

ARMY SECURITY AGENCY

OPERATING AND KEYING
INSTRUCTIONS
FOR
CONVERTER M-325(T)

THIS TEXT WILL BE RETURNED
UPON COMPLETION OF THE
SUBCOURSE WITH WHICH ISSUED

RESTRICTED--Dissemination of restricted matter.--No person is entitled solely by virtue of his grade or position to knowledge or possession of classified matter. Such matter is entrusted only to those individuals whose official duties require such knowledge or possession. (See also paragraphs 21a, and 24b, AR 380-5, 15 August 1946.)

HEADQUARTERS, ARMY SECURITY AGENCY

JULY 1948

ARMY SECURITY AGENCY

OPERATING AND KEYING INSTRUCTIONS FOR CONVERTER M-325(T)

TABLE OF CONTENTS

	<i>Paragraphs</i>	<i>Page</i>
Section I. General.....	1-8	7
II. Initial Instructions.....	4-5	8-9
III. Description.....	6-8	10-11
IV. Keying Elements.....	9-12	12-15
V. Operating Procedure.....	13-18	16-20

ARMY SECURITY AGENCY

JULY 1948

RESTRICTED--Dissemination of restricted matter.--No person is entitled solely by virtue of his grade or position to knowledge or possession of classified matter. Such matter is entrusted only to those individuals whose official duties require such knowledge or possession. (See also paragraphs 21a and 24b, AR 380-5, 15 August 1946.)

