

WAR DEPARTMENT  
WASHINGTON

**OPERATING INSTRUCTIONS**  
**FOR**  
**COMBINED CIPHER MACHINES**

(Short Title of this Document: SIGDUBN-1)

This publication consists of  
8 numbered pages and  
Change 1 to SIGDUBN-1,  
which consists of pages i to vi  
Verify upon receipt.

(Change 1 to SIGDUBN-1, 11 Feb 46)

Cut here

EFFECTIVE UPON RECEIPT

PAGE CHECKED  
18 OCT 1966 *Bw*

**SECRET**

**SIGDUBN-1**

Reports of possession, transfer, or destruction of this document will be forwarded as unclassified correspondence, listing the document by short title and register number only, to one of the following, whichever is applicable: (A) the Chief Signal Officer, Room 3C340, The Pentagon, Washington 25, D. C., Attention: SPSIC; (B) the Signal Officer of the theater or major command headquarters which has been authorized by the Chief Signal Officer to act as suboffice of record for this document in accordance with existing procedures. Reports of loss or compromise will be made in accordance with the provisions of AR 380-5. Instructions for the ultimate disposal of this document will be issued at an appropriate time by the Chief Signal Officer.

SECRET

SIGDUBN-1

WAR DEPARTMENT,  
Washington 25, D. C.,  
13 March 1945.

1. This document, "Operating Instructions for Combined Cipher Machines" (short title: SIGDUBN-1), is published for the information and guidance of all concerned.

2. Comments or recommendations concerning the instructions contained in this document are invited and may be submitted to the Chief Signal Officer, Room 3C340, The Pentagon, Washington 25, D. C., Attention: SPSIS-8A. Direct communication for this purpose is authorized.

AG 311.5 (23 Dec 44) OB-S-B

BY ORDER OF THE SECRETARY OF WAR:

G. C. MARSHALL,  
*Chief of Staff.*

OFFICIAL:

J. A. ULIO,  
*Major General,*  
*The Adjutant General.*

# SECRET

## TABLE OF CONTENTS

	<i>Paragraphs</i>	<i>Pages</i>
Section I. General.....	1-4	3-4
II. Description.....	5-6	4
III. Operating procedure.....	7-14	4-8
Appendix A. Special enciphering and editing requirements.....	1-3	i-iii
B. Paraphrasing and handling and transmission of plain text.....	4-6	iii-vi

(Change 1 to SIGDUBN-1, 11 Feb 46)

### SECTION I

#### GENERAL

	<i>Paragraph</i>
Title and purpose.....	1
Distribution.....	2
Reports and ultimate disposal.....	3
Effective date.....	4

#### 1. Title and purpose.

- a. This publication, "Operating Instructions for Combined Cipher Machines" (short title: SIGDUBN-1), is SECRET and will be handled accordingly. It contains instructions for the operation of combined cipher machines used by the Army: Converter M-134-C (short title: SIGABA) with special cipher unit SIGAMUG,\* and Combined Cipher Machine Mark II (Navy short title: CSP 1700). The document "Keying Instructions for Converter M-134-C" (short title: SIGQZF) contains detailed instructions for the operation of the converter with standard cipher unit SIGIVI. The document "Operating and Maintenance Instructions for Converter M-134-C" (short title: SIGKKK-1) contains detailed instructions relative to mechanical functioning and maintenance of the converter.
- b. No Army personnel will attempt to operate Converter M-134-C with SIGAMUG or CCM Mark II until they have read and thoroughly understand this publication.

2. **Distribution.**—This publication is issued to all Army holders of cryptographic systems employing Converter M-134-C with SIGAMUG or CCM Mark II.

3. **Reports and ultimate disposal.**—Reports of possession, transfer, or destruction of this document will be forwarded as unclassified correspondence, listing the document by short title and register number only, to one of the following, whichever is applicable: (A) the Chief Signal Officer, Room 3C340, The Pentagon, Washington 25, D. C., Attention: SPSIC; or (B) the Signal Officer of the theater or major command headquarters which has been authorized by the Chief Signal Officer to act as suboffice of record for this document in accordance with existing procedures. Reports of loss or compromise will be made in accordance with the provisions of AR 380-5. Instructions for the ultimate disposal of this document will be issued at an appropriate time by the Chief Signal Officer.

