication agency susceptible of interception.

b. It is also possible to determine, with a fair degree of accuracy, the direction of a radio transmitter from a given location and, by establishing the direction from two or more locations, it is possible to determine the geographical location of the transmitter. The science which deals with the means and methods of determining the direction in which a radio transmitter lies is called radio direction nding; the method of deter- mining the geographical location of

a radio transmitter, by the use of two or more direction-nding installations, is called radio position nding.

c. Messages may be transmitted by signals with special apparatus which distort, disguise, or completely hide the signals themselves, so that the processes of interception and recording the signals are very difficult, and intercept personnel may not even be aware Of the existence of such signals. All such methods of transmitting messages fall in the class designated in this manual as system of secret signaling. Signaling by means of so-called black light, that is, invisible or infra-red light waves, falls into this category. Methods of disguising or distorting voice or picture transmissions (par. 2c) require more or less highly-specialized apparatus for the interception of the signals and their inter pretation or recording in recognizable form. As a rule, the signals of practically all systems of secret signaling can be intercepted and recorded in a form suitable to making the signals understood by one of the senses, usually visual or auditory. Ordinarily, this requires special apparatus but can sometimes be done without the specic apparatus used in forming or sending the signals, or the key used in their distortion, or disguise.

14 Traffic Analysis and Cryptanalysis

a. A great deal of information of military value can be obtained by studying signal communications without solving the crytographed mes- sages constituting the trafc. The procedure and the methods used have yielded results of sufcient importance to warrant the application of 3 special term to this eld of study; namely, traffic analysis[4], which is the study of signal communications and intercepted or monitored trafc for the purpose of gathering military information without recourse to crypt analysis.

b. In general terms, trafc analysis is the careful inspection and study of signal communications for the purpose of penetrating camouage superimposed upon the communication network for purposes of security. Specically, trafc analysis reconstructs radio communication networks by: (1) noting volume, direction, and routing of messages; (2) corre lating transmission frequencies and schedules used among and within the various networks; (3) determining directions in which transmitters lie. by means of radio direction nding; (4) locating transmitters geo graphically, by radio position nding; (5) developing the system of assigning and changing radio call signs; (6) studying all items that constitute conversations or chat exchanged among operators on radio channel.

c. From a correlation of general and specic information derived from these procedures, trafc analysis is able not only to ascertain the geo- graphic location and disposition of troops and military units (technically called "order of battle) and important troop movements, but also to predict with a fair degree of reliability the areas and extent of imme- diately pending or future activities. Trafc analysis procedures are fol- lowed to obtain information of value concerning the enemy, and to determine what information concerning our own forces is made

[4]Which may be abbreviated tranalysis.

avail- able to the enemy through our own signal communications.

d. These very important results are obtained without actually'reading the texts of the intercepted messages; the solution and translation of messages are the functions of cryptanalysis and not trafc analysis. However, the cryptanalyst is frequently able to make good use of bits of information disclosed by trafc analysis such as faults noted in mes- sage routing and errors in cryptography causing messages to be duplicated or canceled. Cryptanalysis can provide important information for trafc analysis, since the solution of messages often yields data on impending changes in signal communication plans, operating frequencies and schedules, etc. It also yields data'on specic channels, networks, or circuits

which are most productive of intelligence, so that effective control and direction of intercept agencies for maximum results can be achieved.

e. In addition to (1) trafc analysis and (2) cryptanalysis as means of obtaining information relating to communications, further data may be obtained (3) by the use of secret agents for espionage, (4) by the cap ture and interrogation of prisoners, (5) by the capture of headquarters or. command posts with records more or less intact, and (6) by treason or carelessness on the part of personnel who handle communications. Of these six main sources, trafc analysis and cryptanalysis are the most valuable. The amount of vital information they furnish cannot be accurately estimated as it uctuates with time, place, circumstances, equipment, and personnel. For most effective operation, the results of both cryptanalysis and trafc analysis can be tted together to yield a unied picture of the communications scheme. Therefore, if all transmitting stations can be located quickly and if all communications can be intercepted and solved, extremely valuable information concerning strength, disposition of forces, and proposed moves will be continually available.

f. The facts set forth above are applicable to our own forces as well as the enemys.

g. The process of intercepting and copying our own or friendly radio and wire transmissions for the purpose of detecting and correcting viola- tions of regulations is called monitoring; it provides increased protection of our own signal communications.

15 Communication Intelligence and Communication Security

a. Communication intelligence is evaluated information concerning the enemy, derived principally from a study of his signal communications. The main components of communication intelligence are as follows:

(1). Interception of signals or messages and forwarding raw trafc to communication intelligence centers for study.

(2). Trafc analysis, including radio direction nding and radio position nding. (Evaluated information from this source is often called traic intelligence.)

(3). Cryptanalysis or solution (and translation, when necessary) of the texts of the messages.

(4). Evaluation of data, that is, analysis of results obtained from the preceding steps and their correlation, collation, and comparison with results obtained from other sources of information.

b. Communication security is the protection resulting from all meas ures designed to deny to unauthorized persons information of value which may be derived from communications. The main components of communication are as follows -:

(1). Physical security, that component of communication security which results from all measures necessary to safeguard classi- ed communication equipment, and material from access there- to by unauthorized persons. ,

(2). Cryptosecurity, that component of communication security which results from the provision of technically sound crypto- systems[5] and their proper use.

(3). Transmission security, that component of communication security which results from all measures designed to protect transmissions from interception and trafc analysis.

c. Further details on the subject of communication security will be found in JANAP 122(A) Joint Communications Instructions.

16 Time Needed for Cryptanalysis and its Dependent Factors

a. In military operations time is a vital element. The inuence or effect that analysis of military cryptograms may have on the tactical situation depends on various time factors.

b. Of these factors, the following are the most important:

(1). The length of time necessary to transmit intercepted enemy cryptograms to solving headquarters. This factor is negligible only when signal communication agencies are properly and specically organized to perform this function.

(2). The length of time required to organize raw materials, to make trafc analysis studies and to solve the cryptograms, and the time required to make copies, tabulate, and record data.

[5]Cryptosystems may be categorized as literal and nonliteral. This manual is concerned solely with literal or cryptographic systems.

(3). The nature of information disclosed by traffic analysis studies and solved cryptograms; whether it is of immediate or opera- tional importance in impending action, or whether it is of his- torical interest only in connection with past action.

(4). The length of time necessary to transmit information to the organization or bureau responsible for evaluating the informa- tion. Only after information has been evaluated does it become military intelligence.

(5). The length of time necessary to transmit resulting military intelligence to the agency or agencies responsible for tactical operations, and the length of time necessary for the agency to prepare orders for the action determined by the intelligence and to transmit them to the combat units concerned. The last sentence under (1) above applies here also.

c. Of the factors mentioned in b above, the only one of direct interest in this manual is the length of time required to solve the cryptograms. This is subject to great variation, dependent upon other factors, of which the following are the most important:

(1). The degree of cryptographic security in the system. The degree of security depends upon the technical soundness of the system itself. Technical soundness, in turn, determines the resistance to analysis which the system offers. Cryptographic systems vary widely in technical soundness, but this manual does not attempt to demonstrate such variation.

(2). The adequacy and technical soundness of regulations drawn up by designers of the cryptographic system for the guidance of cryptographic technicians who are its actual users.

(3). The extent to which cryptographic technicians follow these regulations and procedures. Security of a good cryptographic system can be almost completely destroyed by a few crypto- graphic technicians who fail to observe the regulations, are careless in their observance, in sheer ignorance commit serious violations of cryptographic security, or adopt bad technical habits. As a result, these technicians jeopardize not only their own lives but the lives of thousands of their comrades.

(4). The volume of cryptographic text available for study. As a rule, the greater the volume of text, the more easily and speedily it can be solved. A single cryptogram in a given sys tem may present an almost hopeless task for the cryptanalyst, but if many cryptograms of the same system or in the same or closely related specic keys are available for study, the solution may be reached in a very short time.

(5). The number, skill, and efciency of organization and coopera tion of signal intelligence units assigned to the work. Crypt– analytic headquarters are organized in units of ascending size, ranging from a few persons in the

forward echelons to many persons in the rear echelons. Such organization avoids duplica tion of effort and, especially in forward areas where spot intel ligence is most useful, makes possible the quick interpretation of cryptograms in already solved systems. In all these units, proper organization of highly skilled workers is essential for efcient operation.

(6). The amount and character of information and intelligence avail able to the cryptanalytic headquarters. Isolated cryptograms ex- changed between a restricted, small group of correspondents, about whom and whose business no information is available, may resist the efforts of even a highly organized, skilled crypt- analytic ofce indenitely. If, however, a certain amount of such information is obtained, the situation may be entirely changed. In military operations usually a great deal of collateral information is available, from sources indicated in paragraph 146. As a rule, a fair amount of more or less denite informa- tion concerning specic cryptograms is at hand, such as proper names of persons and places, and events in the immediate past or future. Although the exchange of information between intelligence and cryptanalytic staffs is very important, the collection of information derived from an intensive study of already solved trafc is equally as important because it yields extremely valuable cryptanalytic intelligence which greatly facilitates the solution of new cryptograms from the same sources.

17 Degree of Crytographic Security Required of a System for Military Use

The ideal cryptographic system for military purposes would be a single, allpurpose system which would be practicable for use not only by the largest xed headquarters but also by the smallest troop unit in the combat area, and which would also present such a. great degree of crypto- graphic security that, no matter how much trafc became available, all in the same key, the cryptograms composing this trafc would resist solution indenitely. Such an ideal system however, is beyond the realm of possibility so far as present methods of cryptographic communication are concerned; in fact, a multiplicity of systems must be employed, each more or less specically designed for a particular purpose. Of each such system, the best that can be expected is that the degree of security be great enough to delay solution by the enemy for such a length of time that when the solution is nally reached the information thus obtained has lost all its short term, immediate, or operational value, and much of its "long term, research, or historical value.

18 Fundamental Practical Requirements of a Cryptographic System for Military Use

a. Military cryptograms must meet certain fundamental requirements of a practical nature because of denite limiting conditions in present military signal com-

munication means and methods.

b. These requirements are (1) reliability, (2) security, (3) rapidity, (4) exibility, and (5) economy. Their relative importance is in the order named.

c. Reliability is of rst importance. Reliability, as applied to a crypto- graphic system or device, means that the cryptograms produced by the sending or originating ofce will be decryptographed promptly, ac- curately, and without ambiguity by the receiving ofce; that the crypto graphic system, whether a book, machine, or device, will be on hand and in good working order, available for instant use; and that when used it can be expected to be operative as Ionglas needed. Simplicity is implied in reliability; usually, the more simple the system, the more reliable it is. Security is. the protection aorded by a sound cryptographic system; rapidity, the speed with which messages can be cryptographed and de- cryptographed, usually expressed in words or S-letter groups per minute. The conicting requirements of security and rapidity vary according to circumstances. Signal communication personnel must be governed by general principles, subject to existing circumstances, rather than by rigid regulations. Maximum security at all times should be the goal, but in messages exchanged among the higher headquarters some speed may be sacriced to meet greater security requirements, while in messages ex- changed among the lower headquarters security must often- give .way'to greater speed requirements. For this reason various cryptographic sys- tems must be available to meet varying types of situations. As to exi- bility,'a cryptographic system specically adapted for a particular usage cannot serve as an all-purpose system. A codebook designed for front- line use can hardly serve the needs of a high headquarters! in the rear; nor can a cryptographic system designed for use by a high headquarters serve the needs of a small combat unit. As to economy, the simpler-the operations involved, the shorter will be the texts produced, the amount of time required to produce the cryptographic material, use it, and trans- mit the messages; and the greater will be the economy.

d. Specific requirements which should be met by a cryptographic sys- tem for general military use are set forth below.

(1). Cryptograms must be in a form suitable for transmission by standard telegraphic equipment and methods. This requirement generally eliminates all systems except those which produce cryptograms composed of characters readily transmitted by a telegraphic system employing either the Morse or the'itele printer alphabet. Cryptographic systems using Arabic numerals are not so desirable as those using letters because-the-Mofse signals for numbers are longer, except when "cut numbers are used, and are more difcult for the average American tele- graph or radio operator to handle. Systems which produce cryptograms composed of mixtures of letters and gures, or of letters, gures, and punctuation signs, and which must be transmitted by' Morse telegraphy are unsuited for practical usage. However, where Such intermixtures are produced auto- matically by the cryptographic mechanism and. are transmitted, received, and deciphered automatically, as certain teleprinter enciphering systems, their use

is permissible. In order to be Suitable for economical Morse telegraphic transmission, the cryptographic text must be capable of being arranged in regular sets of characters for these reasons: rst, it promotes accuracy in telegraphic transmission (since an operator knows he must receive a definite number of characters in each group, no more and no less) ;' and secondly, cryptanalysis is usually made more difcult when the length of the words,.phrases, and sentences of the plain text is not apparent. The usual grouping is in sets of ve characters, although occasionally other groupings may be made in special circumstances. Such grouping is not necessary in teleprinter encipherment systems.

(2). Regular channels of signal communication carry only a limited volume of trafc. Their most efcient operation demands that the smallest number of characters actually necessary to convey a given mesSage be transmitted. Therefore, the crypto- graphic text should be no longer than its equivalent clear text. In an exceptional ease, the cryptographic text- may be longer than the equivalent clear text, but a system in which the cryptographic text is twice the length of the equivalent clear text is useful only if it is of outstanding merit and suitable for certain restricted or special use. No system in which the crypto- graphic text is more than twice the length of the equivalent clear text is practicable for military usage. Most of the crypto- graphic systems in current use produce cryptograms which cor- respond 1n length with that of the original plaintext message or are somewhat shorter.

(3). General requirements of reliability and speed are that the opera- tions of cryptographing and decryptographing be relatively simple and rapid. For use in the combat zone, operations must be capable of being performed under difcult eld conditions and must not require the remembering and application of a long series of steps or rules. They must be such as to reduce the mental strain on the operator to a minimum. Complex processes requiring several distinct steps are not suited to use in the combat zone, but occasionally systems involving only two steps, if each step is simple and rapid, may be practicable for military usage.

(4). Cipher devices or machines for eld use must be light 1n weight, rugged in construction, and simple in operations, requiring the services of only one operator. Requirements to be met by high speed cipher machines are too complex to be described in this manual.

(5). The system must be such that errors, which invariably occur in cryptographic communications, can be corrected easily and rapidly by cryptographic technicians. A system is impractical if frequently it is necessary to call for a repetition of the whole transmission, or for a rechecking of the original crypto- graphing.

e. Only a few of the systems which fullfill at least several of the fore going practical requirements are included in this manual.

Chapter 2

ELEMENTARY TRANSPOSITION SYSTEMS

I SIMPLE MONOLITERAL TRANSPOSITION METHODS

19 Transposition Ciphers in General

Transposition ciphers are like jig-saw 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' a jig-saw puzzle may be divided are irregular in size and shape, but the pieces into which the plain text forming the basis of a transposition cipher may be divided must be much more regular, for the sake of practicability. They must be either single letters or pairs of letters, or sets of letters in regular groupings, or, in an exceptional case, whole words. Most transposition methods however, deal with individual letters and are therefore termed monoliteral methods. The other methods are termed polyliteral methods.

20 Geometric Designs

a. Practically all monoliteral or polyliteral transposition ciphers involve the use of a design or geometric figure, such as a square, rectangle, tri angle, trapezoid, etc., in which the letters of the plain text are first inscribed or written according to a previously agreed upon direction of writing and then transcribed or rewritten according to another and different, previously agreed-upon direction to form the text of the cryptogram. In nearly all cases the specific key consists in (1) using designs of a specific nature and dimensions, and (2) varying the

direction or manner of inscription or transcription, or both.

b. In working with transposition ciphers or, for that matter, most types of ciphers, crosssection paper will be found very convenient. Cross-section paper with M-inch squares is most suitable. For brevity in reference, the individual small squares of such cross-section paper will hereafter be called cells.

21 Route Transpositions

a. . Suppose the correspondents agree to use the method of monoliteral transposition known as route transpgsition, The message is inscribed within a rectangle in the usu-al manner of writing, that is, from left to right and in consecutive lines from top to bottom. If one or more cells are vacant at the end, nulls or dummy lettersletters having no significanceare inserted as fillers to complete the rectangle. Then, to form the cipher text, the letters in the design are taken out of the design and rewritten or transcribed by following or tracing one of many different routes. It is possible for each route to have a dierent starting point, and normally it is one of the four corners of the rectangle. A few typical routes are illustrated in 2.1 where, for the sake of ease in following the route, the plaintext message is assumed to be merely the sequence of letters A B C X.