RESTRICTED

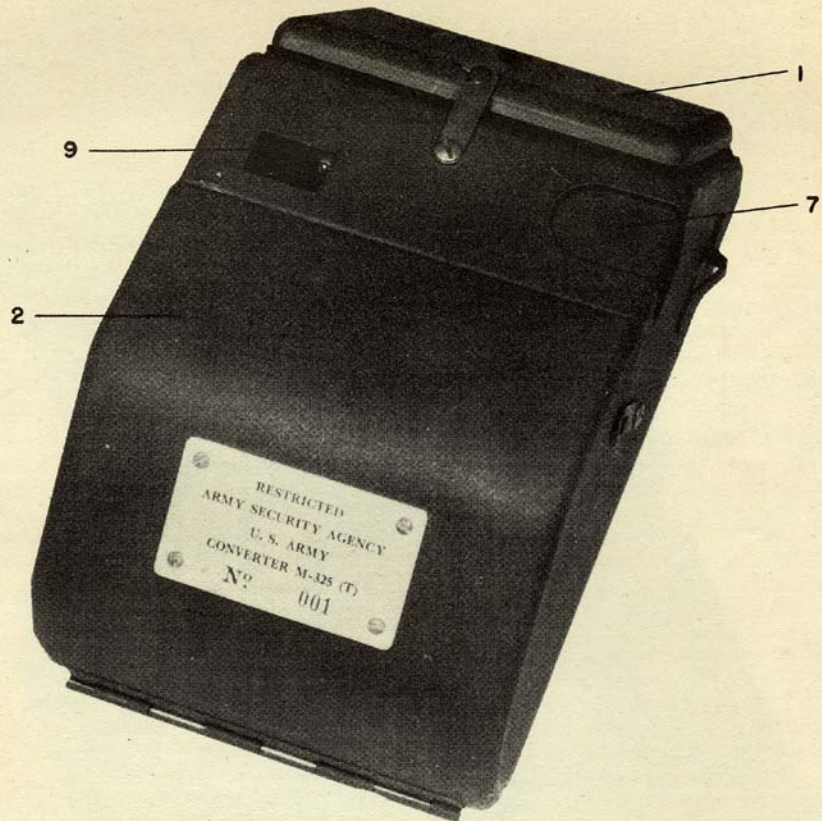


FIG. 1

RESTRICTED

RESTRICTED

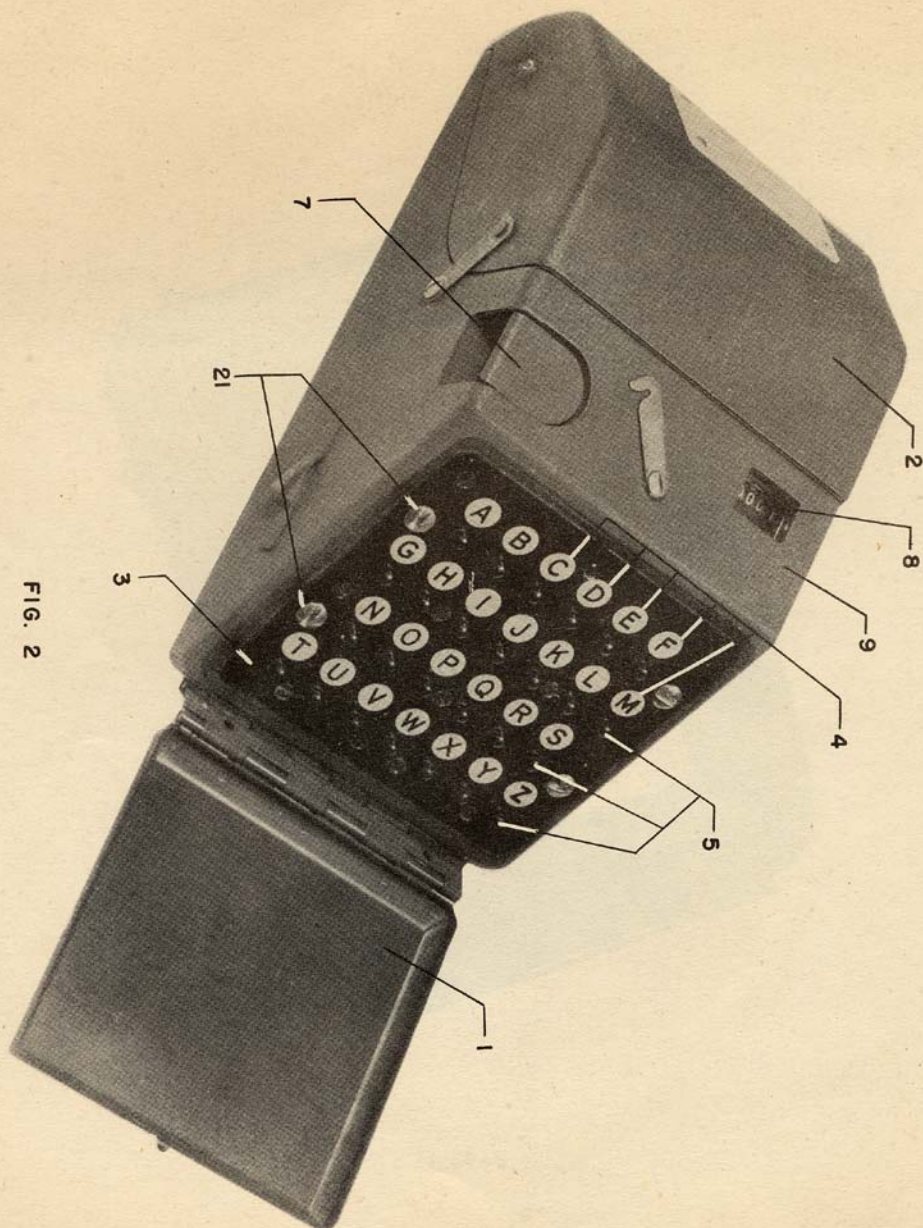


FIG. 2

RESTRICTED

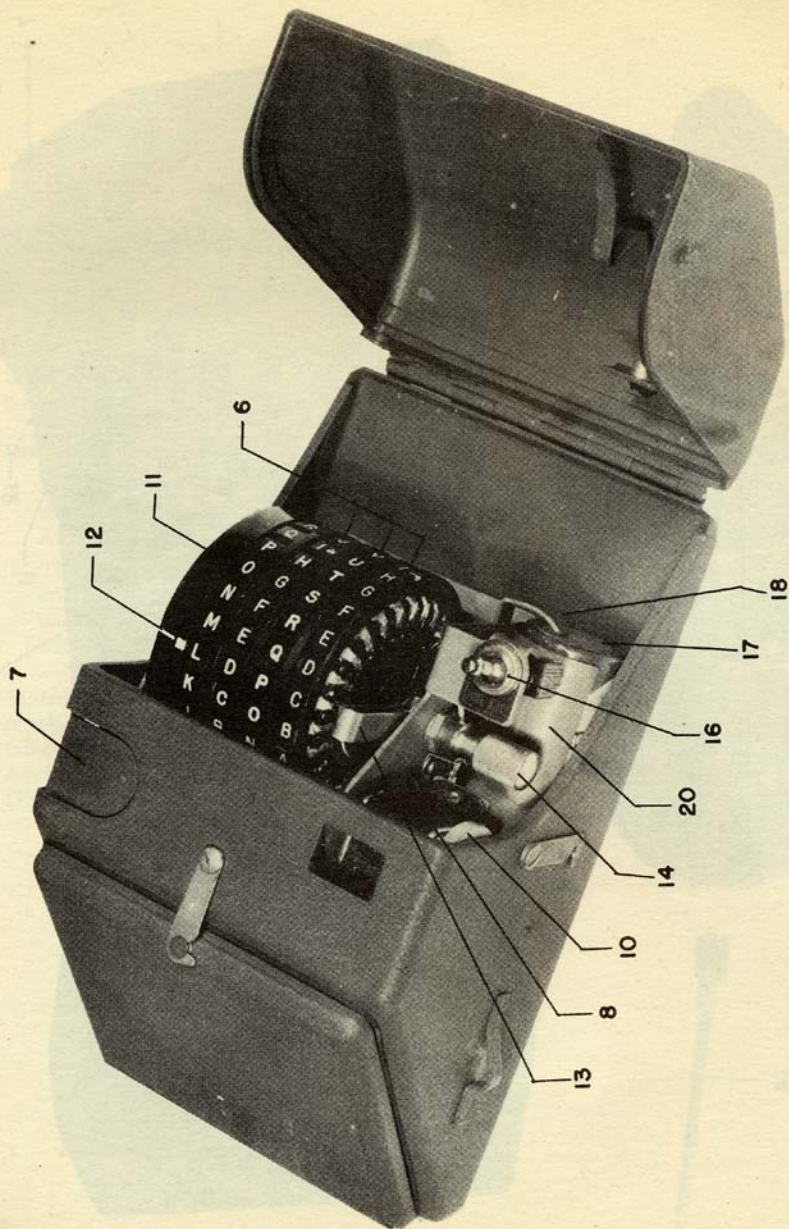
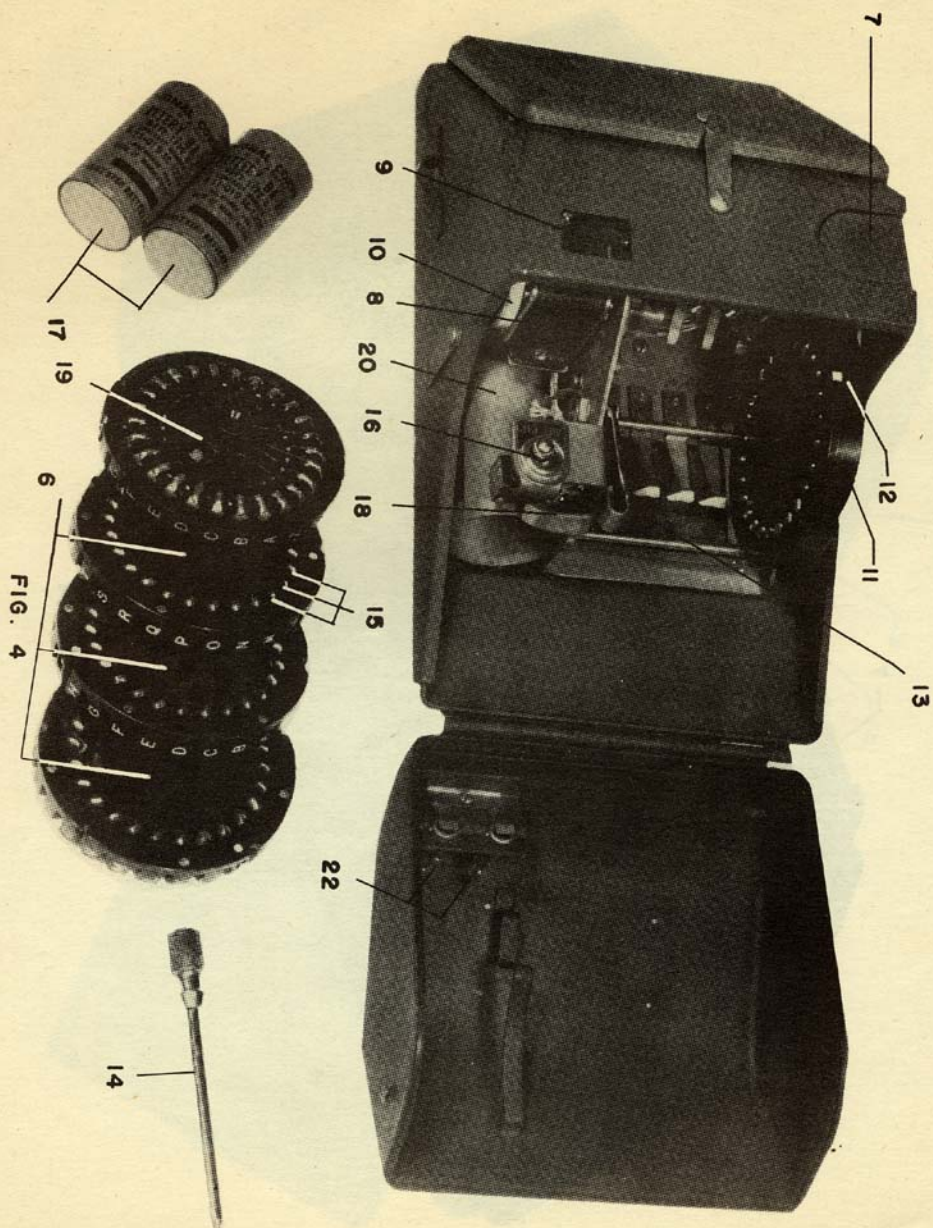


FIG. 3

RESTRICTED



RESTRICTED

SECTION I

GENERAL

	<i>Paragraph</i>
Title and Purpose.....	1
Distribution and Use.....	2
Maintenance of Converter M-325(T).....	3

1. **Title and Purpose.**—This publication, "Operating and Keying Instructions for Converter M-325(T)," is RESTRICTED and will be handled accordingly. It contains detailed procedure for the operation of the Converter M-325(T) and instructions for the setting of the keying elements which are employed in enciphering and deciphering messages by means of the Converter M-325(T).
2. **Distribution and Use.**
 - a. This publication is issued to all holders of the Converter M-325(T), which includes students enrolled in the Army Extension Courses in cryptology and designated Army training schools.
 - b. The Converter M-325(T) is a portable cryptograph developed for training purposes only, to illustrate the employment of electrical rotor-type machines. It will not be used for the encipherment of messages other than those cryptographed in connection with training courses and activities.
3. **Maintenance of Converter M-325(T).**—Maintenance of Converter M-325 (T) is a function and responsibility of the Army Security Agency. Any converters found to be faulty will be returned with a letter outlining the faults, to the Chief, Army Security Agency, The Pentagon, Washington 25, D. C. (Attention: Director, Extension Training Division.)

