SECTION V

CIPHER DEVICE M–94

■ 55. 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. (See fig. 14.)

CAUTION: When in danger of capture, thoroughly destroy the cipher device beyond use or repair and, if possible, beyond recognition.

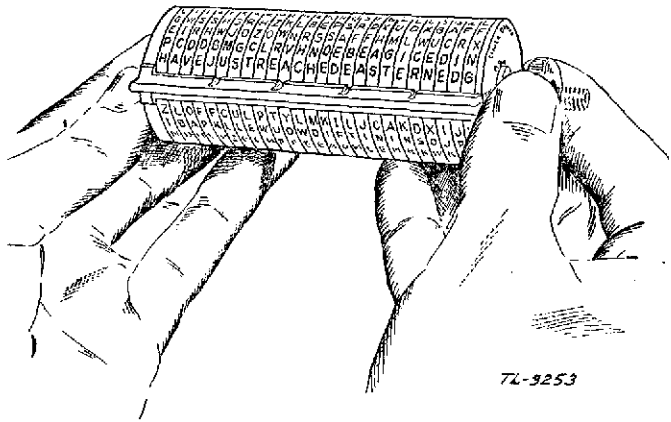


FIGURE 14.—Cipher device M–94.

■ 56. 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 nut 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 58. Either symbol may be used for this purpose (as prearranged) but for the present, only the numerical identifying symbols will be so used.

■ 57. 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. 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.

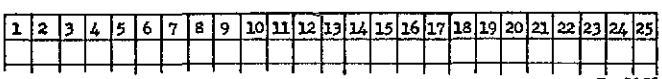
b. The sequence in which the alphabet disks are assembled upon the shaft constitutes the key in this cipher system. When a change in key is to take place, exactly what the new key will be and the exact moment it is to supersede the old key will be determined by the proper commander and will be published in signal operation instructions. (For example, see par. 265*f*.)

■ 58. 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. A relatively long sequence of numbers (which would be difficult to remember) may thereby be derived at will from a word or phrase (which is easy to remember) and the necessity of carrying the key in written form upon the person eliminated. The basic key word or key phrase, together with the numerical key derived as shown below, is distributed throughout the command in signal operation instructions.

b. Assume that the key phrase so distributed is **CHINESE LAUNDRY**. The detailed steps for deriving the numerical key sequence are as follows:

(1) Prepare a sheet of paper by drawing cross sections ¼-inch square, 25 squares to the line, unless prepared sheets are available.

(2) Insert in the top row of squares the series of numbers from 1 through 25. Thus:



(3) Beginning under the number 1, insert the successive letters of the key phrase in the second line 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											

TL-3234

(4) Extend the key phrase by repetition until there is a letter under the number 25, making a key sequence of 25 letters. (If the key phrase should contain more than 25 letters, those after 25 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

TL-3235

(5) Number the letters of the key sequence serially from left to right in accordance with their relative position in the ordinary alphabet. The letter A comes first in the ordinary alphabet, and occurs twice in the illustrative key sequence; therefore, write the number 1 under the first appearance of A in the key sequence and the number 2 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		

TL-3236

(6) The next letter in the ordinary alphabet is B. Examine the key sequence carefully to see if it contains the letter B. Since this letter does not appear in the key sequence, examine the key sequence for the letter C. This letter occurs twice in the illustrative key sequence. Write the number 3 under the first appearance of the letter C and the number 4 under the second appearance of the letter C. 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		

TL-3237

(7) The next letter in the ordinary alphabet is D, which is present in the illustrative key sequence. Assign the number 5 to the only appearance of the letter D and so on through the alphabet taking each letter successively and assigning the next number in sequence to each appearance of the letter in the illustrative key. The work must be done carefully in order that no letter will be overlooked. If an error is made in the early stage of deriving the key, start anew. Be especially careful with letters which follow each other in the ordinary alphabet, but which are present in the key sequence in reversed order, such as the combinations ED, FE, ON, and so on. It is easy to make a mistake in these cases and as a consequence, the assigned numbers will appear in reverse order.

(8) When the numbering process is completed and if the work is correctly performed, there will be a number under every letter of the key sequence and the highest number will be 25. If not, an error has been made. Check the work and better still, if two clerks are available, each should derive the key independently and the final results checked by comparison.

(9) The key phrase selected for the foregoing example will yield the following 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

72-3238

(10) This sequence of numbers indicates the order in which the successive alphabet disks are to be assembled on the shaft from left to right. According to the foregoing key sequence, place the alphabet disk No. 3 on the shaft immediately to the right of the guide rule disk; following disk No. 3, disk No. 10, and so on, are placed successively to the right of the guide-rule disk. Disk No. 19 is the last disk to be placed on the shaft using this particular key. When disk No. 19 is in place on the shaft, put on the retaining plate and the thumb nut. Turn the thumb nut on to the shaft sufficiently to retain the assembly and yet permit the revolving of the individual disks on the shaft. The device is now ready for enciphering and deciphering messages.