\*The Army short title of the special cipher unit is SIGAMUG; the Navy short title of the identical device is CSP 1600. The name plate on the device bears the Navy, but not the Army, short title; however, for purposes of accounting, Army holders will use the Army short title. Throughout this document, only the short title SIGAMUG will be employed when referring to the special cipher unit used by Army holders. Converter M-134-C with SIGAMUG is called CCM Mark I.

4. **Effective date.**—This publication is effective upon receipt and supersedes the publications “CCM MK I Operating Instructions” (short title: SIGWJFM) and “Keying and Operating Instructions for Cryptographic Systems Using the Combined Cipher Machine Mark II” (short title: SIGKAAT). One month after this publication becomes effective, SIGWJFM and SIGKAAT will be destroyed by burning and report of the destruction forwarded to the appropriate office of record.

**SECTION II**  
**DESCRIPTION**

	<i>Paragraph</i>
Combined cipher machines.....	5
Army combined cipher machines.....	6

5. **Combined cipher machines.**—In order to provide rapid and secure cryptographic communications in combined operations, combined cipher machines are used by the U. S. Army, U. S. Navy, and British forces. The combined cipher machines are:

- a. *CCM MK I.*—Converter M-134-C (short title: SIGABA) with special cipher unit SIGAMUG and Electric Cipher Machine Mark II (Navy short title: CSP 888/889) with CSP 1600.\*
- b. *CCM MK II.*—CCM Mark II (Navy short title: CSP 1700).
- c. *CCM MK III.*—TYPE X Cipher Machine with TYPE X CCM adapter.

6. **Army combined cipher machines.**

- a. *Converter M-134-C with special cipher unit SIGAMUG.*—Special cipher unit SIGAMUG is similar to the standard cipher unit SIGIVI used in normal operation of the converter and replaces SIGIVI when Converter M-134-C is used for combined communications. Rotors used in SIGAMUG are specially constructed and *are not interchangeable* with those used in SIGIVI.
- b. *CCM Mark II.*—CCM Mark II is a cryptographic device built to operate only as a combined cipher machine and is used almost exclusively by the United States and British Navies. It is used by the U. S. Army for combined communications only in special situations. CCM Mark II is similar in physical appearance and operation to Converter M-134-C but does not have a detachable cipher unit.

**SECTION III**

**OPERATING PROCEDURE**

	<i>Paragraph</i>
Rotor assembly.....	7
26-30 check.....	8
Indicators.....	9
Initial alignment.....	10
Encipherment.....	11
Long messages.....	12
Decipherment.....	13
Security rules.....	14

(Change 1 to SIGDUBN-1, 11 Feb 46)

7. **Rotor assembly.**—Special cipher unit SIGAMUG, used with Converter M-134-C, and CCM Mark II are so constructed that only five rotors of a set of ten are used at a time. Each rotor bears an identifying letter and number usually opposite the letter O.

\* Electric Cipher Machine Mark II and Converter M-134-C are identical.

A set of rotors is numbered from 0 to 9 inclusive, 10 to 19 inclusive, or 20 to 29 inclusive, etc. Key lists contain information necessary for the proper selection and arrangement of the five rotors. The assembly of the rotors changes daily. Single-digit numbers in the "rotor assembly" column of the key list refer to the units digits marked on the rotors. The number 1 indicates that rotor number 1 (or 11 or 21 or 31, etc.) is to be used; the number 5, rotor number 5 (or 15 or 25 or 35, etc.); and the number 0, rotor number 0 (or 10 or 20 or 30, etc.). The letter "R" appearing after the rotor number in the key list indicates that the rotor so designated is to be inserted in a reversed position (i. e., with the letters appearing upside down to the operator). Assembly of the rotors may be illustrated by means of an example: On 1 January the key list may show the rotor assembly to be 2 7 1 6R 0. On that date rotor number 2 (disregarding the tens digit) will be inserted in the first position on the left (as the operator faces the converter). Rotor number 7 will be inserted in the second position; rotor number 1 in the third position; rotor number 6, reversed, in the fourth position; and rotor number 0 in the last position.

8. 26-30 check.