SECTION II

INITIAL INSTRUCTIONS*

	<i>Paragraph</i>
Unpacking Procedure.....	4
Operation Tests.....	5

4. Unpacking Procedure.—It is suggested that the steps given below be followed in unpacking the Converter M-325(T) so as to save time and prevent possible damage. Read the complete paragraph before attempting to follow instructions.

- a. Remove the Converter M-325(T) from its carton.
- b. Unlatch and open the front [1] and rear lid [2] assemblies.
- c. EXAMINE FOR DAMAGE IN SHIPMENT. (If damaged, notify the Director, Extension Training Division, Army Security Agency, outlining the damage, and await instructions.)
- d. Operate the rotor pressure lock [13] to the rear and downward.
- e. Remove the rotor shaft. [14]
- f. Remove the rotors and examine for damage in shipment. (If damaged, notify the Director, Extension Training Division, Army Security Agency, outlining the damage, and await instructions.)
- g. Replace the rotors in the rotor receptacle. The reversing rotor must be to the extreme right, with the wired side adjacent to the rotor pressure lock.
- h. Move the rotors slightly by hand to line up the rotor shaft holes and replace the rotor shaft.
- i. Operate the rotor pressure lock upward and to the front to lock the rotors in position.
- j. Operate all rotors one complete revolution by hand to insure freedom from binding.
- k. Operate the AUT-CIP switch [16] to the "CIP" position.
- l. Raise the battery terminal lever [18] and insert two flashlight batteries [17] (BA-30 or equivalent) in the battery container [20] in the base of the converter.
- m. Lower the battery terminal lever.

5. Operation Tests.—With the rotors arranged in the rotor receptacle according to the cryptographic date as specified in Signal Operation Instructions, the following tests will check the proper functioning of the converter. The AUT-CIP switch must be in the "CIP" position.

- a. Operate all the push buttons in any desired sequence without operating the stepping button. The lamp associated with each push button should light while the push button is held depressed. Disregard the other lamp which lights. If any lamp fails

*Definitions of terms will be found in Section III. It is recommended that this section also be read prior to unpacking the converter. Numbers in brackets refer to the explanatory markings on the four figures on pages 3-6.

to light when the associated push button is depressed, operate the stepping button and reset. If the lamp still will not light after several retests it is safe to assume that the lamp is defective. To change a defective lamp proceed as follows:

- (1) Using a screwdriver, or a coin, loosen the four keyboard panel assembly mounting screws [21] and remove the keyboard panel assembly.
 - (2) Lamp bases are of bayonet type and must be depressed in the socket and given a half turn to the left to remove. Remove the defective lamp and replace with a spare [22] taken from those furnished in the rear lid.
 - (3) Replace and refasten the keyboard panel assembly.
- b. Perform the 26-30 letter check as outlined in paragraph 14.
- c. Align all rotors to "AAAA." Set the counter at zero. Depress the stepping button and compare the alignment of the rotors with the following list:

When counter reads:

Alignment should read:

000	AAAA
005	FBAA
026	AFBA
050	YJBA
075	XOCA
100	WTDA
150	UCFA
200	SMHA
250	QWJA
300	OFLA

SECTION III

DESCRIPTION

	<i>Paragraph</i>
General Features.....	6
Rotors and Reversing Rotor.....	7
Keying Elements.....	8

6. General Features.

- a. The Converter M-325(T) is a small, compact, manually operated electromechanical device for enciphering and deciphering messages. The internal mechanism is protected by two hinged lids, one at the front [1] of the device and one at the rear¹ [2]. On each side of the case near the front are clips to which a carrying strap may be fastened. Inside the front cover there is a keyboard panel [3] on which the twenty-six letters [4] of the alphabet are arranged in normal order in four rows. Situated behind each letter is a lamp which is illuminated whenever the black push button [5] associated with it is depressed. At the same time some other lamp will be illuminated, designating the letter which is the equivalent of the letter being enciphered or deciphered. The electrical circuits employed in the encipherment and decipherment pass through a set of *rotors* [6] located to the rear of the keyboard. These rotors can be rotated to change these circuits with the encipherment or decipherment of each letter. If the rotors were to remain fixed, the resultants obtained from operation of the keyboard contacts would yield a simple monoalphabetic substitution.
- b. To the left rear of the keyboard on top of the case is located a *stepping button* [7] which is operated downward to advance the rotors. The continually changing position of the rotors produces variations in the electrical paths connecting the push buttons and the lamps.
- c. A *counter* [8] is located to the right rear of the keyboard under a window [9] on top of the case body. The counter registers each time the rotors are advanced. The counter is returned to zero by turning the reset wheel [10] attached to it toward the rear of the device.
- d. A rotor *receptacle* is located under the rear cover. The left wall of the receptacle is called the *stator*. [11] On top of the stator is a white *bench mark*. [12] The right side of the receptacle is the rotor *pressure lock*. [13] Rotors are placed in the receptacle in a vertical position and held in place by a rotor *shaft*. [14] That face of the rotor which has the spring contacts [15] extending above the surface is the face that must be to the right when the rotors are placed in the receptacle. This will happen automatically when the letters on the rotors are right side up, viewing the converter from the front.
- e. To the right of the rotor receptacle is an "AUT-CIP" *switch*. [16] This switch is to remain in the "CIP" position at all times during the enciphering or deciphering operation².

