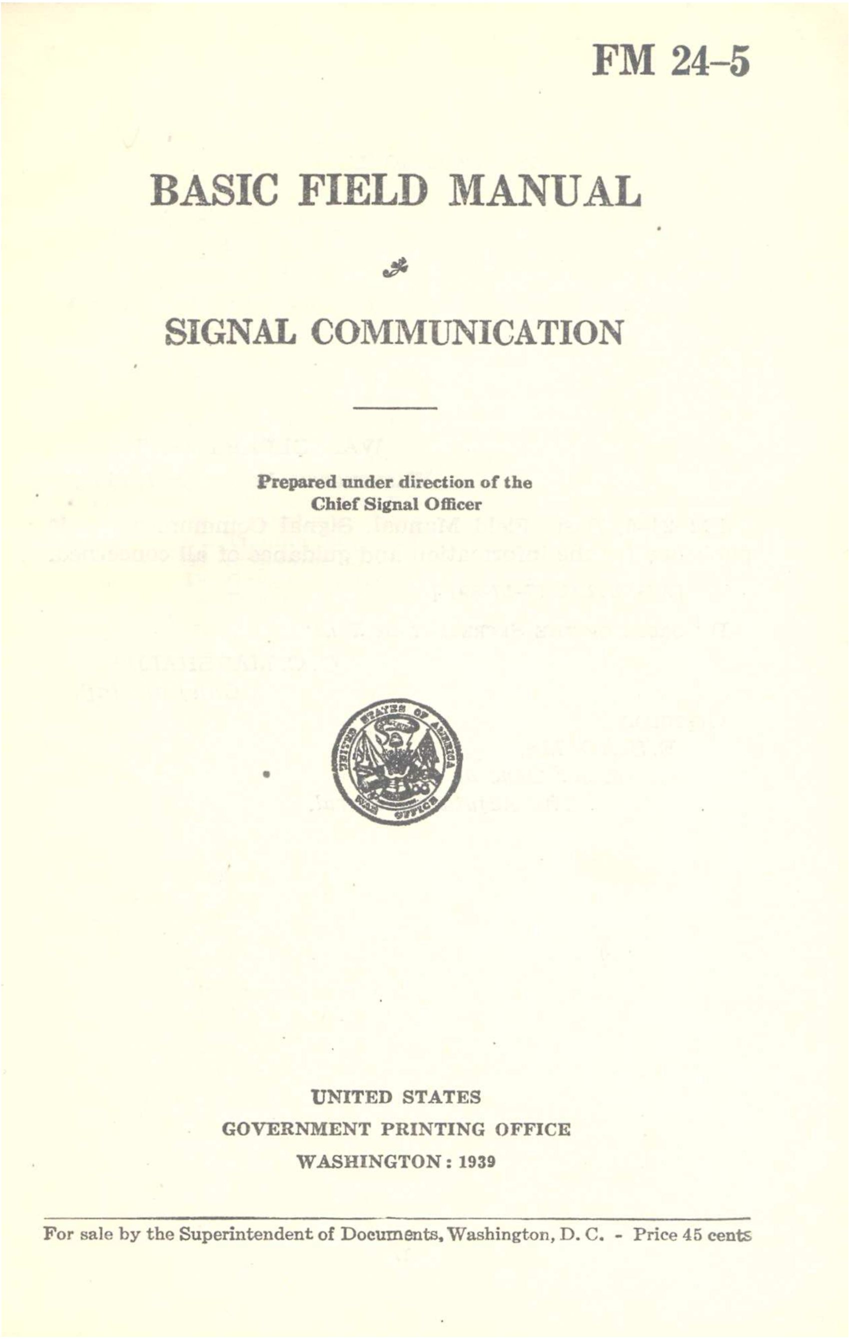
Association des Réservistes du Chiffre et de la Sécurité de l'Information