(A) Simple horizontal:

(1)	(2)	(3)	(4)
ABCDEF	FEDCBA	STUVWX	XWVUTS
GHIJKL	LKJIHG	MNOPQR	RQPONM
MNOPQR	RQPONM	GHIJKL	LKJIHG
STUVWX	XWVUTS	ABCDEF	FEDCBA

(B) Simple vertical:

(1)	(2)	(3)	(4)
AEIMQU	UQMIEA	DHLPTX	XTPLHD
BFJNRV	VRNJFB	CGKOSW	WSOKGC
CGKOSW	WSOKGC	BFJNRV	VRNJFB
DHLPTX	XTPLHD	AEIMQU	UQMIEA

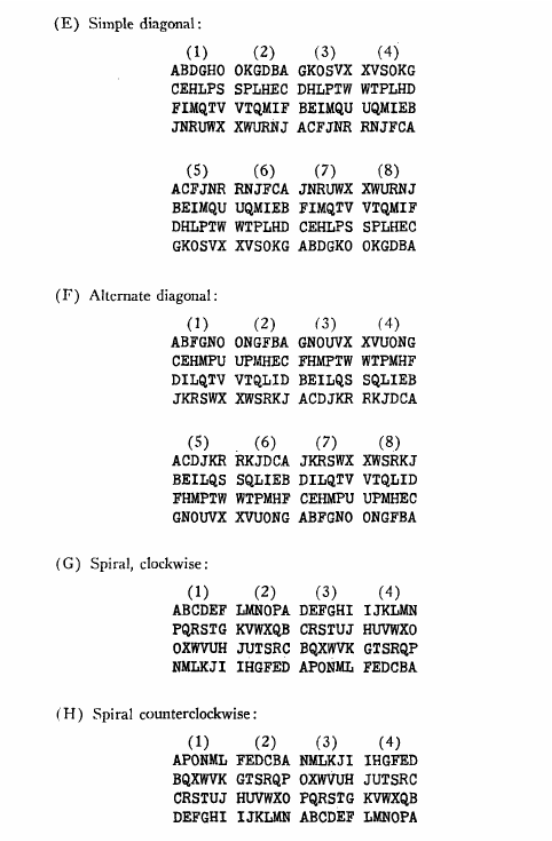
(C) Alternate horizontal:

(1)	(2)	(3)	(4)
ABCDEF	FEDCBA	XWVUTS	STUVWX
LKJIHG	GHIJKL	MNOPQR	RQPONM
MNOPQR	RQPONM	LKJIHG	GHIJKL
XWVUTS	STUVWX	ABCDEF	FEDCBA

(D) Alternate vertical:

(1)	(2)	(3)	(4)
AHIPQX	XQPIHA	DELMTU	UTMLED
BGJORW	WROJGB	CFKNSV	VSNKFC
CFKNSV	VSNKFC	BGJORW	WROJGB
DELMTU	UTMLED	AHIPQX	XQPIHA

Figure 2.1: Figure 1



(E) Simple diagonal:

(1)	(2)	(3)	(4)
ABDGHO	OKGDBA	GKOSVX	XVSOKG
CEHLPS	SPLHEC	DHLPTW	WTPLHD
FIMQTV	VTQMIF	BEIMQU	UQMIEB
JNRUWX	XWURNJ	ACFJNR	RNJFCA

(5)	(6)	(7)	(8)
ACFJNR	RNJFCA	JNRUWX	XWURNJ
BEIMQU	UQMIEB	FIMQTV	VTQMIF
DHLPTW	WTPLHD	CEHLPS	SPLHEC
GKOSVX	XVSOKG	ABDGKO	OKGDBA

(F) Alternate diagonal:

(1)	(2)	(3)	(4)
ABFGNO	ONGFBA	GNOUVX	XVUONG
CEHMPU	UPMHEC	FHMPTW	WTPMHF
DILQTV	VTQLID	BEILQS	SQLIEB
JKRSWX	XWSRKJ	ACDJKR	RKJDCA

(5)	(6)	(7)	(8)
ACDJKR	RKJDCA	JKRSWX	XWSRKJ
BEILQS	SQLIEB	DILQTV	VTQLID
FHMPTW	WTPMHF	CEHMPU	UPMHEC
GNOUVX	XVUONG	ABFGNO	ONGFBA

(G) Spiral, clockwise:

(1)	(2)	(3)	(4)
ABCDEF	LMNOPA	DEFGHI	IJKLMN
FQRSTG	KVWXQB	CRSTUJ	HUVWXO
OXWVUH	JUTSRC	BQXWVK	GTSRQP
NMLKJI	IHGFED	APONML	FEDCBA

(H) Spiral counterclockwise:

(1)	(2)	(3)	(4)
APONML	FEDCBA	NMLKJI	IHGFED
BQXWVK	GTSRQP	OXWVUH	JUTSRC
CRSTUJ	HUVWXO	FQRSTG	KVWXQB
DEFGHI	IJKLMN	ABCDEF	LMNOPA

Figure 2.2: Figure 1 continued

b. It is apparent that instead of following the normal direction of writing, that is, from left to right and from the top downwards, the letters of the plain text may be inscribed according to any one of the routes agreed upon, and then transcribed to form the cipher text by taking the letters from the rectangle in the normal manner, that is,. in this case from left to right, and from the top downwards, or by following any other route of transposition.

22 Example of Encipherment and Decipherment by Monolilteral Route Transposition

a. Now take a special example of encipherment by monoliteral route transposition. Use the message ATTACK HAS BEEN POSTPONED UNTIL TOMORROW TWO AM, and employ a relatively cemplicated method. Suppose that the general system agreed upon is the one being described, and that the specific key consists of the following elements:

(1). Using a completely filled rectangle of seven columns;

(2). Inscribing the letters of the plain text within the rectangle by following route (F) (3) of 2.1.

(3). Transcribing the thus inscribed letters (to form the cipher text) by following route (E) (6) of 2.1.

Since the message contains a total of 40 letters, and it has been agreed to use a completely filled rectangle of seven columns, it is necessary to add two nulls to make the total numberof letters a multiple of seven. A rectangle of seven columns of cells and six lines of cells is therefore prepared. The design is then filled in as shown in 2.

b. To decryptograph such a cryptogram the process is merely reversed. First, the total number of letters in the cipher text must be found. Since

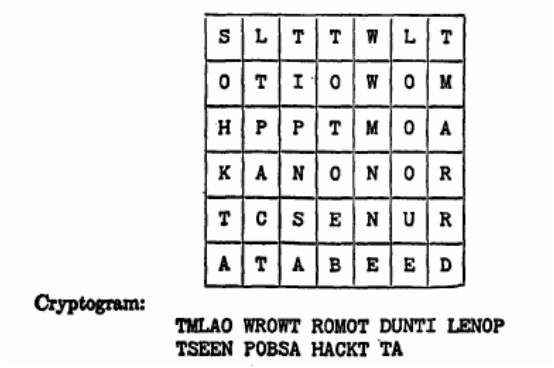


Figure 2.3: Figure 2

it is 42, and since a completely filled rectangle of seven columns has been agreed upon, a design consisting of seven columns and six rows is outlined on cross-section paper. The cipher text is then inscribed according to route (E) (6) of 2.1, and after this has been completed the plaintext letters are read according to route (F) (3), 2.1. It is apparent that it is necessary to remember a relatively long series of rules, and even when the cryptographing has been accomplished correctly the degree of security is very low. Note how obviously the whole word UNTIL mani fests itself in the cipher text. Parts of other words can also be seen. The degree of security remains very low despite the variability afforded by the dimensions of the rectangle, the method of inscription and transcription and their starting points.

23 Use of Nulls in Transposition

a. It will be noted that the two nulls selected as fillers to complete the rectangle in the preceding example were the letters L and T. These were chosen rather than such letters as J, K, Q, X, or Z, for a reason which is important to note. Since

transposition ciphers of this type involve merely a rearrangement of the letters, without any change whatever in their identities, it follows that the natural or normal frequencies of letters of plain text remain unchanged. Now, the letters of every alphabetic language have characteristic frequencies, as a result of which certain clues are afforded in cryptanalysis. The presence, in transposition ciphers, of letters of very low frequency (in English), such as J, K, Q, X, or Z, is very unusual and therefore if these are employed merely as fillers they may afi'ord clues as to the real number of letters in the plain text, the starting or finishing points of the real text, etc. For this reason it is best to insert as fillers in transposition ciphers letters of medium or high fre quency, such as E, T, R, I, N, O, A, S, D, L, or C, for thesct' will not afford any clues to solution. Nulls, when employed for the purpose of making cryptanalysis more difficult, may also be inserted in specific positions as prearranged, or they may be inserted at random if the system permits. This is true of other cryptographic systems, but as a general rule the use of nulls, especially in cipher systems, is to be discouraged. Very often they add little if any security, and thus merely increase the length of the cryptographic text without any compensating advantages.

b. Whenever it is necessary to add nulls in order to complete a transposition message in any respect, or for any reason whatsoever, they must be added before the transposition process is applied and not afterward; otherwise it will be difficult or even impossible for the decryptographing clerk to read the message. This is especially true when the service regulations require that the final group in a cryptogram be a complete group, containing exactly as many letters as all other groups in the message.

24 Special Cases of Route Transposition

a. The oldest and simplest transposition method known, that called reversed writing, is a special case of one of the routes shown in 2.1. Here the text is written in the opposite direction from the normal; for example, BRIDGE DESTROYED is written EGDIRB DEYORTSED. The variability of the scheme, that is, the specific key, consists of the fact that the reversal may be applied to groups of fixed length, to whole words, to sentences, or to the whole text. The security of simple reversed writing may be somewhat increased by disguising the original word lengths, by which is meant a destruction of the normal, or natural word limits by combining a part of one word with a part of the next to form either false words or groups of regular length.

b. Some examples of reversed writing follow. Let the message be: BRIDGE DESTROYED AT ELEVEN PM.

(1). Reversing only the words and retaining original word lengths: Cipher: EGDIRB DEYORTSED TA NEVELE MP

(2). Reversing only the words and regrouping into false word lengths: Cipher: EG DIRB DEYOR'I SEDTA NEVE LEMI¿

(3). Reversing the whole text and regrouping into fives: Cipher: MPNEV ELETA DEYOR TSEDE GDIRB

(4). Reversing the whole text, regrouping into fives, and inserting a null in every fifth position: Cipher: MPNER VELEO TADEB YORTH SEDEA GDIRB

c. A second very simple type of transposition, that known as vertical writing, is a special case of another of the routes shown in 2.1.

The message BRIDGE DESTROYED is written in two vertical columns, and the cipher text is taken from the horizontal pairs thus formed. The message becomes:

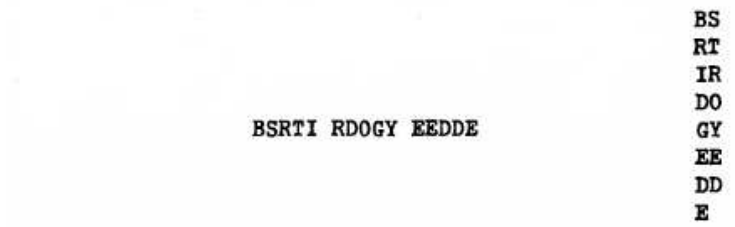


Figure 2.4: Figure 3

When the plain text is inscribed in pairs of letters in vertical writing and then the cipher text is taken by transcribing the columns, a slightly different result is obtained. Using the plain text message BRIDGE DESTROYED, the cipher becomes:

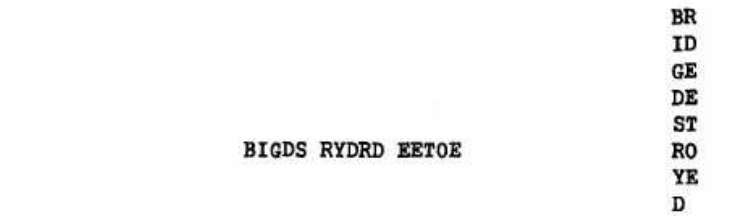


Figure 2.5: Figure 4

This type of transposition is sometimes Called the *rail-fence* cipher because it can be produced by writing the message in the following form:

```
B I G D S R Y D
 R D E E T O E
```

which yields the same cipher result as before.

25 Remarks on Monoliteral Route Transposition

Reversed writing and vertical writing of the types indicated yield ex- tremely simple cryptograms. In practice they are sometimes used in con nection with other more or less simple cryptographing methods to in- crease their security. The cryptographic security of the other methods thus far indicated is also very low, despite the apparently large degree of variability they afford. The reason is that the route to be followed in the inscription or transcription process is definitely fixed under each type of route. In other types Of transposition soon to be discussed, a much wider latitude for variation in the route is afforded by the use of- kley words to control or to guide these processes. Geometric designs are also used in these types of transposition, and key words determine the dimen- sions of the design, or else, if only one key word is used, it determines one dimension, the other being determined by the length of the text. Examples given in their proper place will serve to illustrate the processes.

26 Key Words and Numerical Keys

a. It is often necessary, in performing certain cryptographic operations, to em- ploy a numerical key, which may consist of a relatively long sequence of numbers difficult or impossible for the average cipher clerk to'memorize. To avoid mak- ing it necessary that such sequences of numbers be carried on the person in written form, a dangerous procedure, cryptographers have devised very simple methods of deriving such sequences from words, phrases, or sentences, which can usually be remembered much more easily than can unintelligible, relatively long sequences of numbers. One of the simplest methods is to assign numerical values to the letters of the key in accordance with their relative positions in the ordinary alphabet. Such a key is called a derived numerical key. This method of assigning the numbers is very exible and varies with different uses to which numerical keys are put. For purposes of transposition, the method shown below is very satisfactory. .

b. Let the prearranged key word be the word CARBUNCLE. Since the word contains the letter A, which comes first in the alphabet, the number 1 is written under this letter in the key word. Thus:

```
CARBUNCLE
 1
```

The next letter of the normal alphabet that occurs in the key word is B, which is assigned the number 2. The letter C, which occurs twice in the key word, is assigned the number 3 for its first occurrence, the number 4 for its second occurrence, and so on. The final result is:

```
Basic key word:        C-A-R-B-U-N-C-L-E
Derived numerical key: 3-1-8-2-9-7-4-6-5
```

c. The method may, of course, be applied tophrases or. to- sentences, so that a. very long numerical key, impossible ordinarily to remember, may be so derived at will from an easily remembered key text.

d. It is advisable to make note of a few points valuable 1n connection with the choice of key text:

(1). It should be such as can be easily remembered. Often a key composed of two or more short words is better than one con- sisting of a single long word. Thus, the whole sentence WHEN DO WE EAT would be better than the single word EXTRAORDINARY.

(2). It should consist of one or more simple, familiar words admitting of but one spelling. A word such as REINFORCEMENT is inadvisable because the spelling REENFORCEMENT is also admissible. It goes almost without saying the use of words suitable for spelling bees, even though they may be familiar, everyday words as DEFINITELY, SEPARATELY, REPETITION, etc. is likewise inadvisable.

(3). It should contain as many different letters as possible, in no systematic sequence. Words with several repeated letters, such as ELEMENT, BANANA, MISSISSIPPI, etc., form poor key words.

(4). It should present no associations with the special situation in which it is used, so as not to be easily guessed by the enemy. For example, to use personal or geographic names associated with a region in the theater of operations is bad practice. The key word GETTYSBURG employed in a cryptogram originat- ing in the vicinity of Gettysburg would be bad practice. Or to use for this purpose words of common military usage, such as BATTALION, REGIMENT, ARTILLERY, SIGNAL CORPS, MACHINE GUN, etc., is likewise bad practice.

e. It is convenient to designate key text in letters as a literal key. As noted, a literal key may consist of a single letter, a single word, a phrase, a sentence, whole paragraph, or even a book. The method of deriving a numerical key from a literal key given in b above is only one of a number of methods, but it IS the most commonly employed. It is also subject to variation in detail. But, so far as the cryptanalyst is concerned, just how the numerical key is derived from a specific literal key is usually of interest to him only if this knowledge will assist in subsequent solutions of cryptograms prepared according to the same basic system. Often the cryptanalyst is wholly unconcerned as to whether a literal or a numerical key has been used in connection with cryptographing of the messages, and he may frequently be unaware of the fact that a literal key has been used as the basis for deriving a numerical key.

II COLUMNAR TRANSPOSITION METHODS

27 Columnar Transposition with Completely Filled Rectangles

a. One of the most common types of transposition involving the use of a key word or a derived numerical key is that known as keyed or variable-key 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 lines from left to right and from the top downwards, and then the letters are transcribed by reading the columns in the sequence determined by the numerical key. If the text does not contain a sufficient number of letters to fill the last line completely, as many nulls as are necessary to do so are added at the end. Figure 1 is an example of cryptographing by this method.

Key word: L - I - B - E - R - T - Y
Numerical key: 4 - 3 - 1 - 2 - 5 - 6 - 7

R	E	P	O	R	T	L
O	C	A	T	I	O	N
O	F	S	E	C	O	N
D	B	A	T	T	A	L
I	O	N	C	O	M	M
A	N	D	P	O	S	T
T	O	D	A	Y	D	N

Note. The letters D and N in the final two cells are nulls, inserted to complete the rectangle.

Cryptogram:

PASAN DDOTE TCPAE CFBON OROOD IATRI CTOOY
TOOAM SDLNN LMTN

Figure 2.6: Figure 5

b. To decryptograph such a cryptogram, a rectangle with the proper number of cells, determined by the length of the message and the length of the key, must first be prepared. In the foregoing example, since the cipher text consists of 49 letters and the key consists of 7 letters or numbers, the rectangle shown in (a) of 2 is prepared and then the columns (of cells) are filled in numerical order. An early stage in the decryptographing is represented in (b) of 2. It is only after the process has been finished that the complete message reappears, as shown in (c) of 2.

c. The method indicated above may vary considerably by changing (1)

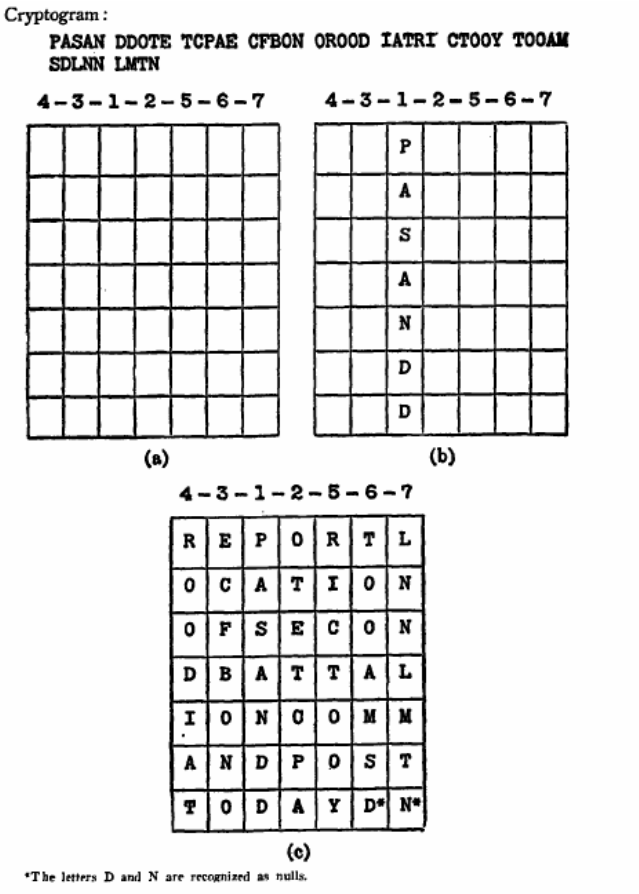


Figure 2.7: Figure 6

the key word, (2) the route followed in inscribing the letters of the plain text, and (3) the route followed in transcribing them to form the cipher text. A change in key daily, or oftener, is possible; or, by drawing up a whole list of daily keys for a given period, automatic change in key can be provided for without indicating in the cryptograms the applicable key. It is also possible to prepare a long list of suitable keys and to designate each key by an indicator inserted in the cryptogram in a prearranged position. Indicators may be words, numbers, groups of letters, or single letters. For example, each key in a list of 500 may be indicated by a single pair of letters inserted at the beginning, at the end, or at any prearranged position of the cryptogram. This procedure has a disadvantage, however: if an error occurs at the particular position of the cryptogram containing the indicator, the decryptographing is made difficult if not impossible. For this reason indicators, if used, are often inserted in at least two positions in the cryptogram, usually at or near the beginning and end.

d. The letters of the plain text may be inscribed in the rectangle according to any one of the routes indicated in 2.1. If the transcribing process is accomplished by reading whole columns or whole rows, according to a prearranged plan which follows a route perpendicular to the inscribing route (except in the case of spiral inscription), the decryptographing process is simple. Only certain of the simpler combinations of inscription and transcription are 'suitable for military use, the most practicable being those illustrated in figures 5 and 6.

28 Columnar Transposition with lncompletely Filled Rectangles

a. The degree of cryptographic security of columnar transposition is much increased if the rectangle is not completely filled. It is impossible to go into the reasons for this increased security without demonstrating solutions; suffice it to say that the solution will be more difficult than would be suspected if one or more cells are vacant in the last row of the rectangle. An example of cryptographing and decryptographing is shown in figure 7.

b. To decryptograph such a cryptogram one must first count the number of letters in the text and then outline on cross-section paper a rectangle which will exactly contain the message, crossing off the cells which must remain vacant. In the foregoing example, the text contains 30 letters and, since the key contains 7 letters, the outlined rectangle is as shown in figure 8 of (a). From the complete rectangle 7 X S = 35 cells, 5 cells must remain vacant at the end.

c. The cipher text is then inserted in keynumber order, the result of inserting the first two groups of the text being shown in (b), figure 8. It is only after the process has been finished that the complete message becomes apparent.