¹When opening the rear lid, exert a slight pressure downward to unfasten the latches.

²The converter is used for a different purpose when this switch is set to the "AUT" position (cf. par. 18).

f. A battery [17] of two dry cells (BA-30 or equivalent) supplies the 3-volt power to light appropriate lamps behind the keyboard panel when a push button is depressed. The battery is located beneath the "AUT-CIP" switch. The battery terminal lever [18] must be raised when inserting and removing dry cells and must be in the "down" position when operating the converter. The dry cells should be taken out of the converter if it is to be out of use for several hours or longer.

7. **Rotors and Reversing Rotors.**—Each Converter M-325(T) is provided with a set of rotors, consisting of three intermediate rotors [6] and one reversing rotor [19]. (The "intermediate" rotors are referred to herein simply as rotors.) Each of the three rotors has a space for an identifying number (in this case, "31," "32," and "33") on the periphery opposite the letter "I." These rotors are interchangeable and may be used in any of the first three rotor positions, counting from the left, in the rotor receptacle. The rotors are always placed right side up (cf. par. 4d). The reversing rotor bears no identifying number, but it is readily distinguishable from the intermediate rotors because it has open wiring on one of its face. The reversing rotor is *always* inserted in the fourth position of the rotor receptacle, counting from the left, with the exposed wiring to the right.

8. **Keying Elements.**—The Converter M-325(T) employs two keying elements as follows:

- a. A daily keying element which consists of a specific rotor arrangement.
- b. A message keying element which changes with every message or part of a multiple part message.

SECTION IV

KEYING ELEMENTS

	<i>Paragraph</i>
Daily Keying Element.....	9
Alignment and Stepping of Rotors.....	10
Message Keying Element.....	11
Indicators and Arrangement of Text.....	12

9. Daily Keying Element.

- a. The daily keying elements for the Converter M-325(T) issued in Signal Operation Instructions include the following items:

- (1) Indicator enciphering table (cf. par. 11c)
- (2) Rotor arrangement
- (3) "26-30" letter check (cf. par. 14).

The term "rotor arrangement" means the order in which the rotors are inserted in the rotor receptacle. A sample rotor arrangement table is illustrated below:

December
Daily Rotor Arrangement*

Date	Rotor Arrange- ment	26-30 Letter Check	Date	Rotor Arrange- ment	26-30 Letter Check	Date	Rotor Arrange- ment	26-30 Letter Check
1	32 31 33	CKOBU	11	32 33 31	SJTOF	21	32 31 33	CKOBU
2	33 32 31	IGLZU	12	32 31 33	CKOBU	22	33 31 32	JYKKP
3	32 33 31	SJTOF	13	31 32 33	QMWGS	23	33 32 31	IGLZU
4	31 32 33	QMWGS	14	32 33 31	SJTOF	24	32 31 33	CKOBU
5	31 33 32	RDLTK	15	31 33 32	RDLTK	25	33 31 32	JYKKP
6	33 31 32	JYKKP	16	33 31 32	JYKKP	26	31 32 33	QMWGS
7	33 32 31	IGLZU	17	31 32 33	QMWGS	27	33 32 31	IGLZU
8	31 33 32	RDLTK	18	31 33 32	RDLTK	28	32 33 31	SJTOF
9	33 31 32	JYKKP	19	32 33 31	SJTOF	29	32 31 33	CKOBU
10	31 32 33	QMWGS	20	33 32 31	IGLZU	30	31 33 32	RDLTK
						31	33 31 32	JYKKP

* The reversing rotor is not indicated but is understood to be inserted in the fourth position.

- b. Referring to the table above, the rotor arrangement for 1 December is 32 31 33. Rotor number 32 is placed at the extreme left side of the rotor receptacle. Rotor number 31 is placed to the right of number 32 and is followed by rotor number 33. The reversing rotor is inserted between the third rotor and the rotor pressure lock. The rotor shaft is then inserted in position and the pressure lock moved upward.

Move each rotor and the reversing rotor slightly to assure proper engaging of rotor notches and rotor detents¹.

- c. The pressure lock applies pressure to the rotors and insures good contact between rotors when the device is operated. When turning the rotors or the reversing rotor by hand and when enciphering (or deciphering) messages, the pressure lock should *not* be released. It must be released, however, when inserting or removing rotors. (The rotor pressure lock should be in the "up" (locked) position when closing the rear lid.)

10. Alignment and Stepping of Rotors.

- a. Alignment of the rotors and reversing rotor to any designated position is accomplished by turning the rotors by hand so that the desired letters are aligned horizontally from left to right in line with the white bench mark on the stator. The rotors may be turned in either directions; however, it is advisable to turn them in the direction of the stepping, i.e., progressing in the alphabetical sequence.
- b. Rotors are advanced, or stepped, by depressing the stepping button. The enciphering (or deciphering) process consists of two operations:
 - (1) Pressing the push button located under the letter to be enciphered (or deciphered) and recording the *other* letter which thereupon is illuminated, and
 - (2) Operating the stepping button.