- a. Each key list contains 26-30 check groups by which the correctness of the rotor assembly and of the stepping of the rotors is checked.
- b. The 26-30 check is accomplished in the following manner:
  - (1) Insert the rotors according to the appropriate rotor assembly given in the key list.
  - (2) Set the rotors manually to an alignment of "00000."
  - (3) Check to see that the zeroize-operate key is at "Operate."\* When SIGAMUG is used, the zeroize-operate key is kept at "Operate" for all operations.
  - (4) Turn the controller to "R" (reset) and, by means of the "Blank" key, step the rotors once. This is necessary because the Army combined cipher machines encipher (or decipher) and then step the rotors, whereas the British TYPE X Cipher Machine with TYPE X CCM adapter, which is cryptographically identical, steps the rotors and then enciphers (or deciphers). Do not set the controller at "E" (encipher) for this operation. If the controller is set at "E" the converter will be in step, but the spacing of the five-letter cipher groups will be displaced one letter.
  - (5) Turn the controller to "E" and set the stroke counter at zero.
  - (6) Press down the "Repeat" and A keys simultaneously and hold until 30 letters are printed.
  - (7) Compare the 26th to 30th letters of the resultant encipherment with the appropriate 26-30 check group in the key list. Any deviation from the check group necessitates a complete recheck of the above procedure.
- c. If the 26-30 check group is not obtained, an error in the rotor assembly, dirty contacts, or faulty mechanical operation is indicated; if the error appears to be caused by faulty mechanical operation, the converter should be checked by trained maintenance personnel.

---

\* Does not apply to CCM Mark II, which has no zeroize-operate key.

## 9. Indicators.

- a. *System indicator.*—Every message will carry a system indicator which is transmitted as the first and last groups. The system indicator identifies both the specific cryptographic system and the classification of the message. Messages classified TOP SECRET will carry the SECRET system indicator and the abbreviation TOPSEC will be buried within the message before encipherment. The key list contains the system indicators ~~to be used during the period for which it is effective.~~
- b. *Message indicators.*—Every message will carry an external message indicator from which the internal message indicator is derived.
- (1) *External message indicator.*—The external message indicator is a five-letter group transmitted as the second and next-to-last groups of the message. The letters must be selected at random and must be different for each message or message part. Bona fide words should not be used except as they occur by chance.
  - (2) *Internal message indicator.*—The internal message indicator is the five-letter group produced by the *encipherment* of the external message indicator and is used as the rotor alignment for encipherment or decipherment of the message. *The internal message indicator must never be transmitted.*
- c. *Example.*—The following example illustrates the position of the indicators and of the text in an enciphered message.

PABOC MLRXB—————TEXT—————MLRXB PABOC

                  └──EXTERNAL MESSAGE INDICATOR──┘

                                  └──SYSTEM INDICATOR──┘

10. *Initial alignment.*—Daily initial alignments are given in the key list for SECRET, CONFIDENTIAL, and RESTRICTED classifications. The initial alignment determines the setting of the first four rotors for the encipherment of the external message indicator. The initial alignment for SECRET messages will be used for messages classified TOP SECRET.

## 11. Encipherment.

- a. Prepare the converter for operation in accordance with paragraphs 7 and 8 above, referring to the appropriate rotor assembly and 26–30 check group in the key list.
- b. Select five letters at random to form the *external message indicator* (see paragraph 9b above). For purposes of reference, make a note of the letters selected.
- c. Select the appropriate daily initial alignment, according to the classification of the message, and set the first four rotors to the white reference mark in accordance with the designated letters. (If the initial alignment in the key list has five letters, disregard the last letter.) *Set the fifth (right hand) rotor to the position designated by the fifth letter of the external message indicator.*
- d. Check to see that the zeroize-operate key is at “Operate.”
- e. Turn the controller to “R” and, by means of the “Blank” key, step the rotors once.
- f. Turn the controller to “E” and type (encipher) the external message indicator (the five-letter group selected at random in subparagraph b above). *This encipherment*



produces the internal message indicator. Tear off the tape on which the internal message indicator is printed.

- g. Align the rotors to the *internal message indicator*.
- h. Turn the controller to "P" (plain text). Type the message heading, and space several times. Type the system indicator and the external message indicator.
- i. Turn the controller to "R" and, by means of the "Blank" key, step the rotors once.
- j. Turn the controller to "E" and set the stroke counter at zero. Type the text to be enciphered, employing *variable spacing* as prescribed in paragraph 2 of Appendix A; spell out numerals and punctuation marks. *Prior to encipherment, the message must have been bisected or padded in accordance with instructions contained in paragraph 1 of Appendix A.* The enciphered text will appear on the tape in groups of five letters. If the last group of the cipher text does not contain five letters, strike the space bar once and then type enough *different* nulls (random letters, with no repetitions) to complete the group. (Change 1 to SIGDUBN-1, 11 Feb 46)
- k. Turn the controller to "P" and type the external message indicator and the system indicator.
- l. Press the right tape release marked "PRESS" and withdraw the tape until all printing has cleared the tape chute. Tear off the tape.