Message:

REQUEST IMMEDIATE REENFORCEMENTS

Key word: P – R – 0 – D – U – C – T
Numerical key: 4 – 5 – 3 – 2 – 7 – 1 – 6

R	E	Q	U	E	S	T
I	M	M	E	D	I	A
T	E	R	E	E	N	F
0	R	C	E	M	E	N
T	S					

Cryptogram:

SINEU EEEQM RCRIT OTEME RSTAF NEDEM

Figure 2.8: Figure 7

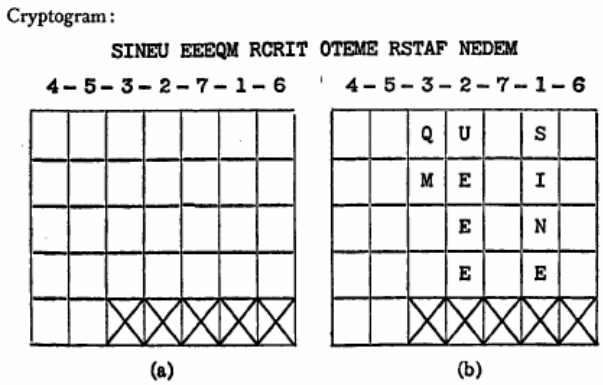


Figure 2.9: Figure 8

29 Modification of Columnar Method

A variation of the columnar procedure, but one that produces exactly the same results, may be found useful. First, write the message in groups corresponding to the length of the key. Thus, using the same key and message as in paragraph 28, the following is obtained:

```
4-5-3-2-7-1-6 | 4-5-5-2-7-1-6 | 4-5-32-7-1-6 | 4-5-3-2-7-1

R E Q U E S T | I M M E D I A | T E R E E N F | O R C E M E

4-5

T S
```

The letters are then taken from the groups and are transcribed in groups of five, all letters marked 1 being taken first, then all those marked 2, and so on. Thus, the first two cipher text groups are SINEU EEEQM, and the complete text is identical with that produced in figure 7.

30 Addition of Nulls to Complete a Final Group

The example given in the preceding case happened to contain 30 letters, a number that is an exact multiple of five. Thus, the final group in the cryptogram automatically became a complete group. For accuracy, the final group of every message should be complete; therefore, if the number of letters in the text of a message is not a multiple of five, it should be made so by the addition of nulls, before the transposition process is applied (see par. 23b).

III MISCELLANEOUS TRANSPOSITIOlN METHODS

31 Transposition Systems Employing Special Designs

a. Triangles, trapezoids, and other polygons are among the many designs used to produce transposition ciphers. Most of them, however, are impractical for wide military use but are used occasionally by secret agents.

b. A grille is a common transposition device of some practical importance. There are several types and one of the most common is that known as the rotating grille. It 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 crosssection 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 a 90 turn clockwise or counterclockwise, as agreed, and the fresh cells exposed by the perforations are filled with the next few letters of the text. 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 occupied by letters. The grille is then removed and the letters of the sheet underneath it are transcribed in accordance with some prearranged route 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 field military use. Furthermore, practical difficulties connected with the preparation and distribution of many grilles would make it almost inevitable that several messages would be enciphered by the same grille. The degree of cryptographic security aorded by them is not so great as may be suspected; sometimes single messages of fair length may be solved.

32 Polyliteral and Word Transposition

a. Thus far only individual letters, as units for the transposition process have been discussed. It is possible to use pairs of letters, sets of three or more letters, or entire words as units; procedures are the same in monoliteral and polyliteral transpositions. Sometimes more complicated routes may be followed in transposition; for example, a route may be a prearranged succession of moves made by a knight in chess. It is usually necessary to have at hand a printed form showing the complete route, and this makes these methods impractical for field use. They may, however, be used in special cases.

b. The cipher system used by the Federal Army in the Civil War represents a good example of word transposition. In the earliest form in which this cipher was used by the Federals only one route was used, which consisted in writing the text in six columns, going up the sixth, down the first, up the fifth, down the second, up the fourth, and down the third. Arbitrary words were substituted

for proper names, nulls were introduced at regular positions, and words even often misspelled for further obscurity. For example, the word operation was often spelled as two words: opera, and shun. Later, many additional routes were provided, relatively long lists of arbitrary equivalents for names, numbers, dates, common military terms, etc., were added, and the whole system was made considerably more complicated. While the security afforded by this system was probably ample for those days, it would hardly be sufficient today to permit its use even in cases where a delay of only a few hours is required. Furthermore, if long lists of arbitrary equivalents must be handled, the system presents all the disadvantages of a poor cipher system with but few of the advantages offered by a good code system.

33 Single and Double Transposition Methods

In single transposition methods the letters go through only one transposition from plain text to cipher text. It is possible to take the letters resulting from a first transposition and apply a second transposition to them; cryptograms so prepared often present a very great degree of security. Triple and quadruple transposition is possible but wholly impracticable for common use. Only a very limited number of double transposition methods are practicable for military use, but the degree of security afforded by certain of them is much greater than that afforded by certain much more complicated substitution methods.

34 Factors Concerning Use of Transposition Systems

a. The transposition methods described above provide a wide range of cryptographic security; in some there is very little security, in others there is a great deal. All transposition systems usually present important advantages in speed and simplicity. These advantages have led to attempts to increase security in some manner or other; double transposition schemes, rotating grilles, and other more complicated methods have consequently been developed. In only certain types are written memoranda or devices required. Very often the entire cryptographing process in even very complex methods may be easily memorized by persons of very good intelligence, such as secret agents. For these reasons transposition systems are often useful in espionage and counterespionage activities.

b. But transposition ciphers for military usage present three very serious disadvantages. In the first place, the methods are such that they do not allow any latitude for errors in handling. Often if a single letter is omitted or added, as not infrequently happens in telegraphic transmission, the whole message becomes difficult if not impossible to decryptograph. In the second place, if two or more messages prepared in the same key and containing exactly the same number of letters are available for study, no matter how complicated the method employed, the cryptograms can be solved, and the key recovered, and applied to other cryptograms in the same key but with different numbers of letters. In military cryptography it is not unusual, in cases of heavy trafic, to have as many

as 100 or 200 messages transmitted on the same day, all in the same key. Control from a central headquarters of the exact message length would obviously be impossible. The chances, therefore, that the enemy may actually intercept and find several messages of identical length are not negligible. Thus, a transposition method presenting an extremely high degree of cryptographic security when only a few messages are to be cryptographed fails seriously when employed for heavy trafiic. Finally, in certain cases, where the double transposition produces a great degree of security, it is almost inevitable that a poorly trained or careless cryptographic clerk will fail to perform both steps correctly. Not only messages prepared by one poor or careless operator, but all other messages, even though correctly prepared, are thus laid open to solution.

Chapter 3

ELEMENTARY SUBSTITUTION SYSTEMS

I GENERAL

35 Fundamental Nature of Substitution Methods. Cipher Systems and Code Systems

Methods now to be described differ from those above in that elements or textual units composing the original plain text retain their relative positions, but not their identities, and are replaced by other elements or textual units so that the external form of the writing is cryptographic in nature. For this reason these methods are called substitution methods. They may deal with individual letters, pairs of letters, sets of letters in regular groups, syllables, whole words, phrases, and sentences. Substitution methods may accordingly be subdivided into letter methods, syllable methods, and word methods, as in the case of transposition methods; but such a classication is a rather arbitrary one and is not based on the nature, form, or external appearance of the cryptographic text. For example, a substitution method dealing with single letters of the plain text may not involve their replacement by other single letters. In some cases whole words may be used to replace single letters. Outwardly, such a cryptogram gives the appearance of dealing with words, but its internal nature is quite clear: single-letter substitution has been effected. The classication indicated is, nevertheless, a useful one. When the cryptographic process involves the treatment of individual letters or pairs of letters, and only exceptionally the treatment of syllables or whole words, the method is known as a substitution cipher system; and when the process involves 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.

36 Nature of Alphabets

a. The simplest kind of substitution cipher is that which is known in literature as Julius Caesars 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 by E, and so on. The word CAB becomes converted into F DE which is cipher.

b. The English language is written by means of 26 simple characters called letters which, taken together and considered as a sequence of symbols, constitute the alphabet of the language. Not all systems of writing are of this nature. Chinese writing is composed of about 44,000 complex characters, each representing one sense of a word. Whereas English words are composite or polysyllabic and may consist-of one to eight or more syllables, Chinese words are all monosyllables and each .mono- syllable is a word. Written languages of the majority of other civilized peoples of today are, however, alphabetic and polysyllabic in construction, so that principles discussed here apply to all of them.

c. The letters composing the English alphabet used today are the results of a long period of evolution, the complete history-of which may never fully be known. They are conventional symbols representing elementary sounds, and any other simple symbols, so long as the sounds which they represent are agreed upon by those concerned, will serve the purpose equally well. If taught from early childhood that the symbols $, *, and @ represent the sounds Ay, Bee, and See, respectively, the combination $* would still be pronounced CAB, and would, of course, have exactly the same meaning as before; or suppose that two persons have agreed to change the sound values of the letters, F, G, and H, and after long practice have become accustomed to pronouncing them as Ay, Bee, and See, respectively. They would then write the word" HFG, pronounce it CAB, and see nothing strange whatever in the matter. But to others not party to their arrangements HFG constitutes cipher. The combination of sounds called for by this combination of symbols is perfectly intelligible to the two who have adopted the new sound values for those symbols and therefore pronounce HFG as CAB, but HFG is utterly unpronounceable and wholly unintelligible to others who are reading it according to their own long established sound-symbol basis. It would be stated that there is no such word as HFG, which would mean merely that the particular combination of sounds represented by this combination of letters has not been adopted by convention to represent a thing or an idea in the English language. Thus it is seen that, in order for the written words of a language to be pronounceable and intelligible to all who speak that language, it is necessary, rst, that the sound values of the letters or symbols be universally understood and agreed upon and, secondly, that the particular combination of sounds denoted by the letters should have been adopted to represent a thing or an idea. Spoken plain language consists of vocables; that is, combinations and permutations of elementary speechsounds which have by long usage come

to be adopted and recognized as representing denite things and ideas. Written plain language consists of words; that is, combina- tions and permutations of simple symbols, called letters, which represent visually and call forth vocally the elementary speech-sounds of which the spoken language is composed.

d. It is clear also that in order to write a polysyllabic language with facility it is necessary to establish and to maintain by common agreement or convention, equivalency between two sets of elements, rst, a set of elementary sounds and, second, a set of elementary symbols to represent the sounds. When this is done the result is what is called an alphabet, a word derived from the names of the rst two letters of the Greek alphabet, alpha and beta.

e. Theoretically, in an ideal alphabet each symbol or letter would denote only one elementary sound, and each elementary sound would invariably be represented by the same symbol. But such an alphabet would be far too difficult for the average person to use. It has been conservatively estimated that a minimum of 100 characters would be necessary for English alone. Attempts toward producing and introducing into usage a practical, scientic alphabet have been made, one being that of the Simplied Spelling Board in 1928, which advocated a revised alphabet of 42 characters. Were such an alphabet adopted into current usage, in books, letters, telegrams, etc., the exibility of cryptographic systems would be innitely extended and the difculties set in the path of the enemy cryptanalysts vastly increased. The chances for its adoption in the near future are, h0wever, quite small. Because of the continually changing nature of every living language, it is doubtful whether an original perfect alphabet could, over any long period of time, remain so and serve to indicate with great precision the exact sounds which it was originally designed to represent.

37 Normal Alphabets and Cipher Alphabets

a. In the study of cryptography the dual nature of the alphabet be comes apparent. It consists of two parts or components, (1) an arbi- trarily arranged sequence of symbols.

b. The normal alphabet for any language is one in which these two components are the ordinary sequences that have been denitely xed by long usage or convention. The dual nature of our normal or everyday alphabet is often lost sight of. When we write A, B, C, . . . we really mean:

```
Sequence of sounds: "Ay" "Bee" "See"

Sequence of symbols: A    B     C
```

Normal alphabets of different languages vary considerably in the number of characters composing them and the arrangement or sequence of the characters. The English, Dutch, and German alphabets each have 26, the French 25, the Italian 21, Spanish 27 (including the digraphs ch and ll), Russian 31. The Japanese language has a syllabary consisting of 72 syllabic sounds, to express which 48 characters are employed.

c. A cipher alphabet or a substitution alphabet, as it is sometimes called, is one in which the elementary speech-sounds are represented by characters other than those representing them in the normal alphabet. These characters may be letters, gures, signs, symbols, or combinations of them.

d. A more technical denition of a familiar cipher may now be given: When the plain text of a message is converted into encrypted text by the use of one or more cipher alphabets, the resultant cryptogram constitutes a *substitution cipher*.

38 Two Components of an 'Alphabet

It is convenient to designate that component of a cipher alphabet con- stituting the sequence of speechsounds the plain component, and the component constituting the sequence of symbols the cipher component. If the plain component is omitted in a cipher alphabet, the latter is understood to be the normal sequence. For brevity and clarity, a letter of the plain text, or of the plain component of a cipher alphabet, is designated by sufxing a small letter p to it: A, means A of the plain text, or of the plain component of a cipher alphabet. Similarly, a letter of the cipher text, or of the cipher component of a cipher alphabet, will be designated by sufxing a small letter c to it: Xc means X of the cipher text, or of the cipher component of a cipher alphabet. The expression A,. = Xe means that A of the plain text, or A of the plain component of a cipher alphabet, is represented by X in the cipher text, or by X in the cipher component of a cipher alphabet.

39 Standard and Mixed Cipher Alphabets

In the arrangement or sequence of letters forming its cipher compo- nent, cipher alphabets arc of two kinds:

a Standard cipher alphabets, in which the sequence of letters in the cipher component is the same as the normal, but reversed in direction or shifted from its normal point of coincidence with the plain component.

b Mixed cipher alphabets, in which the sequence of letters or char- acters in the cipher component is no longer the same as the normal in its entirety.

40 Enciphering and Deciphering Alphabets

All cipher alphabets may be classied on the basis of their arrange- ment as enciphering or deciphering alphabets. An enciphering alphabet is one in which the sequence of letters in the plain component coincides with the normal sequence, and is arranged in that manner for convenience in encipherment. In a deciphering alphabet the sequence of letters in the cipher component coincides with the normal, for convenience in deciphering. For example, in gure 9, (a) shows a mixed cipher alphabet arranged as an enciphering alphabet; (b) shows

the corresponding deciphering alphabet. An enciphering alphabet and its corresponding alphabet present a verse and inverse relationship to each other. To invert a deciphering alphabet is to write the corresponding enciphering alphabet; to invert an enciphering alphabet is to write the corresponding deciphering alphabet.

Enciphering Alphabet

```
(a)    Plain:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
       Cipher: JKQVXZWESTRNUIOLGAPHCMYBDF
```

Deciphering Alphabet

```
(b) Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ
    Plain:  RXUYHZQTNABPVLOSCKIJMDGEWF
```

Figure 9

II MONOALPHABETIC SUBSTITUTION SYSTEMS

41 Single-Alphabet Substitution

If a message is enciphered, letterforletter, by using one cipher alphabet which has been drawn up for the purpose, the resulting crypto- gram is said to be enciphered by a single alphabet and to-be a single- alphabet, or monoalphabetic, substitution cipher. More complex ciphers may use several alphabets in the enciphering of a single message. When two or more cipher alphabets are used, the resulting cryptogram is said to be a polyalphabetic cipher.

42 Standard Alphabet Ciphers

a. Standard cipher alphabets are of two sorts:

(1). Direct standard, in which cipher component is the normal sequence but shifted to the right or left of its point of coincidence in the normal alphabet. Example:

$\longrightarrow$

```
Plain:   ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher : QRSTUVWXYZABCDEFGHIJKLMNOP
```

$\longrightarrow$

It is obvious that the cipher component can be applied to the plain component at any one of 26 points of coincidence, but since the alphabet that results

from one of these applications coincides exactly with the normal alphabet, a series of only 25 (direct standard) cipher alphabets results from the shifting of the cipher component.

Reversed standard, in which the cipher component is also the normal sequence but runs in the opposite direction from the normal. Example:

```
->
Plain:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: QPONMLKJIHGFEDCBAZYXWVUTSR
<-
```

Here the cipher component can be applied to the plain com- ponent at any of 26 points of coincidence, each yielding a different cipher alphabet. There is in this case, therefore, a series of 26 (reversed standard) cipher alphabets.

b. It is often convenient to refer to or designate one of a series of cipher alphabets without ambiguity or circumlocution. The usual method is to indicate the particular alphabet to which reference is made by citing a pair of equivalents in that alphabet. For example, the reversed alphabet above, one of a series of 26 related alphabets, may be designated as that in which Ln = Fc or Wp = Uc. But the most common basis of reference is the letter which represents the rst or initial letter of the plain component, usually A,. Thus, the key for the cipher alphabet just referred to, as well as that preceding it, is A, = Qc, and it is said that the key letter for the cipher alphabet is Qc.

43 Reciprocal Alphabets

a. The cipher alphabet in paragraph 42a (2) is also a reciprocal alphabet; that is, the equivalents show reciprocity and are reversible or reciprocal in pairs. For example, in the alphabet referred to, Ap = Qc and 9,. =Ac ; B, = PC and Pp = Be, etc. The reciprocity exists throughout the alphabet and is a result of the method by which it was formed.

b. A series of related reciprocal alphabets may be derived by juxtaposing at all possible points of coincidence two components which are identical but progress in opposite directions. This holds regardless of whether the components are composed of an even or an odd number of elements. The reciprocal alphabet (par. 42a (2)) is one of such a series of 26 alphabets.

c. A single or isolated reciprocal alphabet may be produced in one of two ways:

(1). By constructing a complete reciprocal alphabet by arbitrary or random assignments of values in pairs. That is, if A, is made Kc, then K,, is made Ac; if B, is made Re, then R, is made Be, and so on. If the two components thus constructed are slid against each other no additional reciprocal alphabets will be produced.

(2). By juxtaposing a sequence comprising an even number of elements against the same sequence shifted exactly half way to the right (or left), as seen below;

```
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
          ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

d. A reciprocal alphabet is an inverse alphabet, since it may serve either as an enciphering or deciphering alphabet.

44 Procedure in Enciphermenf and Decipherment

a. When a message is enciphered monoalphabetically, that is, by means of a single cipher alphabet, letters of the text are replaced by the equivalents in the cipher alphabet selected by prearrangement. Example:

Message: THREE MACHINE GUNS CAPTURED.

Enciphering Alphabet: Reversed Standard, AI) = D.,.