Basic Field Manual
signal communication
Par Daniel TANT



FM 24-5

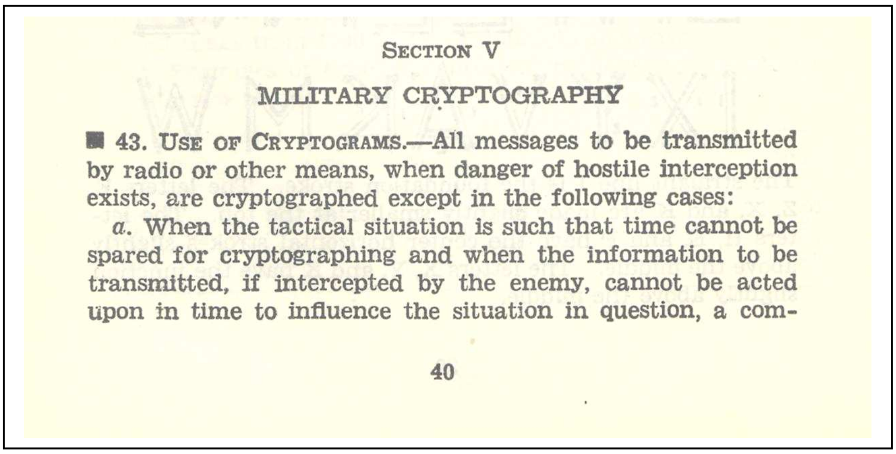
BASIC FIELD MANUAL

SIGNAL COMMUNICATION

Prepared under direction of the
Chief Signal Officer

UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON : 1939

For sale by the Superintendent of Documents, Washington, D. C. - Price 45 cents



Section V

MILITARY CRYPTOGRAPHY

■ 43. **Use of Cryptograms.**—All messages to be transmitted by radio or other means, when danger of hostile interception exists, are cryptographed except in the following cases:

a. When the tactical situation is such that time cannot be spared for cryptographing and when the information to be transmitted, if intercepted by the enemy, cannot be acted upon in time to influence the situation in question, a commanding officer or his authorized representative may order the transmission of a message in plain language by a radio station serving his headquarters or command. Such written messages will be marked "Send in clear," over the signature of the commander or his authorized representative.

b. Commanders may authorize the normal transmission of artillery fire-control messages in clear.

c. All cryptographing and decryptographing of messages at a headquarters are performed in the message center, except as authorized in paragraph 32, unless the message requires a code or cipher not in the possession of the message center. The message center is provided with the authorized codes, cipher devices, and keys.

d. If it becomes necessary to modify the wording of a message in order to cryptograph it or to facilitate cryptographing, the modified text will be submitted to the writer for approval before transmission.

■ 44. DEFINITIONS.—A knowledge of the following terms is essential for all personnel handling code and cipher messages:

a. "Plain text," "clear text," or "plain language" is the text of a message which, on its face, conveys an intelligible meaning in a spoken language.

b. "Secret text" or "secret language" is the text of a message which, on its face, conveys no intelligible meaning in any spoken language. The secret text of a message constitutes a cryptogram.

c. "Cryptography" is the science which embraces all the methods and devices whereby plain text may be converted into secret text.

d. "Cryptograms" are of three fairly distinct types as follows:

(1) *Cipher.*—A cryptogram in cipher is one which has been produced by taking the individual letters of the plain text as units and applying to them either or both of two cryptographic processes known as "transposition" and "substitution" explained below. The resulting secret text is called "cipher text" and the operation of producing it is called "enciphering"; the reverse operation, that of reproducing

the plain text from the cipher text by a direct reversal of the steps involved in its enciphering, is called "deciphering." The basis of every cipher system is an agreement between correspondents covering the general method and the steps to be followed in cryptographing. That portion of the agreement which specifically controls the steps under the general method is termed the "key." The key is usually of a variable nature, changeable at the will of the correspondents. Normally it consists of an easily remembered word, phrase, or sentence; or of a number or series of numbers derivable from a word, phrase, or sentence.

(*a*) *Transposition cipher.*—The cryptographic process known as transposition consists in rearranging the letters constituting the plain text (rarely syllables or whole words) so that the resultant text becomes unintelligible. The letters undergo no change in identity; only their relative order is altered. A cryptogram which has been produced in this way is termed a "transposition cipher."

(*b*) *Substitution cipher.*—The cryptographic process known as substitution consists in replacing the letters constituting plain text by other letters, figures, symbols, or the like. Here the letters undergo a change in identity without a change in their relative order. A cryptogram which has been produced in this way is termed a "substitution cipher."

(*c*) *Combined cipher.*—When both of these processes have been applied in producing a cryptogram, the latter is termed a combined "substitution-transposition cipher."

(2) *Code.*—(*a*) A cryptogram in code is one which has been produced by taking whole sentences, phrases, words, letters, or numbers of plain text as units and replacing them by arbitrary groups of symbols given as their equivalents in a code book. The resulting secret text is called "code text" and the operation of producing it is called "encoding"; the reverse operation, that of reproducing the plain text from the code text by reference to the code book, is called "decoding." A one-part code consists of only one section which serves for either encoding or decoding. A two-part code consists of two sections, one section arranged to facilitate encoding and the other to facilitate decoding. A one-part code is very much less secure than a two-part code.