■ 59. CRYPTOGRAPHING A MESSAGE.—Suppose the following message is to be enciphered with the key used in paragraph 58:

CO 3d INF
HAVE JUST REACHED EASTERN EDGE OF WOODS ALONG 552–592 ROAD WILL REMAIN IN OBSERVATION.
CO 2d BN

a. Omitting the address, write the message down on the work sheet underneath the key line in lines of 25 letters each. (With experienced code clerks, the work sheet may be omitted.) Allow two blank lines between each line of clear text set down on the paper for the insertion of the enciphered text. (For procedure in enciphering abbreviations and numbers appearing in the text of the message, see paragraph 60.) 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									

TL-3239

b. Revolve the disks on the shaft one by one, alining the first 25 letters of the message to form one continuous row of letters from left to right with the aid of the guide rule. After alining all 25 letters, lock the assembly in place so that no disk can become displaced in further manipulation of the cylinder. *The row of letters now appearing along the guide rule should be checked at this point to be sure that the text in clear appears as written on the work sheet.*

c. The circumference of the cylinder now presents 26 rows

of letters, 24 of which are visible, the remaining two being hidden or partially obscured by the guide rule. One of the 24 visible rows is the clear text row; the remaining 23 are cipher text rows, *any one of which may be used as the cipher text.* Select one of the cipher text rows at random and write the letters composing this row immediately under the clear text on the work sheet. Assume that you chose the row beginning JUKLD, the first row on the work sheet would then 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	G	Y	G	V	U	Y	V	P	Y	W	H	J

TL-3240

It is not necessary to make a record of the cipher text row (above or below the plain text row) used as the cipher text nor is it necessary to indicate anywhere in the cipher text which row was used.

d. Loosen the thumb nut but do not remove it from the shaft. Aline the next 25 letters of the plain text as in *b* above and tighten the thumb nut once more. Recheck your work and then select another cipher text line from the 23 lines available, except the one used in enciphering the first line of the text. Write the cipher line thus obtained under the second clear text line on the work sheet. Assume you select the line beginning YUYEZ, the work sheet will now appear 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	G	Y	G	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

TL-3241

e. Continue this process in a similar manner with the third line of plain text. *Do not make a practice of selecting any particular line of cipher text above or below the clear text.* Avoid the selection of the line above the clear text line and the line below the guide rule. Assume that instructions have been followed up to this point and that you have selected the cipher text row beginning EAPTH to represent the third line of clear text, 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
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

TL-3242

f. Because the signature is not enciphered, there are only 16 letters remaining to be enciphered which are not enough to complete a row of cipher text. Aline this third line of clear text consisting of 16 letters and select a row of cipher text

to represent them. Assume that you select the row beginning MEQRH, 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
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									

72-3243

g. Now copy the cipher text on the message form in five-letter groups. It will then appear 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 message is not a complete group of five letters; make it a complete group by adding four X's. These are not cryptographed, but are merely added to complete the cipher group. The final work sheet on this message will appear as follows:

JUKLD YKITZ IIVCY CVUYV PYWHJ
YUYEZ DHVUZ DBQPO ZMCFN BJJIX
EAPTH YOWHK WWTNY GMPRZ JIFAD
MEQRH BPOJT YUQNT WXXXX

The message as it now appears is one of many forms in which the enciphered text might appear externally, depending on which of the cipher text rows were selected for each line of the encipherment.

i. All work sheets utilized in cryptographing the message will be destroyed by burning.

■ 60. 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. The writer of a message must spell out the punctuation signs he wishes transmitted; for example, STOP, COMMA, COLON, etc. Otherwise punctuation signs will not be transmitted. (See par. 38*a*(3).)

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 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 AM=ONETWOZEROONEAM
5.15 PM=FIVEONEFIVEPM

To save time in the encipherment of numerals, an abbreviated method of substituting one letter for each of 10 digits may be authorized in signal operation instructions. Thus "ALONG 552–592" might be enciphered as "ALONG JJP DASH JBP." The substituted letters must then be enciphered.

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 Pk Tn=SEVENTHPKTN; 11th Rgt=ONEONEREGT; 403d Am Tn=FOURZEROTHREEAMTN.

■ 61. DECRYPTOGRAPHING A MESSAGE.—*a.* If the key word or key phrase is known, the numerical key sequence can be de-

veloped as described in paragraph 58 and the set of alphabet disks assembled accordingly. Write the message to be decryptographed in rows of 25 letters on cross section paper, if available; leave space under each line for the insertion of the plain-text letters. Using the cipher message given in paragraph 59*h*, it would appear 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									

TL-3244

b. Set up the first 25 letters of the cryptogram on the cipher device, alining the letters in a row from left to right. Fix the disks in place by screwing down the thumb nut and check your work. Rotate the cylinder scanning successive rows until one is found which is intelligible all the way across from left to right. One row *and only one* will be found. That row contains the first 25 letters of the plain text. Insert these letters in the proper place on the work sheet which will give 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

TL-3245

c. Loosen the thumb nut and set up the next 25 letters of the cipher text. Lock the assembly in position and again check your work before scanning the rows for one containing plain text. Again write these 25 letters down in their proper place on the work sheet and continue the process until the whole message has been decryptographed.

d. If any difficulty is experienced in picking out a plain text row, the context of the preceding row should give a good clue as to the plain text following it. In the message illustrated above, the last four letters of the group are not to be decryptographed since they were merely added to make the last group of the cryptographed text a complete group of five letters. Omit them from the work sheet.

e. Copy the plain text message on a message form. The code clerk may, if authorized to do so by the message center chief, convert the numbers which had to be spelled out to be enciphered to their equivalent arabic numerals. Copy abbreviations and punctuation signs exactly as they stand in the decryptographed message.

SECTION VI

CONVERTER M–209

■ 62. DESCRIPTION AND USE.—*a.* Converter M–209 is a small, hand-operated, all-mechanical cryptographic machine that is an item of equipment issued by the Signal Corps to all message centers serving units below the division, and to certain types of armored force vehicles, and aircraft. In enciphering, it makes a printed record of the cryptogram; in deciphering, it makes a printed record of the plain text message. Its speed of operation is approximately 12 groups per minute.

b. TM 11–380 contains detailed information regarding the construction and operation of the machine, necessary adjustments, and repairs. While the manual may give illustrative examples of keying arrangements, specific cipher keys which are employed in actual field operations are issued in signal operation instructions.