This order of operation will always be followed: *First encipher (or decipher) the letter and then step the rotors.* The push button should be held down only long enough to identify the cipher (or plain-text) letter. Just a light touch on the push button will cause the proper lamps to light. Heavy pressure on a push button is not necessary.

11. **Message Keying Element.**—The rotors and reversing rotor must be set at a horizontal starting alignment before commencing encipherment of a message. This starting alignment must be made known to the deciphering clerk so that the message can be deciphered upon receipt. For reasons of cryptographic security, it is necessary to conceal, or disguise, the actual starting alignment. To accomplish this, the message keying element is divided into two components, the (external) *message indicator* and the (internal) *message rotor alignment*, which are derived as described below.

- a. *Message Indicator.*—This is a *random* group of five letters determined and selected by the operator himself, and will be different for every message enciphered in the same rotor arrangement. *This is the group transmitted as the message indicator.* The fifth letter serves no purpose other than to fill out the indicator group to the customary five letters. *Never* use, as the first four letters of the message indicator, an alignment found on the converter. *Never* use an actual or phonetic word (unless it occurs by pure chance) and *never* use any systematically selected indicator. It is essential that the message indicator be selected in a completely random manner. The message indicator is enciphered as described in the next paragraph.

- b. *Message Rotor Alignment.*

- (1) The message rotor alignment is the *enciphered* version of the message indicator. It indicates the actual alignment of the rotors and reversing rotor at the beginning of the encipherment of the message. *It is never transmitted.* The message rotor alignment is derived as follows:

¹Rotor detents are the four small springs at the bottom of the rotor receptacle that restrict the rotors to 26 equidistant positions during their rotation.

RESTRICTED

- (a) Assemble the rotors according to the arrangement for the cryptographic date
 - (b) Select, *at random*, the message indicator and record it temporarily, since it will be transmitted.
 - (c) By means of the indicator enciphering table (cf. par. 11c), encipher the first four letters of the message indicator using the four alphabets of the table successively. The resulting four letters are known as the *intermediate message indicator*. *This indicator is never transmitted.*
 - (d) Align the rotors and the reversing rotor to the intermediate message indicator.
 - (e) Encipher the letters of the intermediate message indicator. The rotors must be advanced by depressing the stepping button after each letter is enciphered.
- (2) The resulting four-letter cipher group is the *message rotor alignment*. It is the alignment at which encipherment of the message proper begins. *This indicator is never transmitted.*
- c. *Example.*—Assume the date to be 1 December.
- (1) Select a message indicator at random—for instance, LHJAC.
 - (2) Encipher the first four letters by means of the indicator enciphering table.

December

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

LHJA = OETA (intermediate indicator)

- (3) Align the rotors (arranged in the order 32 31 33 for 1 December) to OETA.
- (4) Encipher OETA (stepping the rotors after each encipherment), yielding XDUI.
- (5) Align the rotors to the resultant four cipher letters, XDUI, and begin encipherment of the message.

12. Indicators and Arrangement of Text.

- a. Every message and every part of a multiple part message will carry two indicators: a system indicator (in this case, BROWN) to identify the cryptographic system employed, and a message indicator, each of which will appear twice in every message part. The system indicator will *never* be enciphered. The *message indicator* will appear immediately preceding the first group of actual cipher text and immediately following the last group of actual cipher text. The *system indicator* immediately precedes the first appearance of the message indicator, and immediately *follows* the second appearance of the message indicator. An example is shown below.
- b. Assume a message of two parts is to be sent with the system indicator BROWN. The message indicators are LHJAC and OFHFS for the first and second parts, respectively.

RESTRICTED

The sample message illustrates the relative position of the heading, indicators, and text of the message.

CHL V PXR NR16 P 010830Z GR116 BT
(- - - - - 1 - - - - -)

THREE SEVEN TWO PARTS PART ONE
(- - 2 - -) (- - - - 3 - - -)

BROWN LHJAC TEXT
(4) (5)

LHJAC BROWN PART TWO BROWN OFHFS
(5) (4) (- 3 -) (4) (6)

..... TEXT OFHFS BROWN BT 010830Z
(6) (4)

(Signature, if present
and unenciphered.)

- (1) Heading. (For specific information, consult FM 24-8, FM 24-10, or other pertinent publications.)
 - (2) Writer's number (if present and unenciphered)
 - (3) Data concerning parts into which message has been divided
 - (4) System indicator
 - (5) Message indicator for first part
 - (6) Message indicator for second part
- c. Note that although the system indicator remains the same for the entire message, the message indicators are different for each part, so that cryptographically the parts of a single message are as dissimilar as separate messages would be.
- b. Data concerning the number of parts will be omitted in messages consisting of only one part.
- e. **CAUTION.**—A message indicator once used must not be used again for a second message or message part on the same day.