(*b*) Code groups or code words are arbitrary groups of symbols constituting code text. They usually consist of letters or figures or rarely of both letters and figures.

(3) *Enciphered code.*—A cryptogram in enciphered code is one which has been produced by first encoding the plain text and then enciphering the code text.

e. To "cryptograph" a message is to convert its plain text into secret text. This is a convenient term to use in referring to the processes involved without indicating or specifying whether they are methods of enciphering or encoding.

f. To "decryptograph" a message is to reconvert its secret text into plain text by a direct reversal of the operations involved in its cryptographing. This is a convenient term to use in referring to the processes involved without indicating whether the cryptogram is in cipher, in code, or in enciphered code. As enciphering and encoding are forms of cryptographing, so deciphering and decoding are forms of decryptographing.

g. "Cryptanalysis" is the name applied to the steps and processes involved in converting cryptograms (usually of hostile origin) into plain text by means other than those normally employed in decryptographing messages of friendly origin.

■ 45. SAFETY AFFORDED BY CRYPTOGRAPHY.—Codes and ciphers are used in messages for either or both of two purposes; condensing messages and maintaining secret, except from the addressee, the contents of messages. Unless secrecy is accomplished with certainty, all of the additional time, labor, and danger of error involved in cryptographic messages is wasted; moreover, the correspondents may be lulled into a false sense of security in the belief that their messages are secret, when, in fact, the enemy may have cryptanalyzed them and taken action accordingly. With the increased use of radio as well as other means of electrical communication, the safeguarding of codes and ciphers has assumed a paramount importance. In general it may be stated that no cryptographic system suitable for a voluminous official correspondence is absolutely proof against the organized, cooperative efforts of a large and well-trained staff of cryptanalysts. Practically every cipher system that has ever been employed for military purposes has been solved and practically any code book can be reconstructed by analysis, given a sufficient number of cryptograms and the personnel and time necessary to accomplish it.

■ 46. **Comparison of Codes and Ciphers.**—*a.* Each of these two general methods of secret communication is needed in the military service. The principal factors to be taken into account in comparing code and cipher methods as systems of secret communication are—

(1) Simplicity, rapidity, practicability.
(2) Secrecy.
(3) Accuracy.
(4) Economy.

b. In general, it may be said that code is a more rapid and more simple method of secret communication than is cipher. The processes of enciphering and deciphering require very close mental attention to avoid errors, and are usually much slower than those of encoding and decoding which more nearly approach automatic processes and thus require less concentrated mental effort. This is of greatest importance in the combat zone. There are some very small cipher devices which tend to reduce the mental strain to a minimum, but in general the cryptograms they yield are not as secret as those produced by a good code, especially when many messages are available for interception by the enemy.

c. Code systems are, on the whole, more secret than cipher systems, depending upon—

(1) The type of code. A two-part code is more secret than a one-part code.

(2) The extent of its vocabulary or contents.

(3) The extent to which the code is used; that is, the number of messages transmitted.

d. Furthermore, the solution of one message does not as a rule entail the immediate breakdown of the whole system, with the consequent solution of all other messages in the same key, as is the case in ciphers. On the other hand, in the case of code it is absolutely necessary to guard at all times the code book so that it does not fall into the hands of the enemy. Actual possession is not always necessary, for a single opportunity to copy or memorize certain portions is sufficient to compromise the whole code.

e. On the whole, it may be said that code systems are less accurate than cipher systems and are more subject to the necessity for repetition of messages. This is because a mistake in one or two code groups may obscure, alter, or render unintelligible the meaning of a whole message, whereas, in the case of ciphers, the meaning of a few letters which are in error may be supplied by the context.

f. Since code text is usually shorter than the equivalent plain text, the latter is more economical to handle than cipher. This is of great importance where the amount of signal traffic is heavy. On the other hand, for the purpose of maintaining secrecy in military communication, codes of the two-part type must be changed rather frequently. This necessitates repeated processes of preparation, printing, and distribution, all of which take much time and labor.

■ 47. AUTHORIZED MILITARY CODES.—See AR 380–5 for the manner in which codes are authorized to be used. Among others, the codes listed below are authorized for general use in the military service. See paragraph 100 for their code indicators and the number of characters per code group. Training and maneuver editions of certain confidential codes are given a restricted classification when published. Blank groups are left in codes for the assignment of special meanings by commanders. These meanings are published in signal operation instructions as supplements to the codes. (See examples on pages 266 and 268.)

a. War Department Telegraph Code.—This code is a nonsecret code primarily intended for economy. It furnishes no security from code experts and should never be used for encoding secret messages. It is issued to all those who are required to handle any considerable volume of business by telegraph, radio, or cable.

b. Division Field Code.—This code is issued to message centers of divisions and all lower tactical units down to and including the battalion, and in peacetime for training purposes, it may be issued down to companies.

c. Aerial Observation Codes and Panels.—These codes are prepared by the War Department or the headquarters of the field forces and are issued to all units that engage in communication between ground and air.