12. Long messages.—If the cryptographed text of a message will exceed 200 five-letter groups, the plain text must be divided into two or more approximately equal lengths, so that no part will exceed 200 cipher-text groups. For each part a new external message indicator will be selected. The system indicator and external message indicator are transmitted at the beginning and end of each part.

(Change 1 to SIGDUBN-1, 11 Feb 46)

### 13. Decipherment.

- a. Prepare the converter for operation in accordance with paragraphs 7 and 8 above, referring to the appropriate rotor assembly and 26-30 check group in the key list designated by the system indicator.



- b. Set the first four rotors to the white reference mark in accordance with the letters designated by the appropriate daily initial alignment in the key list. (If the initial alignment in the key list has five letters, disregard the last letter.) *Set the fifth rotor to the position designated by the fifth letter of the external message indicator.*
- c. Check to see that the zeroize-operate key is at "Operate."
- d. Turn the controller to "R" and, by means of the "Blank" key, step the rotors once.
- e. Turn the controller to "E" and type the external message indicator. This encipherment produces the internal message indicator. Tear off the tape.
- f. Align the rotors to the internal message indicator.
- g. Turn the controller to "P" and type any plain text which appears at the beginning of the message.
- h. Turn the controller to "R" and, by means of the "Blank" key, step the rotors once.

- i. Turn the controller to "D" (decipher), set the stroke counter at zero, and type (decipher) the text of the message. *The plain text will appear on the tape with variable spacing.*
- j. Press the right tape release marked "PRESS" and withdraw the tape until all printing has cleared the tape chute. Tear off the tape. *Before delivery to the addressee, every message will be edited as prescribed in paragraph 3 of Appendix A.*

(Change 1 to SIGDUBN-1, 11 Feb 46)

14. Security rules.—The following rules must be followed closely to protect the security of the system:

- a. The *internal* message indicator, produced by the encipherment of the external message indicator, will never be transmitted.
- b. *Enciphered* nulls (random letters) will be used when it is necessary to complete the final cipher group of a message or message part.
- c. A different external message indicator will be selected *at random* for each message or message part.
- d. The plain text of a message will be divided into two or more approximately equal parts if the cryptographed text will exceed 200 five-letter cipher groups. No part will exceed 200 five-letter groups.

# SECRET

## APPENDIX A

### SPECIAL ENCIPHERING AND EDITING REQUIREMENTS

	<i>Paragraph</i>
Bisection and padding .....	1
Variable spacing .....	2
Editing of messages .....	3

1. **Bisection and padding.**—Messages enciphered by means of a combined cipher machine will be treated as follows in the code room:

a. All messages that will contain 50 or more letters of cipher text (exclusive of indicators) will be bisected. If the message is to be transmitted as a single message, the bisection will be performed once regardless of the number of cryptographic parts; if the cryptographic parts of a message are to be transmitted separately, bisection will be applied to each part separately. The bisection instructions below will be followed.

- (1) *Division of message.*—Divide the plain text of a message at any point between words which are not stereotyped, thus separating the text into two segments. Choose the point of division at random. It should not, however, be chosen between sentences, paragraphs, or numbers; and it should not habitually be near the beginning, end, or middle of the text.

*Example:*

REQUEST FULL INFORMATION CLARIFYING YOUR  
RECOMMENDATION RE REVISION OF // CODE ROOM  
PROCEDURE FOR LARGE HEADQUARTERS

**CAUTION:** Do not mark the point of division on the originator's copy.

- (2) *Consonant group.*—Select at random any consonant except X or Z. Repeat the consonant to make a five-letter group, and place this group at the end of the second segment.
- (3) *Transposing.*—Transpose the two segments of the message, placing the second segment first, followed by the five-letter group, and the first segment last, so that the message will be cryptographed in the following order: (1) SECOND SEGMENT; (2) FIVE-LETTER GROUP; (3) FIRST SEGMENT. With R as the repeated consonant, the plain text of the example in subparagraph (1) would read as follows:

CODE ROOM PROCEDURE FOR LARGE HEADQUARTERS  
RRRRR REQUEST FULL INFORMATION CLARIFYING  
YOUR RECOMMENDATION RE REVISION OF

**NOTE:** If most or all of the words in a message are stereotyped, divide the message *within* a word. Do not divide a word so that: (1) only one letter occurs

on either side of the division; (2) letters comprising a stereotype occur on either side of the division. After the segments are transposed, following the portion of the word at the beginning of the message insert the abbreviation RPT followed by the whole word. An example of a message split within the word EIGHT follows:

HT RPT EIGHT RECEIVED GGGGG SHIPMENT FOUR ONE EIG

b. Messages that will contain fewer than 50 letters of cipher text will not be bisected, but will be padded to increase the over-all length to 50 or more letters of cipher text. Padding will be applied as outlined below.