SECTION V

OPERATING PROCEDURE

	<i>Paragraph</i>
Length of Message.....	13
26-30 Letter Check.....	14
Enciphering Operations.....	15
Deciphering Operations.....	16
Correction of Errors.....	17
Authenticator-Cipher Switch.....	18

- 13. Length of Message.**—If the cryptographed text of a message will exceed 100 five-letter groups, the plain text will be divided into parts in such a way that no part will exceed this limit. Each part will be enciphered using a new message indicator, to be selected and enciphered in the manner described in paragraph 9.
- 14. 26-30 Letter Check.**—The 26-30 letter check is performed to assure correct rotor arrangement and that the rotor stepping mechanism functions correctly. This check is performed as follows:
- Arrange the rotors according to the cryptographic data.
 - Align the rotors and the reversing rotor to "AAAA."
 - Step the rotors until the counter reads "25."
 - Encipher the letter "A" five times, stepping the rotors after each encipherment. The result should agree exactly with the 26-30 letter check group in the rotor arrangement table.
- 15. Enciphering Operations.**—Accurate and secure encipherment by means of the Converter M-325(T) is dependent upon the correct employment of the keying elements and carefulness of cryptographing operations. It is advisable, therefore, to establish a definite order of steps which will be followed in setting up the keying elements and in enciphering and deciphering every message. Consulting this order of steps will insure that no item is overlooked and in the end will save much time. The sequence of steps is as follows:
- To facilitate rapid encipherment and protect against failure to step the rotors during encipherment, copy the plain-text message in five-letter groups on a work sheet. Number the first 25 letters as shown in the illustration:

5	10	15	20	25
PREVI	OUSLY	REPOR	TEDLO	CATIO
NSOFE	NEMYA	RTILL	ERYEM	PLACE
MENTS				

b. After assembling the rotors in the particular arrangement for the date as specified in Signal Operation Instructions and performing the 26-30 letter check, proceed as follows:

- (1) Select a message indicator and record it temporarily, since it will be transmitted.
- (2) Encipher the first four letters of the message indicator by means of the indicator enciphering table in Signal Operation Instructions, producing the intermediate message indicator.
- (3) Align the letters of the intermediate message indicator with the bench mark. The first rotor at the left is aligned to the first letter of the group; the second is aligned to the second letter of the group; the third rotor is aligned to the third letter of the group; and the reversing rotor is aligned to the fourth letter of the group.
- (4) Encipher the letters of the intermediate message indicator, advancing the rotors by depressing the stepping button after each letter is enciphered.
- (5) Align the resulting four-letter group (the message rotor alignment) on the rotors.
- (6) Return the counter to zero.
- (7) Encipher the first letter of the message. Find the plain-text letter on the keyboard and press the push button under it. Record as the cipher-text equivalent the other letter that is illustrated. Write the cipher letter under the plain-text letter on the work sheet.
- (8) Operate the stepping button once to advance the rotors.
- (9) Encipher the next 24 letters of the message in a similar manner, making certain the rotors are advanced after each plain-text letter is enciphered.
- (10) As a precaution against failure to step the rotors or introduction of an extra step, note the counter reading after the fifth letter of each group has been enciphered and the stepping button has been operated. The reading should be a multiple of five. The exact reading may be checked after the encipherment of every twenty-fifth letter by comparing the counter reading with the numbers previously written over every twenty-fifth letter of the text.
- (11) To save time in case an error in stepping the rotors is made and not immediately discovered, write on the work sheet the rotor alignment showing on the rotors after every twenty-fifth letter is enciphered, verifying, of course, that the alignment is correct as shown by a comparison between the counter and total letters enciphered at that point.
- (12) When the counter reading and total number of letters agree after enciphering twenty-five letters, number the next twenty-five letters and continue the encipherment. Thus:

(WIVI)				
5	10	15	20	25
PREVI	OUSLY	REPOR	TEDLO	CATIO
RNTQE	ICJZX	PNIVU	ILAWF	HIKNR
30	35	40	45	50
NSOFE	NEWYA	RTILL	ERYEM	PLACE
MENTS				

RESTRICTED

- (13) In following this plan, should an error in rotor stepping be discovered, it is necessary merely to return the rotors to the last alignment known to be correct and reencipher the remaining portion of the message from that position. When it is necessary to realign the rotors because of an error, return the counter to zero and renumber the groups of the message from the place of realignment beginning with zero, as at the beginning of the message. Cipher text which is incorrect must be erased or completely marked out on the work sheet. For example, assume an error has been discovered in the underlined group:

5	10	15	20	25
PREVI	OUSLY	REPOR	TEDLO	CATIO
RNTQE	ICJZX	PNIVU	ILAWF	HIKNR

5	10	15	20	25
~~30~~	~~38~~	~~40~~	~~48~~	~~50~~
NSOFE	NEMYA	<u>RTILL</u>	ERYEM	PLACE
~~OXSGP~~	~~LAJDN~~	~~MSQIW~~		
OXSGP	LAJDN	MSQIW	QFLYT	DAMEQ

30
MENTS

In verifying the counter reading for the total number of letters after the text has been completely enciphered, an adjustment must be made in the counter total for every case where the counter had to be reset to zero.