(1) The *Fire-Control Code* is fixed and is used in adjustment of fire.

(2) The *Air-Ground Liaison Code* is employed in general observation and reconnaissance. In emergencies it may also be used in the absence of other cryptographic means for communication between forward ground stations. It is revised frequently for purposes of secrecy by rearrangement of code groups and their meanings.

d. Special codes.—Such codes as address and signature codes, map coordinate codes, geographic, meteorological, and supply catalog codes, as well as appendixes to the various codes listed above, will be published from time to time.

e. Prearranged messages.—In traffic by radiotelephone, it is often desirable to use some form of prearranged message or groups of letters to indicate meanings which will not readily be apparent to the enemy. These messages or groups will be changed frequently and may be prepared by local commanders as appropriate. These codes or messages being of a temporary nature, the prohibition as to mixing of clear and secret text does not apply. A map coordinate code is particularly appropriate for use in conjunction with such messages. For example, "Advance guard motors move forward to next position" might be transmitted as "CJ" or a prearranged phrase might be used instead of a letter group. For example, "Objective taken" might be transmitted "The fox is in his hole."

■ 48. AUTHORIZED MILITARY CIPHERS.—Among others, the following ciphers are authorized for use in the military service:

a. Cipher device M-94.—This cipher device is explained in section VI.

b. Telegraph printer cipher system.—This is a cipher system operated in connection with telegraph printers and is used only between the higher headquarters where traffic is very great.

■ 49. RULES FOR USE OF CODES AND CIPHERS (AR 380–5).—The following general rules govern the use of codes and ciphers:

a. The instructions contained in each code book or furnished with each cipher system must be carefully studied and thoroughly understood before the code or cipher is used.

b. Care should be exercised to prevent the loss or compromise of a code book or cipher key. If a code book is lost or possibly compromised, the fact should be reported promptly to higher headquarters.

c. Except in emergency, no code or cipher which has not been approved by higher authority should be employed within any unit.

d. Care should be exercised that only one edition of a code of a particular class, or only one cipher key is being used within a unit at one time. When a code is replaced by a new code or a new edition, the replaced code will be destroyed by burning unless otherwise ordered.

e. Cryptographic messages should be short and concise. Long messages facilitate solution by the enemy.

f. Never repeat a message in a code or cipher other than the one in which it was originally sent. If the enemy has already solved one of the codes or cipher keys used, he will translate the message by that code or cipher key and will thus be given clues to the solution of the other code or cipher key.

g. Never cryptograph a message which has been sent previously in clear and never send a message in clear which has been sent previously as a cryptogram. If the enemy compares the cryptographic message with the clear message he will be able to break into the code and solve other messages, or in the case of ciphers, he will have the key for the solution of all other messages.

h. Never mix secret and clear text in the same message except as permitted in paragraph 47*e*. This applies also to abbreviations and signs of punctuation which are equivalent to clear text. If clear text of any kind whatever is left in the message, the enemy can more easily discover the meaning of the secret text. If cryptographed at all the entire message must be cryptographed.

i. A cryptographed message never should be filed with the clear message. (See par. 34*d.*)

j. Capital letters should be employed throughout in writing cryptograms in order to avoid errors. In the case of code, the grouping of the letters of the code text corresponds to the length of the code groups as given by the book; in the case of cipher, the text is written and transmitted in groups of five letters. (See par. 42.)

SECTION VI

DESCRIPTION AND USE OF CIPHER DEVICE M–94

■ 50. PURPOSE AND DISTRIBUTION.—Cipher device M–94 is a cryptographic instrument that is an item of equipment issued by the Signal Corps to all message centers as one of the authorized means for secret communication. It is also an item of equipment possessed by all naval units and stations, including those of the Marine Corps, and can be employed in certain classes of secret intercommunication between the Army and the Navy when specific arrangements therefor have been made by the appropriate commanders.

■ 51. DESCRIPTION.—*a.* The device is made of aluminum alloy and consists of the following parts:

(1) A central shaft, the left end of which terminates with a projecting shoulder, the right end of which is threaded.

(2) A set of 25 alphabet disks, on the rim of each of which there is stamped a different, completely disarranged alphabet.

(3) A guide-rule disk, consisting of a blank or unlettered disk from which projects a guide rule.