```
Plain :  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher : DCBAZYXWVUTSRQPONMLKJIHGFE
```

Letter-for-letter encipherment:

```
THREE MACHINE GUNS CAPTURED
KWMZZ RDBWVQZ XJQL BDOKJMZA
```

The cipher text is then grouped in ves and the indicator letter D[1] inserted as the initial letter of the rst group (or any other prearranged group).

Cryptogram:

```
DKWMZ ZRDBW VQZXJ QLBD-O KJMZA
```

Figure 10

b. The procedure in decipherment is merely the reverse of that in encipherment. The initial letter of the message, D, indicates A, = Dc in the cipher alphabet. The deciphering alphabet is therefore as follows:

```
Cipher : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Plain :  DCBAZYXWVUTSRQPONMLKJIHGFE
```

The message deciphers thus:

```
Cipher: (D) KWMZ ZRDBW VQZXJ QLBDO KJMZA
Plain:      THRE EMACH INEGU NSGAP TURED
```

The deciphering clerk rewrites the text in word lengths: THREE MACHINE GUNS CAPTURED

c. When a mixed alphabet is used, the enciphering and deciphering processes are the same as those described under a and b above. For speed in cryptographing, the cipher alphabet is prepared in the form of an enciphering alphabet, and for speed in decryptographing, in the form of a deciphering alphabet.

[1]If this or any such similar convention has been agreed upon by the correspondents

III TYPES OF MIXED CIPHER ALPHABETS

45 Systematically Mixed Cipher Alphabets

It will be recalled that in a mixed cipher alphabet the sequence of letters or characters in the cipher component does not correspond to the normal sequence. 'There are various methods of mixing up the letters of the cipher component, and those which are based upon a scheme that is systematic in its nature are very useful because they make possible the derivation of one or more mixed sequences from any easily remembered word or phrase, and thus do not necessitate the carrying of written memoranda. They are called systematically mixed cipher alphabets.

46 Key-word Mixed Alphabets

a. One of the simplest types of systematically *mixed cipher alphabets* is the key-word mixed alphabet. The cipher alphabet consists of a key word or phrase (with repeated letters, if present, omitted after their rst occurrence), followed by the letters of the alphabet in their normal sequence (with letters already occurring in the key, of course, omitted). Example, with GOVERNMENT the key word:

```
Enciphering alphabet....  { Plain:  ABCDEFGHIJKLMNOPQRTSUVWXYZ
                            Cipher: GOVERNMTABCDFHIJKLPQSUWXYZ
```

b. Mixed alphabets formed by including all repeated letters of the key word or key phrase were common in Edgar Allan Poes day but are impractical because they make decipherment diicult.

```
Enciphering alphabet.... { Plain:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
                           Cipher: NOWISTHETIMEFORALLGOODMENT
Deciphering alphabet.... { Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ
                           Plain:  P  VHMSGD  QKAB  OEF  C
                                      L   J  RWYN    I
                                      X         T    Z
                                                U
```

The average cipher clerk would have considerable difculty in decryptographing a cipher group such as TOOET, each letter of which has three or more equivalents, and from which the plain-text words (N) INTH, . .FT THI (S), IT THI . . . , etc., can be formed on decipherment.

c. An example of a key-word mixed alphabet is shown in gure 9, where, in its enciphering form, the cipher component presmts to the experienced eye the skeleton of the key upon which the alphabet is based: WESTERN UNION TELEGRAPH COMPANY. Any easily remembered word, phrase, or sentence may be used. The starting point of the sequence, when used as a cipher component, may be indicated in the usual manner. For example, in the alphabet referred to, the alphabet key is A, = In. Two or more correspondents using

the prearranged key, WESTERN UNION TELEGRAPH COMPANY, would obtain the same disarranged sequence; when this sequence is to form the cipher component of a cipher alphabet, the prearranged key letter A1, = Jo would result in giving each correspondent exactly the same cipher alphabet. The key words or phrases need not consist of any denite number of letters, but it is advisable to use for keys such words or phrases as will most thoroughly disarrange the normal sequence. (See, in this connection, par. 26.) A key-word mixed alphabet will manifest the key word or parts of it only when the alphabet is in the form of an enciphering alphabet. Note that alphabet (b) of gure 9 no longer gives any external evidence of having been derived from the phrase WESTERN UNION TELEGRAPH COMPANY.

47 Transposition-mixed Alphabets

a. It is possible to disarrange the sequence even more thoroughly by applying a simple method of transposition to the keyword sequence as if it were a message. An example is illustrated in gure 11.

Key word:

```
TELPHONY
```

(a) Simple columnar transposition:

```
TELPHONY
ABCDFGIJ
KMQRSUVW
XZ
```

Mixed sequence :

```
TAKXEBMZLCQPDRHFSOGUNIVYJW
```

(b) Numerical key, columnar transposition:

```
7-1-5-6-2-5-4-8
T E L P H O N Y
A B C D F G I J
K M Q R S U V W
X Z
```

Mixed sequence :

```
EBMZHFSLCQNIVOGUPDRTAKXYJW
```

Figure 11

b. The last two systematically mixed cipher alphabets are transposition-mixed alphabets. Almost any of the methods of transposition described in sections IV and V of this chapter may be applied to them.

48 Decimation Method of Forming Mixed Alphabets

Another simple method of forming a mixed alphabet is the decimation method. In this method, letters in the normal alphabet, or in a keyword mixed alphabet, are counted off according to a selected odd interval. As each letter is decimat-edthat is, eliminated from the basic alphabet by counting offit is entered in a separate list to form the sequence of the mixed alphabet. For example, to form a mixed alphabet by this method from an alphabet based on the key phrase SING A SONG OF SIX PENCE with 7 the interval selected, proceed as follows:

a Key-word (or basic) alphabet:

```
SINGAOFXPECBDHJKLMQRTUVWYZ
```

b When the letters are counted off by 7s frOm left to right, F will be the first letter arrived at, H the second, T the third:

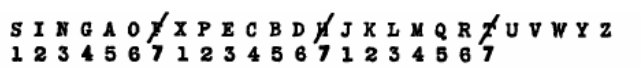


Figure 3.1: Fig. B

These letters are entered in a separate list (F rst, H second, T third, etc.) and eliminated from the keyword alphabet.

c When the end of the key-word alphabet is reached, return to the beginning, skipping the letters already eliminated:

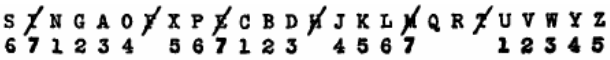


Figure 3.2: Fig. C

d Mixed alphabet.

```
FHTIEMZPQNDWCVBSLXAGOKYJRU
```

49 Random-Mixed Alphabets

Practical considerations, of course, set a limit to the complexities that may be introduced in constructing systematically mixed alphabets. Beyond a certain point there is no object in further mixing. The greatest amount of mixing by systematic processes will give no more security than that resulting from mixing the alphabet by random selection, such as by putting the 26 letters in a box, thoroughly shaking them up, and then drawing the letters out one at a time. Whenever the laws of chance operate in the construction of a mixed alphabet, a thorough disarrangement is bound to be produced. Random-mixed alphabets give more Cryptographic security than do the less complicated systematically mixed alphabets because they afford no clues to positions of letters, given the positions of a few of them. Their chief disadvantage is that they must be reduced to writing, since they cannot readily be remembered, nor can they be reproduced at will from an easily remembered key word.

50 Number of Single Alphabets Available from a Basic Alphabet

It is obvious that the cipher component of a cipher alphabet may be shifted or slid against the plain component at 26 points of contact so as to produce a series of different enciphering alphabets. For example, the mixed sequences given under (b) of gure 11, when used as a cipher component, yields the following two of a series of 26 cipher alphabets:

Enciphering Alphabets

```
(1) Plain:   ABCDEFGHIJKLMNOPQRSTUVWXYZ
    Cipher : EBMZHFSLCQNIVOGUPDRTAKXYJW

(2) Plain:   ABCDEFGHIJKLMNOPQRSTUVWXYZ
    Cipher : WEBMZHFSLCQNIVOGUPDRTAKXYJ
```

The message DAILY REPORT NOT RECEIVED YET would be enciphered by the rst alphabet as:

```
Plain:  DAILY REPOR TNOTR ECEIV EDYET
Cipher: ZECIJ DHUGD TOGTD HMHCK HZJHT
```

and by the second alphabet as:

```
Plain:  DAILY REPOR TNOTR ECEIV EDYET
Cipher: MWLNY PZGOP RVORP ZBZLA ZMYZR
```

Externally the two cryptograms seem different except in length. The two enciphering alphabets present the same sequence in the cipher component, but this entirely disappears in the corresponding deciphering alphabets, which are as follows:

Deciphering Alphabets

```
(1) Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ
    Plain:  UBIRAFOELYVHCKNQJSGTPMZWXD

(2) Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ
    Plain:  VCJSBGPFMZWIDLORKTHUQNAXYE
```

It is possible to write the same message in 25 different external forms, each using a different cipher alphabet of a series derivable from a basic sequence. The basic sequence or alphabet in such a case is often called a primary sequence or a primary alphabet; derived alphabets are called secondary alphabets. In producing secondary alphabets the basic sequence must be juxtaposed and slid against itself, or against the normal sequence, or against another mixed sequence. In all cases secondary alphabets form a series of alphabets that are interrelated and that either directly or indirectly manifest relationships which are important from a cryptanalytic point of view. It should be clear now that by means of a single, prearranged, secret word it is possible for two correspondents to send a whole set of messages all in different mixed alphabet, or to use a different alphabet for each of 26 consecutive days.

51 Miscellaneous Types of Cipher Alphabets

a. The cipher alphabets shown thus far have used only letters, but alphabets in which the cipher component consists of gures, or groups of gures, are not uncommon in military cryptography. Cipher alphabets using signs and symbols are not suitable for military cryptography because they can neither be telegraphed nor telephoned with any degree of accuracy, speed, or facility. Since there are but ten digits it is obvious that, in order to represent a camplete alphabet in gure ciphers, combinations of at least two digits are necessary. The simplest kind of such an alphabet is that in which $A_p = 01$, $B_p = 02$,. . . $Z_p = 26$.

	1	2	3	4	5	6	7	8	9	0
1	A	B	C	D	E	F	G	H	I	J
2	K	L	M	N	O	P	Q	R	S	T
3	U	V	W	X	Y	Z	.	,	:	;

Figure 3.3: Figure 12

b. Instead of a simple alphabet of the preceding type, it is possible to use a simple diagram of the type shown in gure 12. Here the digits at the side and top of the rectangle are used to designate, according to the coordinate system, the

cell occupied by each letter and punctuation mark within the rectangle. When used for such purposes, the gures (or letters) constituting coordinate elements are referred to as raw and column indicators. It is usually necessary to agree beforehand upon which indicator will be given as the rst half of the equivalent for a letter, the row indicator or the column indicator, in order to avoid ambiguity or error. In all of the systems to be described here, the row indicator will always form the rst half of an equivalent. Accordingly in gure 12, the letter A, = 11, B, = 12, and so forth.

c. A variation of the foregoing diagram is exemplied in gure 13. Here, letters of the alphabet are inserted in the 25 cells of a large square, I and I being written together in one cell. Then a key word of ve let- ters is applied to the top of the large square and the same or a differ- ent key word is applied to the side of the square to form column and row indicators. In gure 13, for example, Sp = TI; W: = EH; etc.

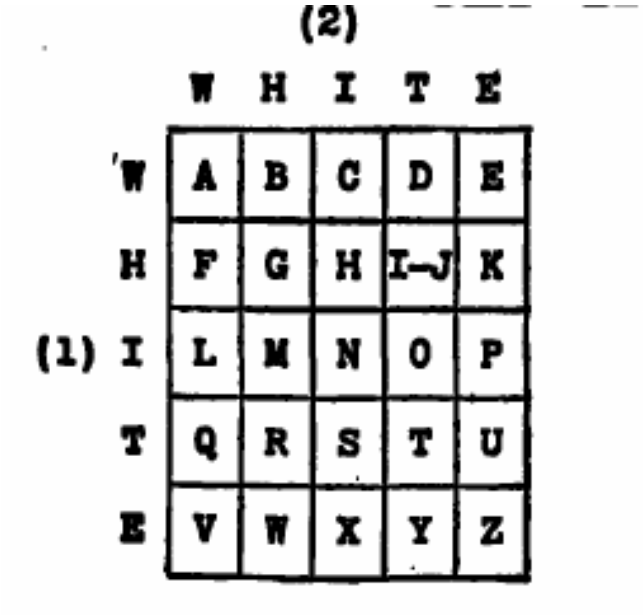


Figure 3.4: Figure 13

The message RAIDERS HAVE GONE is enciphered thus:

```
Plain:   R  A  I  D  E  R  S  H  A  V  E  G  O  N  E
Cipher: TH WW HT WT WE TH TI HI WW EW WE HH IT II WE
```

The cryptogram is then transmitted in groups of ve letters:

```
Cryptogram: THWWH TWTWE THTIH IWWEW WEHHI THWE
```

d. In these two systems just described,

(1). The letters of the alphabet within the square or rectangle may be xed in a mixed sequence, either systematically or random- mixed sequences being possible.

(2). The column and row indicators may be the same, or different; when letters are used they may form a key word or they may not; the key words, if formed, may be identical or nonidentical.

e. When letters are used as column and row indicators, they may be selected so as to result in producing cipher text that resembles made-up words, that is, words composed of regular alternations of vowels and consonants. For example, if in gure 13 the row indicators consisted of the vowels A E I O U in this sequence from the top down, and the column indicators consisted of the consonants B C D F G in this sequence from left to right, the word RAIDS would be enciphered as OCABE FAFOD, which very closely resembles code of the type formerly called articial code language. Such a system may be called a false, or pseudo-code system.[2]

IV MONOALPHABETIC SUBSTITUTION WITH VARIANTS

52 Purpose of Providing Variant Values

The individual letters composing ordinary intelligible plain text are used with varying frequencies; some, such as (in English) E, 'l, R, I, and N, are used much more often than others, such as J, K, Q, X, and Z. In fact, each letter has a characteristic frequency by means of which denite clues are afforded in the solution of simple substitution ciphers. This has led cryptographers to devise methods for disguising, sup pressing, or eliminating the characteristic frequencies manifested by the letters of cryptograms produced by simple monoalphabetic substitution. One such method is that in which the letters of the plain component of the cipher alphabet are assigned two or more equivalents in the cipher component and they are, for this reason, called variant values. In some cases the letters of the plain component receive numbers of variant .values, or variants, in proportion to their normal frequencies; in other cases, all the letters receive equal numbers of variant values, determined by the total number available.

53 Figure Ciphers with Variant Values

a. The use of gures in pairs as substitution equivalents makes available a total of 100 different pairs, those from 00 to 99. They may all be used in a complete system, or only certain ones may be selected, as prearranged.

[2]Prior to 1934, International Telegraph Regulations required code words of ve letters to contain It least one vowel and code words of ten letters to contain at least three vowels. The Madrid Conference held in 1932 amended these regulations to permit the use of code groups containing any combination of letters. These unrestricted eude groups were authorized for use after 1 January 1934.

b. One of the most common varieties of ciphers using all the pairs of digits is that in which the alphabet is reduced to 25 letters (by making 1 and J interchangeable or by eliminating a letter such as Q), and each letter is assigned four values which may be used at will. The assignment of values may be based upon a key word of four letters, each of which designates the starting points of a normal sequence of 25 numbers. An example is shown in gure 14, wherein the key word is TRIP. This means that in the rst set of numbers, 01 to 25, the rst number, 01, is assigned to the letter T; in the second set, from 26 to 50, the rst num- ber, 26, is assigned to the letter R; in the third set, from 51 to 75, the rst number, 51, is assigned to the letter I; nally, in the last set, from 76 to 00, the rst number, 76, is assigned to the letter P.

The letter Ap may be represented by any one of four equivalents, 08, 35, 68, and 87; the letter B, by 09, 36, 69, 88; and so on. The equivalent used in any particular instance is selected at random, so that the word .CAB may be represented in cipher by any one of a total of 64 combina- tions, such as 100809, 703509, 370869, etc. In the nal cryptogram the gures may be run together in groups of ve. The cipher group 10080, on deciphering, would be split up into 10-080.

A-08 35 68 87	I-J-16 43 51 95	S-25 27 50 79
B-09 36 69 88	K-17 44 52 96	T-01 28 61 80
C-10 37 70 89	L-18 45 53 97	U-02 29 62 81
D-11 38 71 90	M-19 46 54 98	V-03 30 63 82
E-12 39 72 91	N-20 47 55 99	W-04 31 64 83
F-13 40 73 92	O-21 48 56 00	X-05 32 55 84
G-14 41 74 93	P-22 49 57 76	Y-06 33 55 85
H-I5 42 75 94	Q-23 50 58 77	Z-07 34 57 86
	R-24 26 59 78	

Figure 14

c. In this case, within each set of 25 the numbers progress serially, each set being treated as a ring or circle. It is of course possible to mix the sequence to destroy this serial progression, thus giving four mixed alphabets which can be used at random.

d. Another variation 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 such as E, T, R, I, and N will have perhaps seven or eight different equivalents, whereas letters of low frequency such as J, K, Q, X, and Z will each have but one equivalent.

54 Use of Rectangles to Provide Variant Values

a. Instead of drawing up alphabets as in gure 14, it is possible to use the diagram shown in gure 12, but with several variant digits as row indicators instead of a single digit for each row. For example, the row indicators may be of the following arrangements:

```
1-6-7    1-2-3   1-2-3   5-4-3
2-5-8    4-5-6   8-9-4   6-9-2
3-4-9    7-8-9   7-6-5   7-8-1, etc.
```

Thus, if the rst arrangement is used, A, would have the equivalents 11, 61, 71; B,,, 12, 62, 72; etc. The word RUN might be represented by any one of 27 different combinations, such as 283124, 289154, etc.

b. A variation of the foregoing system is that in which, by use of a diagram of the type shown in gure 13, a number of different letters are applied to each row and column, or Z-gure numbers may be used for this purpose. In this case a series of as many as 50 pairs of digits may be used as row indicators, and another series of 50 pairs as the column indicators.

c. The use of variants lends itself to application in a pseudo-code system such as described in paragraph 51e. It presents many possibilities for variation, with or without key words, with one or more alphabets distributed within the square or rectangle, with alphabets extended to include gures, punctuation signs, common syllables and words, etc. Some times pseudo-code is encountered when the groups of a numerical cipher system (or a gure-code system) are converted into letters, in order to make the cryptographic text conform to certain telegraph regulations and thus have the message accorded a more favorable rate of charge (sec. II, ch. 4). Thus, a group such as 0125784256 might be converted into the group BAFOSULAFE. If the conversion table "is irregular in its construction and is kept secret, this adds an encipherment step to the system.

55 Disadvantages of Monoalphabotic Substitution with Variants

The obvious disadvantage of all such methods discussed in the preceding paragraph is that the cryptographic text is exactly twice as long as the original plain text. Furthermore, there is no compensating advantage from the standpoint of cryptographic security. When methods are such that the cipher equivalents are passed through another process which returns the cipher text to a length identical with that of the equivalent plain text, they are usually too complicated, too slow, and too subject to error to be practical. They are often the result of combining substitution and transposition processes in one system. Methods which substitute three or more characters for one letter of the original text are not at all practical for military cryptography.

V POLYALPHABETIC SUBSTITUTION SYSTEMS

56 Monoalphabetic and Polyalphabetic Substitution

a. In the substitution methods thus far discussed it has been noted that only one cipher alphabet is used in the encipherment of a message, and that as a class

they constitute the type of system designated as monoalphabetic substitution. It is true that in certain of the systems monoalphabetic substitution with variant equivalents takes place, there are two or more complete alphabets involved and that these systems may, therefore, with apparently good reason be designated as polyalphabetie substitution. This designation, however, will be seen to be somewhat inaccurate when cases of true polyalphabetie substitution come to be studied. The real or essential difference between the two systems may best be made clear by setting forth the primary object in each case.

b. In monoalphabetic substitution with variant values, the object of having di-erent sets of equivalents is to suppress so far as possible by simple methods the characteristic frequencies of letters. One such method consists in merely providing one or more different values as cipher equivalents of the same plain-text letter, of a few different values as equivalents of some of the high-frequency letters. Now there are certain conditions inherent in the method itself, conditions which cannot here be indicated, that result in producing in the cryptograms certain denite clues leading to the rapid establishment, in cryptanalysis, of the equivalence of different variant values. Furthermore, in these systems the varying or alternative equivalents for plaintext letters are subject to the free choice and caprice of the encipherer. If he is careful and conscientious in the work he will actually make use of all the variant values afforded by the system; but if he is slipshod and hurried in his work, he will use the same equivalent repeatedly rather than take pains and time to refer to his charts, tables, or diagrams to nd variants. The result is that the cryptograms based upon these methods are open to easy solution, even when the basic methods are such as would make a solution difficult without the interception of carelessly enciphered messages. What is necessary is a system in which there is established a denite procedure for auto matically shifting or changing the cipher alphabets employed in the encipherment of a single message; a method which within certain limits is beyond the momentary whims of cipher clerks, and which to a higher degree makes difcult the establishment of the equivalency of different cipher values. These are the objects of true polyalphabetic substitution systems. The number of such systems is large. Therefore, it will be possible to describe only a few of the more common or typical examples of methods practicable for military use.

c. The three methods (a) simple monoalphabetic substitution, (b) monoalphabetic substitution with variants, and (c) true polyalphabetic substitution, are attended by the following consequences in the plain text cipher relationship, a careful study of which will help to understand their similarities and differences:

(1). Encipherment

In method (a) each plain-text letter is represented by one and always the same cipher equivalent.

In method (b) and method (c), each plaintext letter is repre- sented by two or more different cipher equivalents, but in method (b) the variations are subject only to the whim of the encipherer, whereas in method (c) the identities of the cipher letters are determiner! by the positions they occupy in the text.

(2). Decipherment

In method (a) and method (b), each cipher equivalent repre sents one and always the same plaintext letter.

In method (c) one and the same cipher equivalent represents two or more different plaintext letters, the identities of which are determined by the positions they occupy in the text.

57 Example of Polyalphabec Substitution

a. A simple example may be used to illustrate what is meant by true polyalphabetic substitution. Suppose that two correspondents agree upon a numerical key, for example, 74030274, 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 en- ciphered by key number 7, it is to be replaced by Y. The numerical key is written under the letters of the plaintext letter for letter, and is repeated until the whole text is covered. Let the message be REENFORCEMENTS BEING RUSHED. The encipherment of a message is shown in gure 15. For convenience in counting forward (to the right) to nd cipher equivalents, a normal alphabet is given at the top of the gure.

```
Normal alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Plain: REENFORCEMENTS BEING RUSHED

Key:    74030274740502 74740 302747
Cipher: YIEQFQYGLQEQTU IIPRG UUUOIK
```

The text is then transmitted in ve-letter groups.

```
Cryptogram: YIEQF QYGLQ EQTUI IPRGU UUOIK
```

Figure 15

b. To decipher such a cryptogram, the clerk writes the numerical key over the cipher letters and then counts backward (to the left) in the normal alphabet as many places as indicated by the key number standing over each letter. Thus:

```
Normal alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Key:    74030 27474 03027 47405 02747
Cipher: YIEQF QYGLQ EQTUI IPRGU UUOIK
Plain:  REENF ORCEM ENTSB EINGR USHED
Message: REENFORCEMENTS BEING RUSHED
```

Figure 16

58 Systematizing the Work

The work of encipherment may be materially shortened by systematizing the procedure. Instead of having to write the key over and over again in order to cover the text completely, the text may be written in sets of letters corresponding in length to the length of the key. Thus the text may be written underneath a single appearance of the key in successwe short horizontal lines, leavmg space between the lines for the insertion of cipher equivalents, as shown gure 17a. Instead of enciphering the letters by individual, repeated countings, two strips

```
7 4 0 3 0 2 7 4
R E E N F O R C
E M E N T S B E
I N G R U S H E
D
```

Figure 17a

of paper bearing normal alphabets may be juxtaposed in the proper relative positions to encipher a whole column of letters at one setting of the strips. Thus, for the rst column, with the key number 7, the strips are juxtaposed so that the rst letter in the column, viz., R (which is to be represented by the seventh letter to the right of it, and is therefore to be enciphered by Y of the lower strip) is directly above Y, as follows:

```
Plain :
ABCDEFGHIJKIMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher:             ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

The equivalents for the rest of the letters of the rst column may now be rewritten down in their proper places, reference being made to the alphabet strips to see what the cipher letters should be: $E_p = L_c$; $I_p = P_c$; $D_p = K_c$. For the second column the two alphabet strips are in these relative positions:

```
Plain :
ABCDEFGHIJKIMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher:                ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

The cipher equivalents for the second column are: $E_p = I_c$; $M_p = Q_c$; $N_p = R_c$. The process is continued in this manner until all the columns have been enciphered, as shown in gure 17b.

The cipher text is then transcribed in groups of ve letters, reading the successive lines in the normal manner, that is, from left to right and from the top downwards, yielding the groups YIEQF, QYGLQ, etc. It is no more difcult to encipher a message by this systematized procedure than by the longer and slower method of writing the text out in long lines and repeating the key over and over again. What is more important is that the shortened procedure promotes accuracy in enc1pl'1erment. A few seconds careful checking of the relative

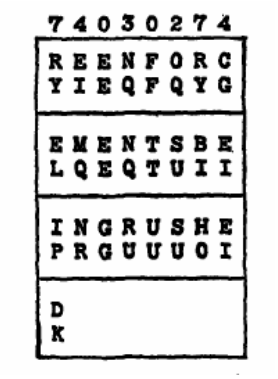


Figure 3.5: Figure 17b

positions in which the two alphabet strips are set is all that is required but this checking is very' necessary, for if that is wrong all the cipher letters in that column to which this setting applies will be in error.

59 Using Key Words to Indicate Number, Identity, and Sequence of Cipher Alphabets Employed

a. If reference is made to the two settings of alphabet strips in paragraph 58, it will be noted that in the rst setting $A_p = H_c$, in the second $A_p = E_c$. If the eight settings of the strips are studied it will be found that the letters which A_p, represents successively are H, E, A, D, A, C, H, and E, giving the word HEADACHE. These settings, when rst presented in the foregoing description, correspond merely to the numerical key 74030274, but this numerical key is also expressible in terms of letters, which when put together properly spell a word. This is only another way of showing that key words may be employed in this type of substitution as in those previously described. Key words of various lengths and composition may be used, consisting of single words, long phrases, or sentences. In general, the longer the key the greater is the degree of cryptographic security. The method as a whole is often referred to as the repeating lacy method.

b. The number of elements in the keythat is, the number of letters or gures composing itdetermines the number of alphabets to be employed. The identity of each element of the key, the specic letter or gure it happens to be, determines specically which of a set of cipher alphabets pertaining to the whole system will be used. And the specic sequence or relative order of the elements of the key determines spe- cically the sequence with which the cipher alphabets are employed within the encipherment. The total number of cipher alphabets pertaining to or composing the system may be limited or unlimited. When they are produced as a result of the sliding of two basic or primary alphabets against each other, the number is limited to 26 in the English alphabet.

c. A brief notation for indicating or designating a specic key letter is to sufx the subscript k to it, just as the subscripts p and c are sufxed to letters to indicate letters of the plain text or cipher text, respectively. When the key letter occurs in an equation, it can be en- closed within parentheses to avoid ambiguity. Thus, $B_p\ (D_k) = E_c$ means that plain-text letter B when enciphered by key letter D (in a certain alphabet system) yields the cipher letter E.

60 Use Of Other Types of Alphabets

a. It has been noted that in the case of monoalphabetic ciphers, alphabets of various types may be employed. This is likewise true of polyalphabetic ciphers. Instead of using two alphabet strips bearing the normal alphabetic sequence to determine the cipher equivalent of a letter enciphered by a given key number or key letter, one may use a pair of strips, one of which bears the normal direct, the other the normal reversed sequence. In the former case one is dealing with direct' standard, in the latter, with reversed standard alphabets.

b. Polyalphabetic substitution with direct or reversed standard alphabets does not result in nearly so great a degree of cryptographic security as that resulting from the simple artice of providing mixed alphabets for the strips. All sorts of mixed alphabets may be used. One of the strips may bear the normal direct or reversed sequence; the other a mixed sequence. Both strips may bear identical mixed sequences proceeding in the same direction, or in opposite directions. Finally, both strips may bear different mixed sequences.

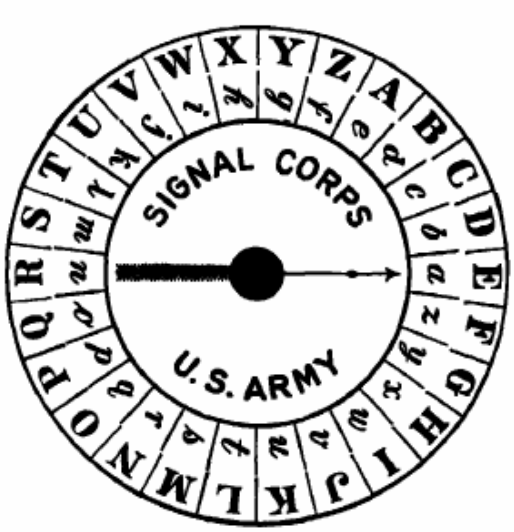
c. In all cases, except where reciprocal alphabets are produced, it is essential that the correspondents agree upon the sequence or strip from which the plain and the cipher letters respectively will be taken, that is, it is necessary to indicate which sequence constitutes the plain component, which the cipher component. If this is not done, two correspond- ents will have diiculty in deciphering one anothers messages. Also, as noted above, it is necessary to agree as to which letter the key letter is to be set against. The usual method is to agree that the initial letter of the plain component, usually Ap, will be set opposite the key letter, though other conventions are possible.

d. The sequences on the strips may be permanent or invariable, but naturally the degree of cryptographic security in this case is considerably lower than if they can be changed easily at the will of the correspondents and by prearrangement. It is possible that a secret word may serve as the basis not only for the key for shifting the strips, but also for the mixing of the alphabetic sequences. For example, two correspondents may agree to use the key CENTRAL AMERICA; to use the rst part as the basis for constructing the mixed plain component; the second part, for constructing the cipher component; and to use the whole phrase as the key for enciphcring the message. All the methods of constructing systematically mixed alphabets as described in section III of this chapter are applicable.

VI CIPHER DISKS AND SQUARE TABLES

61 Cipher Disks

a. In the foregoing section it was noted that the separate alphabets employed in the encipherment are produced by the use of only two strips of paper bearing the normal alphabet. Such strips are often referred to as sliding alphabets, because they can be shifted or slid against each other in any one of 26 points of contact or coincidence. Exactly the same results, so far as cipher equivalents are concerned, can be obtained by the use of other devices. First, there are the so-called cipher wheels or cipher disks in which an alphabet is written on the periphery of a rotating disk, the circumference of which is divided into 26 equal segments, and this disk is made to revolve concentrically upon a similar but slightly larger xed disk. Figure 18 shows the now obsolete U. S. Army Cipher Disk, which is of this simple type. Here the alphabetic sequences are printed on glossy celluloid, are permanent, and admit of no variatiom The use of unglazed celluloid upon which blank segments appear would permit of writing letters and erasing them as often as desirable. Thus, quick and easy change of alphabets would be possible.



To encipher a message, the key letter or the rst letter of the key word or phrase is set opposite a. Let us assume it to be "E." The cipher letters to be written are those opposite the text letter when a" on the circle is set opposite "E on the card. For example, send powder" would be written "MARBPQIBAN." To use a key word or phrase, each letter is used in turn to encipher one letter only. When the last letter of the key word is used, repeat until all letters of the message are enciphered. Numbers when enciphered with the disk must be spelled out.

Figure 3.6: Figure 18

b. The cipher alphabetsproduced by the cipher disk shown in the gure are merely reversed standard alphabets, the same as are produced by the use of sliding strips of paper, and by the use of certain; tables which are discussed below. The method of employing the disk needs no discussion. It may serve in monoalphabetic or polyalphabetic substitution with a key word or key number.

62 Square Tables

a. Tables known in the literature of cryptography under various names, such as Vigenre Table", "Square Table, "Quadricular Table, Pythagorean Table, Cipher Square, Cipher Chart", etc., are often employed in polyalphabetic substitution. All the results produced by their use can be duplicated by the employment of sliding alphabets or revolving disks. The modern form of the Vigenre Table is shown in gure 19. Such a table may be used in various ways, diering from one another in minor details. The most common method is to consider the top line of the table as containing the plain-text letters, the rst column at the left as containing the key letters. Then each successive horizontal line con-

Plain-Text Letter

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

Figure 3.7: Figure 19. The Vigenere Table.

tains the cipher equivalents for the plain-text sequence ABC . . . Z enciphered by the key letter which stands at its left in the rst column. Thus, the

cipher alphabet corresponding to key letter D is the sequence of letters in the fourth horizontal line under the plain-text line, where A, = Dc, Bp = EC, etc. It will be easy to remember, in using such a table, that the equivalent of a given plain-text letter, T,,, for example, enciphered by a given key letter, 0);, lies at the intersection of the vertical column headed by T, and the horizontal row begun by O. In this case Tp (0k) = He. The same result will be found on referring to sliding, direct standard alphabets.

b. Minor modications of the Vigenere Table are encountered. If the top line is made a reversed normal sequence, leaving the interior of the table unchanged, or if the successive horizontal rows are made to contain the reversed normal sequence, leaving the top row (plain text) unchanged, then the results given by using the table are the same as those given by using the obsolete cipher disk shown in gure 18. Again, the same general results can be obtained by using a set of alphabets in tabular form known under the names of Portas Table and Napoleons Table, which is Shown in gure 20.

AB	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
CD	A	B	C	D	E	F	G	H	I	J	K	L	M
	Z	N	O	P	Q	R	S	T	U	V	W	X	Y
EF	A	B	C	D	E	F	G	H	I	J	K	L	M
	Y	Z	N	O	P	Q	R	S	T	U	V	W	X
	etc.												
WX	A	B	C	D	E	F	G	H	I	J	K	L	M
	P	Q	R	S	T	U	V	W	X	Y	Z	N	O
YZ	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	P	Q	R	S	T	U	V	W	X	Y	Z	N

Figure 3.8: Figure 20

In this table the alphabets are all reciprocal, for example, G, $(W_k) = V_c$, V_p $(W_k) = G_c$. Reciprocal alphabets when arranged in this form are sometimes called complementary alphabets. Note that in each alphabet either of two letters may serve as key letter indifferent1y: G_p (W_k) or G_p $(X_k) = V_c$.

c. Another modication of the basic table, and one that employs numbers instead of letters as cipher equivalents is shown in gure 21. Since many more than 26 different equivalents are available (100 pairs of digits from 00 to 99, it is possible to insert many plaintext elements in the top line of the table in

*	a	b	c	d	e	f	g	h	i	*
a	10	11	12	13	14	15	16	17	18	a
b	11	12	13	14	15	16	17	18	19	b
c	12	13	14	15	16	17	18	19	20	c
d	13	14	15	16	17	18	19	20	21	d
e	14	15	16	17	18	19	20	21	22	e
f	15	16	17	18	19	20	21	22	23	f
g	16	17	18	19	20	21	22	23	24	g
h	17	18	19	20	21	22	23	24	25	h
i	18	19	20	21	22	23	24	25	26	i
j	19	20	21	22	23	24	25	26	27	j
k	20	21	22	23	24	25	26	27	28	k
l	21	22	23	24	25	26	27	28	29	l
m	22	23	24	25	26	27	28	29	30	m
n	23	24	25	26	27	28	29	30	31	n
o	24	25	26	27	28	29	30	31	32	n
p	25	26	27	28	29	30	31	32	33	p
q	26	27	28	29	30	31	32	33	34	q
r	27	28	29	30	31	32	33	34	35	r
s	28	29	30	31	32	33	34	35	36	s
t	29	30	31	32	33	34	35	36	37	t
u	30	31	32	33	34	35	36	37	38	u
v	31	32	33	34	35	36	37	38	39	v
w	32	33	34	35	36	37	38	39	40	w
x	33	34	35	36	37	38	39	40	41	x
y	34	35	36	37	38	39	40	41	42	y
z	35	36	37	38	39	40	41	42	43	z
*	a	b	c	d	e	f	g	h	i	*

*	j	k	l	m	n	o	p	q	r	*
a	19	20	21	22	23	24	25	26	27	a
b	20	21	22	23	24	25	26	27	28	b
c	21	22	23	24	25	26	27	28	29	c
d	22	23	24	25	26	27	28	29	30	d
e	23	24	25	26	27	28	29	30	31	e
f	24	25	26	27	28	29	30	31	32	f
g	25	26	27	28	29	30	31	32	33	g
h	26	27	28	29	30	31	32	33	34	h
i	27	28	29	30	31	32	33	34	35	i
j	28	29	30	31	32	33	34	35	36	j
k	29	30	31	32	33	34	35	36	37	k
l	30	31	32	33	34	35	36	37	38	l
m	31	32	33	34	35	36	37	38	39	m
n	32	33	34	35	36	37	38	39	40	n
o	33	34	35	36	37	38	39	40	41	o
p	34	35	36	37	38	39	40	41	42	p
q	35	36	37	38	39	40	41	42	43	q
r	36	37	38	39	40	41	42	43	44	r
s	37	38	39	40	41	42	43	44	45	s
t	38	39	40	41	42	43	44	45	10	t
u	39	40	41	42	43	44	45	10	11	u
v	40	41	42	43	44	45	10	11	12	v
w	41	42	43	44	45	10	11	12	13	w
x	42	43	44	45	10	11	12	13	14	x
y	43	44	45	10	11	12	13	14	15	y
z	44	45	10	11	12	13	14	15	16	z
*	j	k	l	m	n	o	p	q	r	*

*	s	t	u	v	w	x	y	z	*
a	28	29	30	31	32	33	34	35	a
b	29	30	31	32	33	34	35	36	b
c	30	31	32	33	34	35	36	37	c
d	31	32	33	34	35	36	37	38	d
e	32	33	34	35	36	37	38	39	e
f	33	34	35	36	37	38	39	40	f
g	34	35	36	37	38	39	40	41	g
h	35	36	37	38	39	40	41	42	h
i	36	37	38	39	40	41	42	43	i
j	37	38	39	40	41	42	43	44	j
k	38	39	40	41	42	43	44	45	k
l	39	40	41	42	43	44	45	10	l
m	40	41	42	43	44	45	10	11	m
n	41	42	43	44	45	10	11	12	n
o	42	43	44	45	10	11	12	13	o
p	43	44	45	10	11	12	13	14	p
q	44	45	10	11	12	13	14	15	q
r	45	10	11	12	13	14	15	16	r
s	10	11	12	13	14	15	16	17	s
t	11	12	13	14	15	16	17	18	t
u	12	13	14	15	16	17	18	19	u
v	13	14	15	16	17	18	19	20	v
w	14	15	16	17	18	19	20	21	w
x	15	16	17	18	19	20	21	22	x
y	16	17	18	19	20	21	22	23	y
z	17	18	19	20	21	22	23	24	z
*	s	t	u	v	w	x	y	z	*

*	0	1	2	3	4	5	6	7	8	9	*
a	36	37	38	39	40	41	42	43	44	45	a
b	37	38	39	40	41	42	43	44	45	10	b
c	38	39	40	41	42	43	44	45	10	11	c
d	39	40	41	42	43	44	45	10	11	12	d
e	40	41	42	43	44	45	10	11	12	13	e
f	41	42	43	44	45	10	11	12	13	14	f
g	42	43	44	45	10	11	12	13	14	15	g
h	43	44	45	10	11	12	13	14	15	16	h
i	44	45	10	11	12	13	14	15	16	17	i
j	45	10	11	12	13	14	15	16	17	18	j
k	10	11	12	13	14	15	16	17	18	19	k
l	11	12	13	14	15	16	17	18	19	20	l
m	12	13	14	15	16	17	18	19	20	21	m
n	13	14	15	16	17	18	19	20	21	22	n
o	14	15	16	17	18	19	20	21	22	23	o
p	15	16	17	18	19	20	21	22	23	24	p
q	16	17	18	19	20	21	22	23	24	25	q
r	17	18	19	20	21	22	23	24	25	26	r
s	18	19	20	21	22	23	24	25	26	27	s
t	19	20	21	22	23	24	25	26	27	28	t
u	20	21	22	23	24	25	26	27	28	29	u
v	21	22	23	24	25	26	27	28	29	30	v
w	22	23	24	25	26	27	28	29	30	31	w
x	23	24	25	26	27	28	29	30	31	32	x
y	24	25	26	27	28	29	30	31	32	33	y
z	25	26	27	28	29	30	31	32	33	34	z
*	0	1	2	3	4	5	6	7	8	9	*

Figure 3.9: Figure 21

addition to the 26 letters. For example, one could have the 10 digits; a few common double-letter combinations, such as DD, LL, RR, SS; a few of the most frequently used pairs of letters, such as TH, ER, IN, or even such common syllables as ENT, INC, and ION

63 Square Tables Employing Mixed Alphabets

a. In the tables thus far shown the alphabets have been direct or reversed standard sequences, but just as mixed sequences may be written upon sliding strips and revolving disks, so can mixed alphabets appear in tabular form. The table shown in gure 22, based upon the key word sequence derived from the word LEAVENWORTH, is an example that is equivalent to the use of a strip bearing the same key word sequence sliding against another strip bearing the normal alphabet.

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

Figure 22

The usual method of using such a table is the same as that in the preceding cases. The only difference is that the key letters must now be sught in a mixed

sequence, whereas in the preceding tables they were located in normal direct or reversed sequences. Example, using figure 22:

$C_p\ (S_k) = X_c$.

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

Figure 23

b. Figure 23 illustrates a case in which a mixed alphabet is sliding against itself. The usual method of employing such a table is exactly the same as that explained before. The only difference is that both the plaintext letters and the key letters must be looked for in mixed sequences. Example, using figure 23: $U_p\ (R_k) = V_c$.

c. It has been indicated that the basis of reference in most cryptographic operations involving key words is the letter A. In employing sliding alphabets it is usual to set the key letter as located in the cipher component opposite the letter A as located in the plain component. But, as shown in paragraphs 42!; and 60c, the key letter as located in the cipher component is usually set opposite the initial letter of the plain component. In all examples preceding that in gure 23, the key letter has been A. In gure 23, since the plain component is also a mixed sequence and its initial letter is Q, the sliding alphabets are set against

each other so that the given key letter in the cipher component is opposite Q in the plain component. Thus, to duplicate the results given by the use of gure 23 in nding the value of Up (R1,), it is necessary to set the sliding strips in the following relatiVe positions:

```
Plain: QUESTIONABLYCDFGHJKMNPRVWXZQUESTIONABLYCDEFGHJKM
Cipher:     QUESTIONABLYCDFGHJKMNPRVWXZ
```

Here it is seen that $U_p\ (R_k) = V_c$, which is identical with the, result obtained from the use of the table. There are other ways of using the table, however, each having a correspondingly modied method of employing sliding strips in order to obtain identical results.

VII OBSERVATIONS ON CIPHER SYSTEMS

64 More Complex Substitution Systems

a. The substitution systems discussed above are all based on relatively simple methods. They can all be solved rapidly. More complicated systems have been devised, however, and are used in certain situations. They are briey described in this section.

b. Virtually all systems based upon the principle of a repeating key can be solved because of certain cyclic or periodic phenomena, which the use of a repeating key exhibits externally or internally in the cryptograms. There are methods for preventing the external manifestation in the cryptograms of these phenomena, or their suppression and disguise if present internally. In some, the principle is to make the elements of a xed or invariable-length key apply to variable or irregular-length groupings of the plain text so that no cyclic phenomena are exhibited by the cryptograms. In others, the principle is to apply irregular lengths of the key, or a variable-length key to regular and xed groupings of the plain text, with the same object in view. In still other methods, both principles are combined, or the key itself is of such a nature that it does not repeat itself. This may be brought about by constructing or establishing a non-repeating key, or by employing the key in a special manner. Systems in which the successive letters of the cipher text or successive letters of the plain text after the initial letter serve as successive key-letters are also used with the object of avoiding or eliminating periodicity.

c. In the majority of the methods described the encipherment deals with single letters, and is therefore monagraphit: in nature. There are, however, certain methods in which encipherment is by pairs of letters, called digraphic substitution, or by sets of three letters, called trigraphic substitution. Polygraphic substitution methods, as they are mlled, have for their object the suppression, so far as possible, of the characteristic frequencies of individual letters, by means of which solution may be reached. The methods may employ extensive tables, small squares, rectangles, and other designs, or sets of sliding or rotating alphabets. The Playfair C ipher, which was for many years a standard eld cipher in

the British Army and was for a short time during World War I em ployed by the U. S. Army, is an example of digraphic substitution.

65 Combined Substitution-Transposifion Systems

In paragraph 10b, reference was made to the possibility of combining within a single system both transposition and substitution methods; that is, of rst enciphering by a method of one type and then taking the re- sulting cipher text and passing it through an encipherment of the other type. The usual order is rst to substitute and then to transpose, but the reverse of this order of procedure is also possible. In some methods, quite complex, there may be a rst substitution, then a transposition, and nally a substitution again. Despite the fact that three steps are in- volved, certain of these systems may be practical for military use under special conditions where speed is not as important as security. These cannot be described in this manual.

66 Cipher Devices and Cipher Machines

a. Only a little practical experience with any of the methods described is necessary to convince one that on the 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 traffiic they leave much to be desired. Consequently, cryptographers, both experienced and inexperienced, have been led to attempt to devise ap- paratus which will not only facilitate cryptographing and decryptographing, but will also increase the degree of cryptographic security. Small instruments constructed for this purpose, operated by hand, are called cipher devices. Scores of them have been devised, but only a few are sufciently practicable for eld use, and still fewer are of such construction that they produce cryptograms of unusual security. Among the better examples of such cryptographs is one which was for some years (192242) employed in the U. S. Army under the name of Ciphef Device, Type M94. Modern security requirements made such a device obsolete, however, and it has been replaced by a better one, the Converter M-209 ( ) (TM 11380).

b. There are larger cryptographic machines which are much more nearly automatic in nature 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 results of the enciphering or deciphering operations. 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 modied printing telegraph machine, or else it consists of an auxiliary piece of apparatus used in conjunction with the teleprinter. Such apparatus can obviously be practicably employed only among the larger headquarters where trafc is suiciently heavy to warrant its use.

67 Disadvantages and Limitations of Cipher Systems

Except for certain electrically operated cipher machines equipped with a typewriter keyboard, most cryptographic methods using manual" or pencil and paper cipher systems are unsatisfactory for military pur poses. Practically all such systems can be solved by enemy cryptanalysts, and those suitable for use in the theater of operations offer fewer ob stacles to solution than systems suitable for use in the rear areas. Cipher systems are not economical in time units required in electrical transmis- sion; the best that they can do is to produce cryptograms no longer than the original plain text. For use within small tactical units in the forward areas there are other cryptographic methods which offer advantages of speed, simplicity, and brevity and which, properly used, afford suicient cryptographic security. These are often preferred over cipher methods in the forward echelons of the combat zone. These methods involve the use of lists of groups of letters or gures to which arbitrary meanings have been assigned. They are called eld codes, prearranged-message codes, brevity codes, voice codes, jargon codes, etc. Codes will be discussed in the succeeding sections of this manual.

Chapter 4

ELEMENTARY CODE SYSTEMS

I GENERAL

68 Difference Between Code and Cipher Systems as Methods of Cryptography

A code system is a more or less highly specialized form of substitution. The basic principle underlying substitution cipher systems is the replacement of the individual letter in the plain text of a message by other letters, gures, or symbols. Occasionally the replacement or substitution process is applied to groups of letters, and when this is done the groups are usually of denite, or regular length. In cipher systems the units with which the cryptographic treatment deals are the smallest of which plain text can be composed. The basic principle underlying code systems, however, is the replacement of entire words, long phrases, or complete sentences constituting the plain text of a message by arbitrarily selected equivalents having little or no relation to the elements they replace. These equivalents may be other words, groups of letters, groups of gures, or combinations. It is only exceptionally that the replacement or substitution process is applied to elements smaller than whole words, and when this is done the elements are single letters, groups of letters, or syllables. In code systems the units with which the cryptographic treatment deals are aggregates of smaller unitsindividual letters combined in various groups of irregular length; that is, words, phrases, sentences.

69 Code Books and Codes

a. If it were possible to memorize a long list of words, phrases, and sentences, together with the arbitrary equivalents called code groups as- signed to represent them, there would be no need of having written or Printed code books. In a code

book, the words, phrases, and sentences are listed in a systematic manner and accompanied by their code equiv alents. Correspondents must possess identical copies of the document in order to communicate with one another. An ordinary dictionary may, and Often does serve the purpose of code communication, so far as single words are concerned, but as a rule a specially prepared document con taining the words, phrases, and sentences, suited to particular types of correspondence, is used. Such documents are called, in the United States and in Great Britain, *code books* or, simply, *codes*. In other countries they are called *repertories*, *word books*, *cipher dictionaries*, *enciphering and deciphering tables*, etc., although the term code" is becoming prevalent throughout the world.

b. There are various types of codes each suited to particular types of corresp0ndence. Some are large books used for general business or social correspondence; others are intended for particular industriesfor example, rubber, sugar, steel, and automobileand contain highly specialized technical vocabularies. Most large commercial rms have their own private codes, constructed especially for their use. This manual however, is concerned only with codes suitable for military communication. While the resemblances between the ordinary commercial codes and the usual military codes are marked, their primary purposes are different. Code is used in commercial communications principally to effect economy in cost of communicating, secrecy being of secondary importance. In modern military signal communications code is used to effect secrecy, brevity, and speed, especially in frontline signal communications. However, in lengthy administrative messages, the economy afforded by a properly constructed code is important.

70 Brevity Afforded by Code Systems

a. Messages cryptographed by means of a code book are secure only when the code book is kept secret. There are, however, code systems in which secrecy is not a factor. Such systems are intended for brevity or, in transmission by commercial telegraph, for economy. Code books afford a means for abbreviating or condensing the writing necessary to convey information. A single, comparatively short group of code characters may represent a whole word of as many as 15 or more letters, a long phrase, or a complete sentence. Thus, as a rule, the text of a code message is much shorter than the plain text, and therefore costs less to send. Naturally, the condensing power of a code book varies with the extensiveness of its vocabulary, since in a small book there can be listed only the most common words and only a few phrases and sentences; whereas, in a large book practically all the words likely to be used in telegraphic communication, and many common phrases and sentences may be included. When a code book is used to condense text only for purposes of economy, it is called a nonsecret code. Examples of such codes are the ordinary commercial codes sold in book stores. A code book may combine the features of economy and secrecy, in which case the book itself must be safeguarded from the enemy as a secret code.

b. In addition to money saving, code systems save time and labor in transmission and reception, as the number of characters handled in code systems

is smaller than in cipher systems. The saving of time is an important factor in front line communications where speed is essential and sometimes outweighs security considerations.

c. In military cryptography, the greatest degree of condensation is a'orded by prearrangedmessage codes, brevity codes," and the like. A prearranged-message code is a tactical code adapted to the use of units requiring special or technical vocabularies; it is composed almost exclusively of groups representing complete or nearly complete messages and is intended for shortening messages and concealing their content. A brevity code has for its sole purpose the shortening of messages. A eld code is primarily a small tactical code which contains a large number of code groups representing words and a few common short phrases, from which sentences can be composed; a syllabary, which is a list of code groups representing individual letters, combinations of letters, or syllables, is usually provided for spelling out words or proper names, not present in the vocabulary; numerical tables, or lists of code groups representing numbers, dates, and amounts, are also included. A jargon code is another name for a simple, very short code in which bona de dictionary words, baptismal names of persons, the names of rivers, lakes, etc., are used as code groups. A voice code is used for transmission by the small radio-telephone sets used in combat areas and may be a prearranged-message code, a brevity code, or a jargon code. Other names used to designate such codes are combat code, and operations code.

71 Operation of Encoding and Decoding

These two terms apply to the cryptographing and decryptographing respectively, of messages by means of a code. In encoding a message, a code clerk merely replaces the various words, phrases, sentences, and numbers of plain text by their code equivalents. The code text is built up from code units each representing the longest possible plain-text unit the code book affords. For example, if the sentence ENEMY FORCE ESTIMATED AT ONE BATTALION EN COUNTERED ONE MILE SOUTH-EAST OF ROCK CREEK CHURCH is to be encoded, and the code book lists the phrase ENEMY FORCE ESTI MATED AT, the code group representing this phrase would be used rather than separate code groups representing the individual words ENEMY, FORCE, ESTIMATED, and AT, all of which might also be present in the code. The process of decoding is the reverse of that of encoding. Each code group is looked up in the code book, its meaning found and written down. Where the errors in transmission are few, the process is rapid; but even a small number of errors in a message may obscure the meaning or render a message unintelligible.

II CODE GROUPS

72 Composition of Code Groups

a. The elements of which code groups are composed may be of one or more of the following types:

(1). Bona de wordsreal words taken from the dictionaries of one or more languages. The usual languages employed as sources for code words of this type are Dutch, English, French, German, Italian, Latin, Portuguese, and Spanish.

(2). Articial wordsgroups of letters having no real meaning, constructed more or less systematically by arrangements of vowels and consonants so as to give these groupings the appearance and pronounceability of bona de words.

(3). Groups of letters presenting no appearance of bona de or articial words and resembling cipher groups.

(4). Groups of arabic gures.

b. For special purposes, code groups composed of intermixtures of letters and gures within groups may be used. Call signs for radio stations, such as WZKA and WSAZZ, are examples of such intermixtures often used in radio callsign codes. In certain highly specialized naval or military codes, the intermixture of letters and gures is sometimes necessary. Such intermixtures, however, are either not accepted or, if accepted, are charged for at a greatly increased rate when they appear in messages transmitted by commercial communications agencies.

c. A code may contain two or more parallel sets of code groups of different types. For example, in many commercial codes and in some military and naval codes, there is one series of code groups of the bona de or articial word type and another series of the gure-group type, both applying to the same series of words, phrases, and sentences of the code. There are several reasons for this. In most parts of the world where italic or roman letters are used for writing, letters possess greater advantages in accuracy of reading and handling by telegraph personnel. This is necessary for correct transmission and reception of messages. How- ever, in some parts of the worldfor example, Turkey, Russia, China telegraph personnel, except in the large cities, are unfamiliar with the English alphabet and hence many errors in transmission arise. But arabic digits are almost universally recognized and used, so that for communications between obscure ports and small cities in foreign countries, gure groups are preferred over letter groups. There are certain methods of condensing code groups composed of gures into still smaller groups Composed of letters by means of condensers, so that many rms use gure groups for such purposes in expensive transmissions. Finally, in certain methods of enciphering code messages for the sake of greater secrecy, gure groups often form the basis for the encipherment more readily than do letter groups.

d. Prior to 1 January 1934, in practically all modern codes constructed by experts, letter code groups were of the articialword type. On that date new rules in international communication became effective,[1] permitting the use of letter code groups without restriction in their formation, as class (3) in a above. It is probable that almost all of the codes published subsequently to the above date will contain letter code groups of the unrestricted type.[2]

e. The greatest advantage possessed by letter groups over gure groups lies in the availability of a far greater number of permutations, or inter- changes, of letter groups, because there are 26 letters which may be permuted to form letter code groups, whereas there are only 10 digits which may be permuted to form gure groups. If code groups of ve elements are used, then there are available 26", or 11,881,376 groups of ve letters, and only 105, or 100,000 groups of ve gures. Now since the number of permutations of 26 letters taken in groups of ve is so great, only permutations conforming to special types may be selected for use, and there will still remain a sufcient number of code groups for even the largest codes. Certain types of code groups are selected so that possible error in telegraphic transmission can be reduced to a minimum. If the code groups have been constructed scientically it is possible to correct such errors quickly without having the message repeated.

73 Length of Code Groups

The length of code groups used, whether the groups consist of two, three, four, or ve elements, depends upon the size of the code. This applies almost exclusively to eld military or naval codes, where trans- mission is through a governmental agency; in commercial messages or in governmental communications transmitted over privately-operated lines, veletter or vegure groups are used almost exclusively because of the regulations adopted by the International Telegraph Conferences and by commercial telegraph and cable companies. As a general rule in the transmission of code and cipher messages, each group of ve letters is counted as one word regardless of the number and arrangement of vowels; each group of ve gures is counted as one word.

74 Permutation Tables of Two-Letter Differential

a. Code groups of modern codes are constructed by use of tables which permit more or less automatic and systematic construction in the form desired. These are called permutation tables. Because they may be used to correct most errors made in transmission or writing, such tables are usually included in the code book and are called *mutilation tables*, *garble tables*, error-detector charts, *etc.* Before the invention of permutation tables, code as a system of communication

[1] See Telegraph Regulations, International Telecommunication Convention, Madrid, 1932.

[2] For a treatise on the development of codes see "The History of Codes and Code Language, the International Telegraph Regulations pertaining thereto, and the bearing of this history on the Cortina Report," by Major William F. Friedman, Sig.-Res., Government Printing Oice, 1928.

was not wholly reliable. Scientically constructed tables, however, include a feature (see b below) which has remedied this fault to a great extent.

b. To make an error in a group of ve letters is not unusual on the part of the average telegraph or radio operator. If a difference of only one letter distinguishes one code group from another in the same code, as ABABA and ABABE, then serious errors may be introduced in the meaning of a message, or the message may be made unintelligible by only a few transmission errors. If, however, every code group in the code book is distinguished from all other code groups in the same code by a difference of at least two letters, then there would have to be two errors in a single group and these two errors would have to produce a code group actually present in the code before a wrong meaning would be conveyed. This principle of making code groups within the same code differ from each other by a minimum of two letters is called the *two letter differential*. It is most easily incorporated in code groups by constructing the permutation table to this end. The differential may be the absolute difference in the identities of two letters or the relative positions occupied by them. For example, BACOF, and BACUG differ from each other in the identities of the nal pair of letters; considered as a combination of letters, the two groups present a twoletter difference. The two groups BACOF and BOCAF, however, differ in the relative positions occupied by two of their letters, but considered as a permutation of letters, these two groups as well as the two groups BACOF and BACUG, present a twoletter difference. In short, when at least two corresponding letters in a pair of code groups differ in their identities, the two code groups are said to present a 2letter difference. Errors arising from the exchange of position of two letters, without a change in their identities, are referred to as errors of transposition. They are not unusual but fortunately, as a rule, they involve only letters which are either adjacent or alternate. For example, in the pair of groups BACOF and BOCAF there is a transposition of the alternateletter type. In recent codes, attempts have been made to devise permutation tables which will eliminate one of the two members of every pair of groups which differ from each other by the mere transposition of two adjacent or alternate letters. Codes using groups based upon a permutation table will show the table and exPlain how to use it in correcting the usual mutilations of groups.

c. The use of the two-letter differential reduces the possibilities for constructing letter-code groups from 26^5 (11,881,376) to 26^4 (456,976), but, considering the advantages, the sacrice is worthwhile.

d. Permutation tables for the construction of gure-code groups are similar in nature and purpose to tables for the construction of lettercode groups. However, because of the more limited number of characters available for permutations, the maximum number of 2-gure difference groups possible in a 5-gure code is 10^4, or 10,000.

III ONE-PART AND TWO-PART CODES

75 Arrangement of Contents of Codes

a. In their construction or arrangement, codes are generally of two types:

(1). *One-part*, or alphabetical codes. The plain-text groups are arranged in alphabetical order accompanied by their code groups in alphabetical or numerical order. Such a code serves for decoding as well as for encoding.

(2). Two-part, or randomized codes. The plain-text groups are arranged in alphabetical order accompanied by their code groups in a nonalphabetical order. The code groups are assigned to the plain-text groups at random by drawing the code groups out of a box in which they have been thoroughly mixed, or by some other manner in which the element of chance operates. Such a list can serve only for encoding. For decoding, another list must be provided in which the code groups are arranged in alphabetical or numerical order and are accompanied by their meanings as given in the encoding section. For this reason a two-part code is often called a *cross-reference code*. The following brief extracts from typical onepart and two-part codes illustrate the difference between them:

One-part code.	
ABABD	A
ABACF	Abaft
ABAHK	Abandon
ABAJL	. . . . it
ABALN	Abandoned
ABAMP	. . . . by
ABAWZ	Abandoning
ABBAD	Abandonment
----------	----------
----------	----------
ZYZYZ	Zero

Two-part code.			
Encoding Section		Decoding Section	
GAJVY	A	ABABD	Obstructed
TOGTY	Abaft	ABACF	Term
FEHIL	Abandon	ABAHK	Zero
BAYLT	. . . . it	ABAJL	If it has not
ZYZYZ	Abandoned	ABALN	To be sent by
NYSYZ	. . . . by	ABAMP	Acceding
IFWUZ	Abandoning	ABAWZ	Building
RUMGO	Abandonment	ABBAD	Do not attempt
----------	----------	----------	----------
----------	----------	----------	----------
ABAHK	Zero	ZYZYZ	Abandoned

b. Between the two extremes are codes which have features of both; that is, complete sections may be arranged in random sequence, but within each section the contents are arranged in some systematic or logical order. This is true, however, only of some of the older codes. In modern types, the two-part construction is more common.

c. When a strict alphabetical arrangement is used in the sequence of the phrases, the code is said to be a strictly alphabetical code; when the phrases are listed under separate headings based upon the principal word or idea in the whole expression, the code is said to be a caption code. The following extracts will serve to illustrate the two types:

Caption code	*Strictly alphabetical*
Assistance	Assistance
Give *assistance*	Assistance for
Require *assistance*	Assistance from
No *assistance* required	Assistance has been sent
Assistance has been sent	Assistance to
Assistance for	Assistant
Assistance from	Assisted
Assistance to	.....
Assistant	Give
Assisted	Give assistance
etc.	.....
	No
	No assistance required
	.....
	Require
	Require assistance

d. More precise and economical encoding is possible with a caption code than with an alphabetical code. With the caption code it is easier to assemble an extended variety of expressions and shades of meaning under specic headings than with the alphabetical code. On the other hand, the use of a caption code involves more time and labor in encoding, especially by untrained or unskilled personnel, than the use of an alpha- betical code. Where the phraseology of communication is standardized or stereotypic, the most common expressions may be listed in an alphabetical code as readily as in a caption code. In both types of codes there may be tabulated material, such as tables of numbers, dates, equipment, geographical or personal designations, either fomiing isolated sections in the code or inserted in the vocabulary under appropriate headings.

e. Two-part codes are used by many governments for their secret diplomatic, military, and naval communications because the advantages they offer over one-part codes are greater than their disadvantages. The disadvantages are: a two-part code is harder to handle than a onepart code because it is at least twice as large in content, since each code group and each plaintext element must appear twice; the cost of printing is approximately double; the amount of labor in compiling a two-part code is nearly four times greater because of the necessity for preparing the accurate crossreference arrangement which is its basic principle.

76 Purposes of Two-Part Type of Code

a. The two-part code is a comparatively recent development in code systems. Its purposes are greater secrecy, and greater accuracy.

b. In a one-part code the plain-text groups progress from A to Z in a regu-

lar alphabetical sequence, accompanied by their code groups, also in a regular alphabetical or numerical sequence. If the word ABAFT is represented by a code group whose initial letter is A, or whose initial number is 1, then the word ABANDON will be represented by a group whose initial letter is also A, or whose initial number is also 1. In other words, the enemy cryptanalysts have denite clues to follow in breaking down the code because of the parallelism of the two sequences; the determination of the value of one code group affords denite clues to the value of many other code groups. In a twopart code, however, the word ABAFT might be represented by a group whose initial letter is T, or whose initial number is 8, and the word ABANDON might be repre- sented by a code group whose initial letter is F, or whose initial number is 3. In other words, the two sequences are not alike in progression; hence the determination of the value of one code group will give no clues to the value of any other group.

c. In considering the greater accuracy of. a two-part code over a one- part code, the following pair of phrases (in a hypothetical one-part code) are given as an example:

```
WOVAM Will be ready to attack
WOVEN Will not be ready to attack
```

Such an arrangement is subject to two sources of error. A code clerk working under great difculties, in a hurry, may accidentally write down WOVAM instead of WOVEN as a result of the contiguity of the two sets of letters which are similar in appearance and are so close together on the page that his eye may take the group from the wrong line. Again, on account of the similarity in sound, his ear may deceive him into writing WOVEN when he should have written WOVAM. Now the meaning of the one group is the exact opposite of the meaning of the other and, since either meaning may t in correctly with the context of the message, the error may remain undiscovered for some time, thus causing serious inconvenience or, in the case of combat, actual loss of life. Furthermore, although the making of two errors in a single group is rather unusual in transmission or reception, yet it does happen and, in such a case as the above, would not be detected. This is especially true in connection with tabular material such as lists of numbers, dates, and names, in which the context often fails to yield clues to the correction of garbles or errors, or to give conclusive evidence of the presence of an error. But in a two-part code such errors are improbable. In the rst source of error mentioned above, the code clerk would be very much less likely to confuse two entirely different groups of letters; in the second source, if two errors are made in the transmission or reception, and if these errors involve two letters producing a group which actually has a meaning in the code, this meaning is so unlikely to t in correctly with the context that its probability of occurrence may be negligible. Thus, if this sort of error does happen, the meaning of the group fails to t in with the context and at once indicates an error. Knowledge of such an error, even if it is impossible to correct it, is more preferable than ignorance of its existence, with a possible action based upon incorrect decodement.

IV ENCIPHERED CODE

77 Purposes of Enciphered Code

a. Sometimes the code groups of a code message undergo a further process of encipherment. The resulting cryptogram constitutes an enciphered code message.

b. It is desirable to use enciphered code in two instances:

(1). When the basic code has had wide distribution and the message might fall into unauthorized hands. Commercial codes sold in bookstores, and even special codes distributed widely throughout governmental ofces, illustrate the type of code to which this added safety factor should be applied.

(2). When increased security is necessary for highly classied communications. Although the basic code book may already be secret, further encipherment would greatly delay the solution of the code if it fell into the hands of enemy cryptanalysts.

c. It has already been stated that code messages may be solved by cryptanalytic principles without possession of the code. The length of time required for the process varies widely, and is dependent upon the conditions under which the work is done (see ch. 1). To increase the length of time required for solution, as in secret codes, the code text of the messages resulting from the use of the code is passed through a cipher process so that the messages will be in different keys, thus delaying the assembling and study of data, which is necessary to the solution.

78 Types of Encipherment

a. Both of the two general classes of cipher methods, transposition and substitution, may be used in enciphering code. The increased degree of secrecy because of encipherment depends entirely upon the nature of the system applied.

b. Transposition systems involving a rearrangement of complete groups may be employed where the degree of increased security does act have to be of a high order, and where the original form of the groups must be retained even after encipherment. Transposition systems in which the order of the letters within groups is changed may also be employed. For example, a numerical key may indicate the transposed order of the letters of the code groups, so that a group such as XDFGY will become DFYXG.

c. Substitution systems of many sorts may be employed, ranging from simple monoalphabetic to the most complex types of substitution with cipher machinery. Tables of alphabets are often used. In some systems, a simple transposition process may be combined with a simple substitu tion process.

d. A favorite method in onepart codes having both letter-code and gure-code groups is that in which the letter-code group standing at a prearranged interval before or after the lettercode group representing the actual word or

phrase intended to be conveyed is substituted. The interval may remain xed within a single message, or it may vary according to some predetermined key. Numerical code groups make the use of large intervals practicable.

e. In modern practice, the most common methods of enciphering gure-code groups are those using addition or subtraction, with a key book containing arbitrary groups of gures. When such methods are properly used, they yield a high degree of security. The highest degree of security is attained when such a key book is used *only once*.

Chapter 5

COMPARISON OF CODE AND CIPHER SYSTEMS

79 Advantages and Disadvantages of Each Type of System

a. From the viewpoint of purely military cryptography, a comparison of the advantages and disadvantages of each method can be made only between systems suitable for each of the following three general categories:

(1). Highsecurity, or highgrade, systems for cryptographic intercommunication among the largest military units and the highest echelons of command.

(2). Medium-security, or mediumgrade, systems for crypto- graphic intercommunication among the intermediate units and echelons of command.

(3). Low-security, or low-grade, systems for cryptographic inter- communication among the small units and the lowest echelons of command.

b. The principal factors to be taken into account in comparing code and cipher methods in cryptographic communication are reliability, security, rapidity, exibility, and economy.

(1). *Reliability.* Reliable cipher machines made possible by modern engineering and cryptographic techniques satisfy all or a majority of these factors to a great degree, and such machines are now used in the U. S. Army for these highgrade systems. Although the machines are complex, their reliability can be assured by having properly trained personnel to operate and maintain them. Accuracy is also one of the elements of reliability and a good cipher machine can yield a higher degree of accuracy or completeness of text in cryptographic communi- cation than can a code system. A mistake in one or two code groups may obscure, alter, or render unintelligible the meaning of a whole message, but in cipher systems, often wrong letters may be corrected, or missing letters may be supplied, by the context. It must be remembered, however, that in some cipher systems a single error

of a fundamental type, such as using the wrong key or the wrong setting, may prevent the deciphering of the message.

(2). *Security.* If reliability were the only or the most important factor, code would be preferable to cipher for all echelons of command, because the simplicity of a code book is to be preferred to the complexity of a large cipher machine. But unen- ciphered code is not sufciently secure for the communications of the highest echelons and headquarters. If encipherment must be added as a second step in the cryptographic process, it practically destroys the simplicity features of a code system; unless the enciphering method is fairly complex, it adds little security. In a properly designed cipher machine, embodying sound cryptographic principles based upon a thorough knowl- edge of cryptanalytic principles, the singlestep-encipherment process can yield cryptograms of very great security. In a good code system, however, the solution of one or even of several messages does not entail the immediate breakdown of the entire system, with the consequent ability to read all messages, as is usually the case in a cipher system.[1] Codebooks, of course, can be rendered useless by compromise. Actual possession for a long period of time is not necessary; methods of rapid photography may be applied and a book of several hundred pages copied in a few minutes.

(3). *Rapidity.* The speed with which a cipher n-iachine equipped with a typewriter keyboard can be operated leaves even simple, unenciphered code far behind in the matter of rapidity. Flexibility. Complete exibility would permit cryptographing the originators own language without change necessitated by the limitations that exist in all but the most extensive codebooks. Thus, a cipher machine is much more exible than a code and can be used for all sorts of messages; whereas, in a code containing words, phrases, and sentences prepared for a specic type of communication, rewording the original text as written by the originator is often necessary, if the words, phrases, and sentences in the codebook are to be used; otherwise the original wording must be encoded word by word, or even syllable by syllable.

(4). *Economy.* Whether expressed in terms of money or manpower, cipher systems are more economical than code systems for high-echelon communications. Code text is usually shorter than the equivalent plain text, because

[1] A good cipher system may be compared to a library housed in a large structure of many rooms with all doors and all windows securely locked. If an intruder can force an entry into the structure, he will nd a master key which will open all the locks and give him access to all the books in the library. A good code system (especially a two-part code) may be compared to a library housed in a similar structure, but no two locks are alike and no master key is available or can be made. Therefore, the lock on each door must be worked at patiently as a separate problem. Thus, although the intruder may force his way into one room, this gives him access to only a small part of the library; in order to read all the books, he must force his way into each room, which takes much time, since each lock presents a separate and special problem.

it is condensed or abbreviated, but a single clerk operating a rapid cipher machine can turn out 10 to 15 times as much work as one operating a code system; furthermore, codes must be prepared, printed, and distributed. These steps take much time and labor and are often performed under considerable difculty. A continuously operative code compilation section must be maintained to replace codes as fast as they become compromised by continued use, or by capture. The handling of the manuscript and proofs in printing entails the necessity of ever watchful secrecy; and nally, the prompt and thorough distribution of codes to all who must use them is sometimes very difcult, especially where the distribution must be made over an extensive territory. Therefore, for highechelon cryptographing communications, ciphers are more economical than codes, but the economy factor is least important.

c. It is clear that high-grade systems should include all or as many as possible of the ve factors listed in b above; moreover, the advantages afforded by good cipher machines make cipher systems more desirable than code systems for the high-grade cryptographic systems required by high-echelon cryptographic intercommunication. In addition, secondary or backup" systems must be provided so that in case of machine or power failure, there will be available some means for cryptographic communication. Finally, emergency systems must be provided for crypto graphic communication when neither apparatus nor codebooks can be employed.

d. Medium-grade cryptographic systems for intercommunication among intermediate echelon commands must meet almost the same severe requirements as systems for intercommunication among highechelon commands. Here again, cipher machines are preferable to code. The machines may not be so large or complex, but if the same basic crypto graphic system is employed by both the highgrade and the mediumgrade machine, many advantages are noted. The problems of manufacture, maintenance, instruction of personnel in the operation of the system, distribution of keying data, etc., are simpler if they are basically the same for both types of machines. Moreover, it is possible for a message from an intermediate command to be deciphered by a highechelon com- mand, and vice versa, without using a second cryptographic system. For these reasons, cipher machines are widely used in the U. S. Army for medium-grade cryptographic communication and, in addition, certain manual systems requiring simple types of apparatus are also used. These may serve also as the secondary or backup systems required for the high-echelon cryptographic communications.

e.

(1). Even in the socalled low-grade systems, cipher machines are serving the purposes for which eld codes were formerly sup plied. Converter M209( ) is a small, mechanical cipher machine widely used in the U. S. Army for communications within the small combat units. If properly used, it yields crypto- grams of considerable security. It is a complicated device; it has no keyboard, and is slow in operation. Despite its reduced size and weight, this device is not convenient for use in frontline areas, nor is it suitable

for use in voice communication by small radiotelephone equipments such as the walkytalky or "handy-talky sets.

(2). Manual or hand-operated cipher systems are also unsuitable for such purposes. The processes of enciphering and deciphering by means of such systems require very close mental attention to avoid errors; the more secure methods are hopelessly slow and the faster ones are not secure, in comparison with the security that a small, frequently-changed two-part code yields.

(3). Practical experience indicates that in messages of very small tactical units, in certain types of air-to-air or air-toground communications, and in certain forms of messages where the subject matter is highly stereotypic, as in weather reports and re-control observations, code is often preferred over cipher. In all these cases, speed must give way to security; size and weight of equipment are important factors; simplicity of operation undcr battle conditions is vital, which eliminates methods requiring much training and concentrated attention. Also, if code is properly prepared, one or two code groups may express a command or a report that would require many groups of cipher text. Small codes meet the requirements in all these respects, and for this reason, code is still used to some extent in the U. S. Army, especially in the forward areas.

80 Fundamental Assumption of Military Cryptography

It has been seen that every good cryptographic system combines two more or less separate .and distinct elements: a basic or unchangeable method or process, which is termed the general system; and a specic or variable factor which controls the steps under the general system and is termed the specic key. The secrecy of any military cryptographic system must be entirely dependent upon the specic key because it must be assumed that the enemy is in full possession of all the details concerning the general system. This assumption is warranted by the whole history of military cryptography and is based upon the two following considerations which all experienced cryptanalysts regard as valid. In the rst place, in military cryptography there are more prolic sources from which to obtain information concerning cryptographic methods than there are in the isolated methods used by private individuals. In fact, by one means or another, the enemy can sooner or later come into possession of full information regarding the general cryptographic system. In the second place, within a very short time the number of messages available for study becomes so great, and the inevitable blunders in the handling of communications have become so numerous that a solution by detailed study can always be made by the enemy, with a consequent disclosure of the general system. If a cryptographic system adopted for military use were such that messages in that system could be solved easily without the specic keys applicable to the messages once the underlying methods became known, the entire system would have to be changed, a new system devised, and thousands of persons in the military service trained in its operation. This, of

course, would be impracticable. It is assumed that the enemy has knowledge of the general cryptographic system, its cipher devices, instruments, or machines. Only cryptographic documents which are given a limited distribution can be kept secret from the enemy, but they can be kept secret only for a variable length of time before they must be changed. These changes, as a rule, do not affect their method of usage. In cipher sytems, the specic key must be susceptible of easy and rapid changes by prearrangement between correspondents. In systems for use by secret agents or very small military parties in the theater of operations, the key may be an easily remembered word, phrase, sentence, or number; it must not require the carrying of written notes on the person. In systems for use by commanders of large and intermediate or even small headquarters in the theater of operations, the specic key may be in the form of written memoranda, paper tapes, and the like. Generally, the specic key must be the same throughout a given period of time for all the members of an intercommunicating network, or at least only a very limited number of specic keys must be in simultaneous effect; otherwise confusion and delay are inevitable. As a consequence of this requirement, the enemy may intercept a good many messages all in the same specic key. A cryptographic system for military use must conform to all requirements of practicability set forth in section IV, chapter 1, and to the foregoing section concerning the specic key; this system must be such that it is practically impossible for the enemy to solve any message quickly enough to make the information obtained of real or immediate value in the tactical situation, even though he is in full knowledge of the general method of the system, possesses the cipher device or apparatus, if used, and may have available for study 1,000 or more cryptograms sent on the same day. There is no single cryptographic system yet known which fully meets all these requirements, and in order to provide the necessary degree of security for a large army several different types of ciphers and cipher machines, as well as small codes for front line use, must be employed simultaneously.

Chapter 6

CORRECTION OF ERRORS

81 Sources of Error in Cryptography