- Before copying the cipher text on a message blank, mark through the plain text so that it will not be copied accidentally as the cipher text. After copying the cipher text on a message blank, place the system indicator and message indicator, in that order, at the beginning of the message. At the end of the cipher text write the message indicator and the system indicator. Carefully check the message to be certain that no plain text is included in the text.
 - If the last group is incomplete, encipher an X or a Z, and, if necessary, add enough enciphered random letters to make a total of five letters in the group. The rotors should of course be advanced after the encipherment of each letter, so that the final counter reading should coincide with the total number of letters in the cipher text.
 - Rotate each rotor and the reversing rotor several (random) letter notches after finishing the message so that the alignment on the device at the end of the message will not accidentally be used for the encipherment of a subsequent message.
16. Deciphering Operations.—The sequence of steps in deciphering a message is as follows:
- Ascertain from the system indicator the cryptographic system used.
 - Assemble the rotors in the order specified in the rotor arrangement table for the appropriate cryptographic date.
 - Encipher the first four letters of the message indicator by means of the indicator enciphering table in Signal Operation Instructions.

- d. Align the rotors to the result—the intermediate indicator.
- e. Encipher the intermediate indicator. Step the rotors after each letter is enciphered.
- f. Align the rotors to the result obtained in subparagraph e above—the message rotor alignment.
- g. Return the counter to zero.
- h. Number the first twenty-five letters of the message in the manner explained in subparagraph 13a.
- i. Commencing with the first group of cipher text, decipher the first twenty-five letters of the message. Find the cipher letter on the keyboard and press the push button under it. Record as the plain-text equivalent the other letter that is illuminated.
- j. Record the rotor alignment after every twenty-five letters are deciphered. The plan described in subparagraphs 13b(10) through (13) should be followed. If an error is discovered, return to the last alignment known to be correct and again decipher the succeeding portion of the message.

17. Correction of Errors.

- a. Operational errors can be eliminated if the enciphering operator is acquainted with the more frequent cause of errors and will take precautions to prevent their occurrence. However, if they do occur the deciphering operator should be able to apply tests for and correct errors when the occasion arises.
- b. Always apply the following tests before calling for a service:
 - (1) Check the group count.
 - (2) Check the message indicator at the beginning and end of the message. If the two versions differ, try both, and combinations of letters from both versions.
- c. Suggestions for correcting the more common mistakes likely to be committed by the enciphering clerk are listed below.
 - (1) Try the rotor arrangement for the dates preceding and following the date on the message.
 - (2) Use the message indicator as the message rotor alignment. The enciphering clerk may have failed to encipher the message rotor alignment or through error may have copied the message rotor alignment on the message blank.
 - (3) Encipher the message indicator by means of the indicator enciphering table and use the result (the intermediate message indicator) as the message rotor alignment.
 - (4) Transpose adjacent letters of the message indicator and encipher. Try each version of the resulting intermediate message indicator.
 - (5) Encipher the message indicator as received. Transpose adjacent letters of the resulting intermediate indicator and try each new version.
 - (6) Transpose adjacent letters of the message rotor alignment as originally derived and try each new version.
- b. The message may yield some plain text and then become unreadable. This condition may be caused by one of the following errors. Try the corrective measures given for each error before asking for a service.

RESTRICTED

- (1) Occasionally a cipher-text group as received will consist of 4 or 6 letters. Record the rotor alignment at the point in the message just preceding the 4- or 6-letter group. If a 6-letter group appears, decipher, omitting the first letter of the group, and check for plain text. If no plain text results try dropping the other letters, one at a time, until all the possibilities have been exhausted. If a 4-letter group appears, depress the stepping button once for the missing letter and continue to decipher the message. Align the rotors to the last correct alignment before trying each test.
- (2) The enciphering clerk may fail to step the rotors after recording a cipher letter, or he may step the rotors two or more times after recording a cipher letter. After deciphering the last letter which yields plain text, *without* moving the rotors, decipher the next letter of the message. Try stepping the rotors twice at the point where plain text ends, and then continue to decipher the message.

18. Authenticator-Cipher Switch.

- a. The authenticator-cipher (AUT-CIP) switch has been incorporated into the Converter M-325(T) to provide a means of authentication affording a much higher degree of security than that imparted by the usual square tables or similar systems. This authentication system is illustrative of the possibilities of using a mechanical or mechanico-electrical means of authentication, where speed is not an essential criterion.
- b. The authentication system using the Converter M-325(T) employs *three* letters as the test elements, and the reply (or authenticator) consists of a digraph (i.e., two letters). The location of the particular letters which constitute the test elements will be specified in Signal Operation Instructions in those special cases when authentication by means of the Converter M-325(T) is applicable.
- c. The method of using this special authentication system is as follows:
 - (1) The test elements are aligned horizontally on the three rotors (reading from left to right), in line with the white bench mark on the stator. The rotors of course are arranged for the cryptographic date, according to Signal Operation Instructions.
 - (2) The *first* letter of the authentication is derived by aligning a *random* letter on the reversing rotor in line with the three letters of the test elements on the three rotors.
 - (3) With the AUT-CIP switch in the "AUT" position, the stepping button is depressed just once and held in that position. During this operation, *one* lamp will light, without any push button having been touched. The letter associated with this lamp constitutes the *second* letter of the authenticator.
- d. Cryptographically, this method of authentication is equivalent to the encipherment of the letter "E" at one position of the rotors and reversing rotor. The lamp associated with the encipherment of the letter "E" is lit each time the stepping button is depressed. The lamp associated with the enciphered version is the only lamp that will normally light, and only during the period the stepping button is depressed. Other lamps will light if any other push button is depressed.