(4) A retaining plate, consisting of a thin disk upon one surface of which is stamped the name and type number of the device.

(5) A knurled thumb nut.

b. Each disk has a hole at the center suitable for mounting it upon the central shaft upon which the disk can be revolved forward or backward. The left face of each alphabet disk is provided with a circle of 26 equidistant slots; the right face is cupped and carries at one point on the inside rim of this cup a small projecting lug. The guide-rule disk also carries such a lug. When the disks are assembled upon the shaft, the lug on each disk engages with one of the slots on the adjacent disk on the right and thus the disks can be held in engagement in any desired relative positions by screwing down the knurled thumb but against the retaining plate which is inserted between the last alphabet disk and the nut.

c. When the thumb nut and the retaining plate are removed and the alphabet disks are taken off the shaft, it will be noted that each alphabet disk is stamped on its inside or cup surface with an identifying symbol consisting of a number that is above the central hole and a letter that is below it. The numbers run from 1 to 25, inclusive, the letters from B to Z, inclusive. These symbols are employed to designate the sequence in which the alphabet disks are to be assembled upon the shaft in cryptographing or decryptographing messages as described in paragraph 53. Either symbol may be used for this purpose (as prearranged) but for the present only the numerical identifying symbols will be so used.

■ 52. NECESSITY FOR KEY AND PROVIDING FOR CHANGES THEREIN.—*a*. Messages cryptographed by the same sequence of alphabet disks can remain secure against solution by a well-organized and efficient enemy cryptanalytic section for only a relatively short time. It is impossible to state exactly how long, because solution depends upon a number of variable factors; a conservative estimate would place the minimum at 6 hours, the maximum at 2 or 3 days. For this reason it is necessary to change the sequence from time to time, and the method for determining or indicating the new sequence must be agreed upon in advance and thoroughly understood by all who are to use the instrument.

b. The sequence in which the alphabet disks are assembled upon the shaft constitutes the key in this cipher system. When a change in key is to take place, exactly what the new key will be and the exact moment that it is to supersede the old key will be determined by the proper commander and will be published in signal operation instructions. (For example, see page 272.)

■ 53. **Detailed Instructions for Setting Device to a Predetermined Key.**—*a.* The method prescribed herein is based upon a key word or key phrase from which the sequence of numbers constituting the key for assembling the alphabet disks may be obtained by following a simple, standardized procedure. The reason for employing such a procedure is that it makes it possible to derive at will a relatively long sequence of numbers (which woul dbe difficult to remember) from a word or phrase (which is easy to remember) and thus eliminates the necessity of carrying the key in written form upon the person. It is this basic key word or key phrase which is communicated throughout the command in signal operation instructions. The exact method of deriving the numerical key sequence from the key word or key phrase is given step by step in *b* below.

b. Assume that the key phrase so communicated is CHINESE LAUNDRY. The following are the detailed steps to be followed in deriving the numerical key sequence:

(1) A set of rows of cross section squares, 25 squares in each row, is prepared. (Prepared sheets of ¼-inch squares are suitable.)

(2) In the top row the series of numbers 1, 2, 3–25 are inserted. Thus:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

(3) Beginning under the number 1, the successive letters of the key phrase are written in the second row of squares under the successive numbers. Thus:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
C	H	I	N	E	S	E	L	A	U	N	D	R	Y											

(4) The key phrase is extended by repetition until there is a letter under the number 25, making a key sequence of 25 letters. If the key consists of a word or phrase containing

more than 25 letters, those after the twenty-fifth letter are merely omitted. Thus:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
C	H	I	N	E	S	E	L	A	U	N	D	R	Y	C	H	I	N	E	S	E	L	A	U	N

(5) The letters of the key sequence are now numbered serially from left to right in accordance with the relative position that each letter occupies in the ordinary alphabet. Since the letter A comes first in the ordinary alphabet and since this letter occurs twice in the illustrative key sequence, the number 1 is written under the first appearance of A in this sequence and the number 2 is written under its second appearance. Thus:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
C	H	I	N	E	S	E	L	A	U	N	D	R	Y	C	H	I	N	E	S	E	L	A	U	N
								1														2		

(6) The next letter in the ordinary alphabet is B. The key sequence is carefully examined to see if it contains the letter B. Since this letter does not appear in the illustrative key sequence, the latter is examined to see if it contains the letter C. This letter occurs twice in the illustrative key sequence and the first C, therefore, is assigned the number 3, the second C the number 4. Thus:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
C	H	I	N	E	S	E	L	A	U	N	D	R	Y	C	H	I	N	E	S	E	L	A	U	N
3								1						4								2		

(7) The next letter in the ordinary alphabet is D, which, being present in the key sequence, is assigned the next number, and so on. Thus, the process is continued until each letter has been assigned a number. The work must be done carefully so as not to overlook a single letter. If an error is made in the early stages of the work, it necessitates starting anew. The operator should be especially careful with letters which immediately follow one another in the ordinary alphabet but are present in the key sequence in reversed order, such as ED, FE, ON, and so on. It is easy to make a mis-

take in such cases and to assign numbers to these letters in a sequence that is the reverse of what it should be.