Errors, mutilations, and garbles are some of the names applied to the inaccuracies that occur in cryptographic communication. They are so common and so troublesome that commanders who, for the most part, already regard cryptographic processes as hopelessly slow and cumbersome, often become much prejudiced against their use in active opera- tions. Therefore, instruction in the correction of errors is an essential part of the training of personnel assigned to cryptographic work. Train ing and experience will reduce the time necessary to correct the most common types of errors, which may be traced to the following sources:

a Cryptographing and decryptographing, including the simple process of copying by hand or by typewriter.

b Transmission and reception by all means of signal communication other than those in which the cryptograms are physically carried from origin to destination.

82 Practical Suggestions for Eliminating Errors

a. Errors in cryptographing and decryptographing can be much reduced though not wholly eliminated, by systematizing the work so far as possible and invariably checking it. Great care must be exercised in the formation of letters in writing, and roman capitals should always be used. If copied messages are checked for correctness by two operators, one reading the letters to the other, a phonetic alphabet must be used in order to prevent misunderstandings. In forward areas it is impossible to provide suitable or convenient quarters for personnel engaged in cryptographic work, but in rear areas and at the larger headquarters this per- sonnel will work much more efciently in a quiet, well ventilated ofce. To

check the accuracy of cryptographic work it is always advisable, when possible, that an operator other than the original cryptographic clerk decryptograph the message. In checking his own work, an operator should actually decryptograph itnot merely check his cryptographingbecause it is a psychological fact that persons have a tendency to repeat an error unconsciously. The most serious errors in cryptographic work leading to difculties and delays in decryptographing are not the mere mistakes in the writing down of letters, but are errors of a fundamental nature which the operator says, when it comes back to him, I dont see how I could have made it. Checking by actually decryptographing will usually elimi- nate such errors. At the destination, the nal copy of a decryptographed message should invariably be checked against the original work sheets before being turned over to the addressee, and again preferably, by another operator. It is easy to omit the word NOT from a decoded message and to fail to note the omission, if the same operator merely reads over the decryptographed message. Here, again, psychological factors are involved, and clerks who are disposed to transpose letters and words, an unconscious habit of a peculiar psychological origin, must be especially careful in their work.

b. Carelessness in the writing of system and message indicators, or failure to insert them in their proper places in the message, will usually make prompt decryptographing of the received message difcult or impossible. They should be written with the greatest of care.

c. If an incoming message is partially or wholly unreadable, an attempt should be made to nd the error in the faulty message. Often a message can be decryptographed by a simple expedient such as applying the key for the day preceding or following and correct date, or applying the daily key for a classication higher or lower and the correct classication. If, however, the garbled text still resists all efforts of correction, a procedure (service) message should be sent. The length of time one should con- tinue with the attempt to break the faulty message before sending a service will depend upon the classication and precedence of the message, transmission problems involved, time required to complete service, etc.

d. The procedure in preparing and handling service messages dealing with errors in cryptographic messages is quite involved, in order not to compromise the cryptographic system or give clues as to the contents of the faulty message. Instructions covering the procedure to be followed in such Servicing are issued from time to time and should be carefully followed.

e. The most important precaution to be observed, in order to avoid the transmission-of messages which cannot be promptly decryptographed at the receiving end, is the rigid adherence to all instructions set forth in documents describing the cryptographic operations to be followed. Misunderstanding or ambiguity is rarely found in properly prepared docu- ments detailing cryptographic operations, and a careful study and observance of the instructions will result in the preparation of messages without fundamental errors.

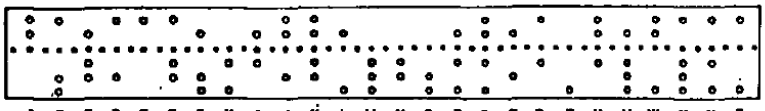
f. To be efficient in cryptographic work requires, in addition to the usual qualities -of carefulness, accuracy, and attention to detail, the possession of certain psychological characteristics peculiar to the work. If absent, these char-

acteristics as a rule cannot be developed, but if present they can be intensied and made more efcient by constant practice and experience. It is therefore advisable to select personnel for cryptographic work as for any other specialized work, to train them carefully, and retain them as long as possible; the longer they remain in this work the less likely they are to repeat the errors with which the work abounds and :the more likely they are to render highly efcient service.

g. Errors in transmission and reception are frequently made, especially in transmission by radio, because of interference, atmospheric disturb:ances, and the like. Cryptographic clerks should be familiar with the Morse and Bandot alphabets and the most common errors of wire and :radio transmission methods, so as to be able to refer an error to its probable origin or to nd clues for the correction of badly garbled groups all other means fail. The following tables will be found useful:

International Morse alphabet (used in radio, cables, and outside United States)			American Morse alphabet (used in the United States, except for radio)		
Letters and figures	Alphabet	Frequent errors	Letters and figures	Alphabet	Frequent errors
A	• —	i, m, t, et	A	• —	i, t, et
B	— • • •	d, ts	B	— • • •	d, h, ts
C	— • — •	f, k, j, r, nn	C	• • •	s, z, ie
D	— • •	b, s, l, ti	D	— • •	b, ti
E	•	t, a, i	E	•	t
F	• • — •	q, r, in	F	• — •	r, q, en
G	— — •	m, n, o, q, me	G	— — •	n, c, me
H	• • • •	s, v, b, se	H	• • • •	s, p, z, y, es
I	• •	a, n, s	I	• •	a, o, e
J	• — — —	w, o, eo, am	J	— • — •	c, k, ke
K	— • —	a, n, d, o, ta	K	— • —	j, n, ta
L	• — • •	x, r, d, ed	L	——	t, n
M	— —	a, n, i, tt	M	— —	n, a, tt
N	— •	i, m, t, te	N	— •	o, t, te
O	— — —	g, k, m, w, mt	O	• •	n, i, ee
P	• — — •	j, w, g, l, r, an	P	• • • • •	h, s
Q	— — • —	g, k, o, x, z, ma	Q	• • — •	f, g, u, in
R	• — •	a, n, f, g, s, l, w	R	• — •	s, i, ei
S	• • •	h, d, i, r, u, v	S	• • •	h, r, i
T	—	a, e, n	T	—	l, e, n
U	• • —	a, s, v, it	U	• • —	v, a, w, it
V	• • • —	h, u, x, st	V	• • • —	u, st
W	• — —	a, m, o, r, u, at	W	• — —	f, a, u, m, at
X	— • • —	d, v, u, k, y, tu	X	• — • •	l, y, f, al
Y	— • — —	x, w, k, c, nm	Y	• • • •	h, il
Z	— — • •	b, d, g, q, mi	Z	• • • •	h, c, se
1	• — — — —	0, 2	1	• — — — •	p
2	• • — — —	1, 3	2	• • — — • •	3
3	• • • — —	2, 4	3	• • • — — •	4
4	• • • • —	3, 5	4	• • • • —	3
5	• • • • •	4, 6	5	— — — —	
6	— • • • •	5, 7	6	• • • • • •	p
7	— — • • •	6, 8	7	— — • •	
8	— — — • •	7, 9	8	— • • • •	
9	— — — — •	8, 0	9	— • • —	x
0	— — — — —	9	0	——	L

TELETYPEWRITER GARBLE TABLE



	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	
GAIN OF 1ST PULSE	–	?	(	$	3	!	FIG.	&	7	,	(	2	/	!	?	1	1	,	Bell	"	7	LTR	2	/	6	"	UC
	A	B	K	D	E	F	FIG.	Y	U	J	K	W	X	F	B	Q	Q	J	S	Z	U	LTR	W	X	Y	Z	LC
GAIN OF 2ND PULSE	–	FIG.	:	.	–	(	&	ø	8	,	(	)	:	:	&	ø	1	4	7	)	7	:	2	LTR	1	2	UC
	A	FIG.	C	J	A	K	G	P	I	J	K	L	V	C	G	P	Q	R	U	L	U	V	W	LTR	Q	W	LC
GAIN OF 3RD PULSE	7	/	1	1	Bell	1	,	£	8	(	(	ø	.	,	.	ø	1	,	Bell	£	7	:	1	/	6	6	UC
	U	X	C	F	S	F	V	H	I	K	K	P	M	N	M	P	Q	C	S	H	U	V	D	X	Y	Y	LC
GAIN OF 4TH PULSE	.	?	:	$	$	1	&	.	:	,	(	&	.	,	9	:	LTR	4	1	9	(	:	FIG.	/	/	?	UC
	J	B	C	D	D	F	G	M	C	J	K	G	M	N	O	V	LTR	R	F	O	K	V	FIG.	X	X	B	LC
GAIN OF 5TH PULSE	2	?	:	?	"	/	&	£	ø	FIG.	LTR	)	.	.	9	ø	1	8	5	1	:	2	/	8	"		UC
	W	B	V	B	Z	X	G	H	P	FIG.	LTR	L	M	M	O	P	Q	G	Y	T	O	V	W	X	Y	Z	LC
LOSS OF 1ST PULSE	LF	9	:	CR	Blnk	.	&	£	8	4	:	)	.	,	9	ø	ø	4	SPC	5	8	:	)	.	£	5	UC
	LF	O	G	CR	Blnk	N	G	H	I	R	G	L	M	N	O	P	P	R	SPC	T	I	V	L	M	H	T	LC
LOSS OF 2ND PULSE	3	?	,	$	3	1	9	£	SPC	$	1	5	.	,	9	£	6	CR	Bell	.5	Bell	.	"	/	6	"	UC
	E	B	N	D	E	F	O	H	SPC	D	F	T	M	N	O	H	Y	CR	S	T	S	M	Z	X	Y	Z	LC
LOSS OF 3RD PULSE	–	?	4	$	3	$	&	5	LF	.	.	)	9	CR	9	)	2	4	3	5	-	8	2	?	'	"	UC
	A	B	R	D	E	D	G	T	LF	J	J	L	O	CR	O	L	W	R	E	T	A	G	W	B	Z	Z	LC
LOSS OF 4TH PULSE	–	"	8	3	3	Bell	)	£	8	–	7	)	£	SPC	5	ø	1	LF	Bell	5	7	ø	2	4	6	"	UC
	A	Z	I	E	E	S	L	H	I	A	U	L	H	SPC	T	P	Q	LF	S	T	U	P	W	Y	Y	Z	LC
LOSS OF 5TH PULSE	–	$	1	$	3	1	4	SPC	8	,	(	LF	.	.	CR	6	7	4	Bell	Blnk	7	:	–	1	Bell	3	UC
	A	D	C	D	E	F	R	SPC	I	J	K	LF	N	N	CR	I	U	R	S	Blnk	U	C	A	F	S	E	LC

	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	

AT THE TOP AND BOTTOM OF THE CHART ARE THE LETTERS ORIGINALLY TRANSMITTED. IN THE SQUARES ARE THE CHARACTERS WHICH WOULD BE RECEIVED WITH GAIN OR LOSS OF PULSE DEPENDING UPON WHETHER MACHINE IS IN "UC" (UPPER CASE) OR "LC" (LOWER CASE).

Chapter 7

FUNDAMENTAL RULES FOR SAFEGUARDING CRYPTOGRAMS

83 General

The rules given in this chapter are to be considered as a general guide only. Under actual operating conditions much is dependent upon special situations, and the specic cryptographic systems employed. Therefore, the particular rules and regulations currently in effect always will take precedence over those stated herein.

84 Fundamental Rules of Cryptographic Security

a. Failure to observe the fundamental rules of cryptographic security often makes possible the solution of cryptographic systems by enemy cryptanalysts. These rules apply to the originators of messages to be cryptographed as well as to cryptographic personnel. Detailed instructions for the writers of such messages are outside the scope of this manual. It is, however, desirable to indicate the following points:

(1). Stereotypic phraseology must be avoided, especially at the beginning and ending of a message. The known or suspected presence of stereotypic phraseology constitutes the basis of many methods employed in cryptanalysis; in some cases, indeed, the only possible method of solution makes use of the presence of stereotypic phraseologies, or, as they are often called, cribs. Operating instructions for currently authorized cryptosystems prescribe the application of measures which effectively reduce the dangers of stereotypic phraseology to the security of those systems; however, as an added precaution, routine reports of all kinds should be sent by agencies of signal communication not susceptible to interception.

(2). Special care must be taken to see that the messages are clear and concise. If a message is ambiguous or incomplete, unnecessary confusion results and the accuracy of the cryptographic operation is brought into question.

(3). Messages should be shortened by the deletion of unnecessary words. Conjunctions, prepositions, repetitions of words, and, especially, punctuation should be reduced to a minimum. When punctuation is necessary, it should be spelled out, either in full or in abbreviated form. Numbers should also be spelled out. Where letters of the alphabet must be used, as in certain symbols designating types of equipment, it may be necessary to represent these letters by their authorized phonetic equivalents, where it is essential that there be no possibility of error. Such spelling out however, should be reduced to a minimum.

(4). Authorized abbreviations should be used whenever practicable.

(5). Regulations regarding the manner of indicating addresses and signatures should be carefully followed.

(6). Regulations governing the security classication of messages (Top Secret, Condential, Restricted) must be observed at all times.

b. *Much of the success which attends the eorts of cryptanalysts is based upon ignorance and carelessness on the part of cryptographic personnel.* Rarely are cryptographic blunders the result of willful violation of instructions; but if cryptographic personnel realize, that, by carelessness or ignorance, their own lives and those of thousands of their comrades are jeopardized, they will be more attentive to rules set up for their guidance. The most important of these rules are as follows:

(1). *Questionable messages.* Never cryptograph a message which, in the opinion of the cryptographer, violates any of the provisions or regulatons relating to the drafting of messages, until the question has been referred to and passed by someone with authority to change the message.

(2). *Mixing plain and cryptographic text.* Never allow cryptographic text with its equivalent plain language to appear in a cryptogram, and never mix plain and cryptographic text, except in messages where such mixtures are specically permitted. This includes punctuation and abbreviations of any description. Such messages afford valuable clues to the enemy. If a message is to be cryptographed at all, it should be completely cryptographed.

(3). *Text of messages.*

a Never repeat in the clear the identical text of a message once sent in cryptographic form, or repeat in cryptographic form the text of a message once sent in the clear. Anything which will enable an alert enemy to compare a given piece of plain text with a cryptogram that supposedly contains this plain text is highly dangerous to the safety

of the cryptographic system. Where information must be given out for publicity, or where information is handled by many persons, the plaintext version should be very carefully paraphrased before distribution, to minimize the data an enemy might obtain from an accurate comparison of the cryptographic text with the equivalent, original plain text. To paraphrase a message means to rewrite it so as to change its original wording as much as possible without changing the meaning of the message. This is done by altering the positions of sentences in the message, by altering the positions of subject, predicate, and modifying phrases or clauses in the sentence, and by altering as much as possible the diction by the use of synonyms and synonymous expressions. In this'process, deletion rather than expansion of the wording of the message is preferable, because if an ordinary message is paraphrased simply by expanding it along its original lines, an expert can easily reduce the paraphrased message to its lowest terms, and the resultant wording will be practically the original message. It is very important to eliminate repeated words or proper names, if at all possible, by the use of carefully selected pronouns; by the use of the words former, latter, rst mentioned, secondmentioned; or by other means. After carefully paraphrasing, the message can be sent in the other key or code.

b Never send the literal plain text or a paraphrased version of the plain text of a message which has been or will be transmitted in cryptographed form except as specically provided in appropriate regulations.

(4). *Keys.* Never repeat in a different key or system, without paraphrasing, a cryptographed message which has once been trans- mitted, unless specically authorized by the appropriate authority.

(5). New cipher keys. Never transmit a new cipher key by means of a message cryptographed in an old key.

(6). Addresses or signatures. Never place cryptographed addresses or signatures at the beginning or end of the cryptographed text. Bury them in the body of the message.

(7). Identifying information. Include in the address of a cryptographed message only the minimum information necessary for the message to reach the headquarters for which it is intended.

(8). *Replies.* Never reply to a cryptographed message in the clear.

(9). *Short titles.* Never use short titles as system or message indicators in cryptographed messages.

(10). *Dummy letters and padding.* Never use dummy letters or padding unless their use is specically authorized.

(11). *System indicator.* Never encipher, encode, or disguise in any way the system indicator, unless specically authorized.

(12). *Notations.* Never place on the cryptographed copy of a message any notations about the system or the subject matter of the message.

(13). *Work tables.* Never allow unnecessary materials such as books, documents, or papers to be on the work table during the process of cryptographing and decryptographing.

(14). *Filing messages.* Never tile cryptographic messages and their equivalent plain text together. Work sheets must be destroyed by burning.

(15). *Check for accuracy.* Cryptographed messages should be checked for accuracy by decryptographing the message before transmission. Whenever practicable, this should be done by a cryptographer other than the one who originally cryptographed the message.

(16).) *Safeguarding material.* Observe all rules of physical security established to safeguard the cryptographic material and message translations. Utmost care should be taken to prevent the loss or unauthorized sight of the codes or lists of cipher keys in use. It is possible to photograph an entire code in two or three hours. Mere continued possession of the cryptographic material is, therefore, no absolute guaranty that it has not been compromised by photography or some other method of reproduction. The only absolute assurance of its not having been compromised is that it has never left the possession of the person into whose care it has been entrusted or the safe in which it is kept when not in use. Even if knowledge that a code or cipher has been compromised follows immediately after such compromise, the amount of time and the diiculties involved in notifying all concerned and distributing new cryptographic material are so great that serious damage is caused by the delay and interruption in communication, not to speak of the danger resulting from the enemys reading the most recent messages in the compromised system.

(17). *Reporting compromise.* Finally, it must be realized that the compromise or capture of cryptographic material is a most serious matter. If there is any reason to suspect that such material or related documents have been compromised, higher authority should be notied by the fastest means possible. Not only is such material available to the enemy for reading current and old messages, but also the cryptanalytic data afforded thereby become most useful in working on similar systems to replace the compromised one. The failure to notify higher authority promptly, if compromise is suspected, may jeopardize the lives of thousands of soldiers and is therefore more serious than permitting compromise to take place, if it could have been avoided. Regulations for reporting compromise should be carefully observed at all times.