(8) When the numbering process has been completed and if the work has been correctly performed, it will be found that every letter of the key sequence has a number under it and that the greatest number that appears is 25. If this is not the case, it is an immediate signal that an error has been made. It cannot, however, be assumed that so long as every letter has a number under it, with the greatest number 25, this is immediate and conclusive proof of accuracy in the work. The operator should invariably check his work; better yet, if two clerks are available, each one should derive the numerical key independently and check final results by comparison.

(9) The key phrase selected as an example in the foregoing description yields the following numerical key:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
C	H	I	N	E	S	E	L	A	U	N	D	R	Y	C	H	I	N	E	S	E	L	A	U	N
3	10	12	16	6	21	7	14	1	23	17	5	20	25	4	11	13	18	8	22	9	15	2	24	19

(10) It is this sequence of numbers which indicates the order in which the successive alphabet disks are to be assembled upon the shaft from left to right. Thus, according to the foregoing key sequence, alphabet disk No. 3 comes first, that is, immediately to the right of the guide-rule disk; alphabet disk No. 10 comes next, and so on. Alphabet disk No. 19 is the last in this particular key, and after it has been placed on the shaft, the retaining plate and thumb nut are added and the latter screwed down a distance sufficient to keep the assembly together and yet permit of revolving individual disks freely upon the shaft. The device is now ready for use in either cryptographing or decryptographing messages.

■ 54. Cryptographing a Message.—Suppose the following message is to be enciphered with the key used in paragraph 53:

CO 3d INF

HAVE JUST REACHED EASTERN EDGE OF WOODS ALONG 552–592 ROAD WILL REMAIN IN OBSERVATION

CO 2d BN

a. The message is written down on the work sheet underneath the key lines of 25 letters each. Space is left under each line for the insertion of cipher letters. For procedure in connection with abbreviations and numbers appearing in the text of messages, see paragraph 55. Thus:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
C	H	I	N	E	S	E	L	A	U	N	D	R	Y	C	H	I	N	E	S	E	L	A	U	N
3	10	12	16	6	21	7	14	1	23	17	5	20	25	4	11	13	18	8	22	9	15	2	24	19
H	A	V	E	J	U	S	T	R	E	A	C	H	E	D	E	A	S	T	E	R	N	E	D	G
E	O	F	W	O	O	D	S	A	L	O	N	G	F	I	V	E	F	I	V	E	T	W	O	D
A	S	H	F	I	V	E	N	I	N	E	T	W	O	R	O	A	D	W	I	L	L	R	E	M
A	I	N	I	N	O	B	S	E	R	V	A	T	I	O	N									

b. By revolving the disks upon the shaft one by one, the first 25 letters of the message are alined to form a continuous horizontal row of letters reading from left to right along the outside of the cylinder. The guide rule will be found very convenient in marking the row upon which the letters are being alined, thus relieving the eyes of unnecessary strain and reducing the chance of making errors. After all 25 letters have been alined, the assembly is locked in position so that no disk can become displaced accidentally in further manipulation of the cylinder. *The row of letters is immediately checked to make sure that no displacement has occurred among the first few disks while manipulating the last few.*

c. The outside of the cylinder now presents a series of 26 rows of letters of which 24 rows are fully visible, the other two being hidden or partially obscured by the guide rule.

One of the 24 visible rows is the plain-text row that has just been set up and the other 23 rows are cipher-text rows *any one of which may be selected to represent the plain-text row*. One of these cipher-text rows is selected at random and the letters composing this row are written underneath the row of plain-text letters on the work sheet. Thus, supposing the row beginning **JUKLD** has been selected, the first cipher line will read as follows:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
C	H	I	N	E	S	E	L	A	U	N	D	R	Y	C	H	I	N	E	S	E	L	A	U	N
3	10	12	16	6	21	7	14	1	23	17	5	20	25	4	11	13	18	8	22	9	15	2	24	19
H	A	V	E	J	U	S	T	R	E	A	C	H	E	D	E	A	S	T	E	R	N	E	D	G
J	U	K	L	D	Y	K	I	T	Z	I	I	V	C	Y	C	V	U	Y	V	P	Y	W	H	J

It is not necessary to make any record on the work sheet as to which cipher-text row (above or below the plain-text row) was selected, nor is it necessary to indicate it in any manner whatever in the cipher message.

d. The thumb nut is loosened but not removed from the shaft. The next 25 letters of the message are alined, the thumb nut screwed down against the retaining plate, the letters in the alinement are checked, and again any one of the 23 visible cipher-text rows, except the one used to encipher the first line, is selected at random for the cipher text. The letters in the row selected are written down under the second line of plain-text letters on the work sheet. Thus, supposing the row beginning **YUYEZ** was selected, the work sheet now appears as follows:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
C	H	I	N	E	S	E	L	A	U	N	D	R	Y	C	H	I	N	E	S	E	L	A	U	N
3	10	12	16	6	21	7	14	1	23	17	5	20	25	4	11	13	18	8	22	9	15	2	24	19
H	A	V	E	J	U	S	T	R	E	A	C	H	E	D	E	A	S	T	E	R	N	E	D	G
J	U	K	L	D	Y	K	I	T	Z	I	I	V	C	Y	C	V	U	Y	V	P	Y	W	H	J
E	O	F	W	O	O	D	S	A	L	O	N	G	F	I	V	E	F	I	V	E	T	W	O	D
Y	U	Y	E	Z	D	H	V	U	Z	D	B	Q	P	O	Z	M	C	F	N	B	J	J	I	X

e. This process is continued in similar manner with the third line of the plain-text message. *It should never be made a practice to "favor," that is, frequently to select a particular cipher-text row above or below the plain-text row.* As irregular a selection as possible should be made, and the selection of the cipher-text row immediately above the plain-text row or immediately below the lower edge of the guide-rule should be avoided. Suppose these instructions have been followed and that there has been selected for the cipher-text row representing the third plain-text line of the message the row beginning **E A P T H**, the message now stands as follows:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
C	H	I	N	E	S	E	L	A	U	N	D	R	Y	C	H	I	N	E	S	E	L	A	U	N
3	10	12	16	6	21	7	14	1	23	17	5	20	25	4	11	13	18	8	22	9	15	2	24	19
H	A	V	E	J	U	S	T	R	E	A	C	H	E	D	E	A	S	T	E	R	N	E	D	G
J	U	K	L	D	Y	K	I	T	Z	I	I	V	C	Y	C	V	U	Y	V	P	Y	W	H	J

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

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

f. There are left only 16 letters to be enciphered, not enough to make a complete row of 25 letters. This, however, makes no difference in procedure; these 16 letters are merely alined and a cipher-text row is selected to represent them. Supposing the row beginning MEQRH is selected, the message now stands as follows:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
C	H	I	N	E	S	E	L	A	U	N	D	R	Y	C	H	I	N	E	S	E	L	A	U	N
3	10	12	16	6	21	7	14	1	23	17	5	20	25	4	11	13	18	8	22	9	15	2	24	19
H	A	V	E	J	U	S	T	R	E	A	C	H	E	D	E	A	S	T	E	R	N	E	D	G
J	U	K	L	D	Y	K	I	T	Z	I	I	V	C	Y	C	V	U	Y	V	P	Y	W	H	J

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

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

A I N I N O B S E R V A T I O N
M E Q R H B P O J T Y U Q N T W
```

g. The cipher text is now copied on the message form in 5-letter groups. It is as follows:

```
JUKLD  YKITZ  IIVCY  CVUYV  PYWHJ

YUYEZ  DHVUZ  DBQPO  ZMCFN  BJJIX

EAPTH  YOWHK  WWTNY  GMPRZ  JIFAD

MEQRH  BPOJT  YUQNT  W
```

h. The last group of the cipher message is, however, not a complete group of 5 letters. It is made so by adding four X's. *These are not to be cryptographed;* they are added merely to complete the last cipher group. The final message becomes as shown below:

```
JUKLD  YKITZ  IIVCY  CVUYV  PYWHJ

YUYEZ  DHVUZ  DBQPO  ZMCFN  BJJIX

EAPTH  YOWHK  WWTNY  GMPRZ  JIFAD

MEQRH  BPOJT  YUQNT  WXXXX
```

The message as it now reads is but one of many different forms in which this same message could appear externally, depending on exactly which of the available cipher-text rows is selected for each line of the encipherment.

■ 55. CRYPTOGRAPHING ABBREVIATIONS, PUNCTUATION SIGNS, AND NUMBERS.—*a.* Authorized abbreviations appearing in the original plain-text message may be enciphered as abbreviations without periods. *Examples:* Am Tn=AMTN; E. V. Brown Sch=EVBROWNSCH.

b. Normally the writer of a message spells out the punctuation signs he wishes transmitted, for example, STOP, COMMA, COLON, etc. If a message contains punctuation signs not so spelled out, they are spelled out and transmitted.

c. Cardinal and ordinal numbers when spelled out in letters in the original plain-text message are always enciphered exactly as spelled.

d. Cardinal numbers when expressed in figures in the original plain-text message must always be spelled out digit by digit in cryptographing. Examples:

4=FOUR
40=FOURZERO (*not* FORTY)
400=FOURZEROZERO (*not* FOUR HUNDRED)
455=FOURFIVEFIVE
2005=TWOZEROZEROFIVE
12.01 A. M.=ONETWOZEROONEAM
5.15 P. M.=FIVEONEFIVEPM

e. Ordinal numbers above the ordinal number 10th, when expressed in figures followed by "d," or "th," are cryptographed merely as digits spelled out without adding the "d" or "th". The omission of the "d" or the "th" will cause no confusion or ambiguity. Examples: 3d Bn=THIRDBN; 7th Pack Tn=SEVENTHPACKTN; 11th Regt=ONEONEREGT; 403d Am Tn=FOURZEROTHREEAMTN.

■ 56. DECRYPTOGRAPHING A MESSAGE.—*a.* Knowing the key word or key phrase, the numerical key is developed as described in paragraph 53 and the set of alphabet disks is assembled accordingly. The message to be decryptographed is written down in lines of 25 letters on cross section paper, if available, space being left under each line for the insertion of plain-text letters. Using the cipher message given in paragraph 54*h*, it appears under the key in the following form:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
C	H	I	N	E	S	E	L	A	U	N	D	R	Y	C	H	I	N	E	S	E	L	A	U	N
3	10	12	16	6	21	7	14	1	23	17	5	20	25	4	11	13	18	8	22	9	15	2	24	19
J	U	K	L	D	Y	K	I	T	Z	I	I	V	C	Y	C	V	U	Y	V	P	Y	W	H	J
Y	U	Y	E	Z	D	H	V	U	Z	D	B	Q	P	O	Z	M	C	F	N	B	J	J	I	X
E	A	P	T	H	Y	O	W	H	K	W	W	T	N	Y	G	M	P	R	Z	J	I	F	A	D
M	E	Q	R	H	B	P	O	J	T	Y	U	Q	N	T	W									

b. The first 25 letters of the cryptogram are set up on the device, the letters being alined in a row from left to right just above the guide rule. Fixing the disks in this position by screwing down the thumb nut, the whole cylinder is turned slowly, forward or backward, and each row of letters is carefully examined. One of these rows *and only one* will read intelligibly all the way across from left to right. That is the row which gives the plain text for the first 25 cipher letters. These letters are inserted in their proper place on the work sheet, giving the following:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
C	H	I	N	E	S	E	L	A	U	N	D	R	Y	C	H	I	N	E	S	E	L	A	U	N
3	10	12	16	6	21	7	14	1	23	17	5	20	25	4	11	13	18	8	22	9	15	2	24	19
J	U	K	L	D	Y	K	I	T	Z	I	I	V	C	Y	C	V	U	Y	V	P	Y	W	H	J
H	A	V	E	J	U	S	T	R	E	A	C	H	E	D	E	A	S	T	E	R	N	E	D	G

c. The thumb nut is then loosened, the next 25 cipher letters are set up, the assembly is locked into position, again the whole cylinder is slowly revolved, and the plain-text row of letters found. These are written down in their proper place and the process is continued with the rest of the cipher letters until the message has been completely decryptographed.

d. In the case of a cryptogram the last few letters of which do not form a complete set of 25, if any difficulty is experienced in picking out the plain-text row, the context of the preceding part of the message should give a good clue. In the case of the illustrative message above, it should be realized that the last four letters of the cryptogram are not to be decryptographed since they are merely added after cryptographing to make the last group of the cryptogram a complete group of five letters. They are omitted from the work sheet.

e. The plain-text message is then copied on a message form. The code clerk may, if authorized to do so by the message center chief, convert numbers which had to be spelled out in letters to permit of their cryptographing into their equivalent arabic figures. Abbreviations and punctuation signs are, however, copied exactly as they stand in the decryptographed message.

■ 57. Precaution.—*When in danger of capture, the alphabet disks of a device that has recently been used to cryptograph or decryptograph a message must be taken off, thoroughly disarranged, and reassembled.*