- (1) Add words for padding at both the beginning and the end of the message. CAUTION: Do not write these words on the originator's copy.
- (2) Select words for padding according to the following instructions:
  - (a) Care will be taken to avoid the use of any word which could be interpreted as having any relation to the text of the message.
  - (b) Words used at the beginning will bear no relation to words used at the end. For example, such beginnings and endings as the following will not be employed: "trolley . . . . car," "Chicago . . . . Illinois."
  - (c) The types of words used for padding will vary from message to message and within a single message. Names of cities, flowers, fruits, etc., will not habitually be used.
  - (d) Care will be taken that the words selected for padding do not become stereotyped. It is suggested that lists of randomly chosen words of varying lengths be prepared and check-off methods used to prevent repetitions of words. A dictionary may be used for this purpose as long as the words are chosen at random.
- (3) Vary the total amount of padding used from message to message; within a single message vary the amount of padding used at the beginning from that used at the end. Do not attempt to limit the length of each message to exactly 50 letters; vary the length from message to message.
- (4) Separate the padding from the beginning and from the end of a message by the insertion of any doubled consonant except X and Z. Do not use the same doubled consonant at both the beginning and the end of a message.
- (5) An example of the use of padding follows:

*Padding*  
FLY SALT HH DETAILS NOT YET AVAILABLE REUR THREE

*Padding*  
ONE CC DISK JAIL CUE

NOTE: While the use of phrases as padding is not prohibited, the use of unrelated words is more desirable. If phrases are used, the phrase at the beginning will bear no relation to that at the end of the message. For example, such beginning and endings as the following will not be employed: "Little Jack Horner . . . . sat in a corner," "Spare the rod . . . . and spoil the child."

2. **Variable spacing.**—*Every message* enciphered by means of a combined cipher machine will be variably spaced upon encipherment, in addition to being bisected or padded as prescribed above. Variable spacing will be accomplished as follows: At occasional intervals throughout the text, the operator will eliminate the space between adjacent words by not striking the space bar of the converter. This should be done near the beginning of the encipherment and at random intervals thereafter. For each 100 groups of cipher text a minimum of six and a maximum of fifteen eliminations will be effected. A space will not be eliminated between digits of a number if local rules at the enciphering headquarters prohibit running together the digits of a number.
3. **Editing of messages.**—Before delivery to the addressee, every message enciphered by means of a combined cipher machine must be edited by authorized U. S. or British personnel, as follows:
  - a. Restore the message to normal order and delete the five-letter group if bisection was applied.
  - b. Delete padding if padding was applied.
  - c. Replace all eliminated spaces.
  - d. Remove internal addresses and signatures from the body of the message.
  - e. Delete the phrase CRYPTO SECURITY APPLIES if it appears in the message.
  - f. Delete any nulls which may have been added at the end of the message.
  - g. Correct errors in the text.

Appropriate measures will be taken to safeguard the unedited copy.

## APPENDIX B

### PARAPHRASING AND HANDLING AND TRANSMISSION OF PLAIN TEXT

	<i>Paragraph</i>
Recryptographing .....	4
Plain-text copies of messages .....	5
Indication of normal paraphrasing requirements for plain-text copies of messages ...	6

4. **Recryptographing.**—The following rules will be observed by U. S. Army personnel when using a combined cipher machine:
  - a. Paraphrasing is *not* required:
    - (1) When a message enciphered in a system employing a combined cipher machine is re-enciphered in the same system or in another system employing a combined cipher machine, except as provided below. (However, a new external message indicator must always be selected.)
  - b. Paraphrasing is *required*:
    - (1) When a message enciphered in a combined or limited combined\* system employing a combined cipher machine has been or is to be cryptographed in any system other than one employing a combined cipher machine, Converter M-134-C,\*\* one-time tapes, or literal or numerical one-time pads.\*\*\*

\* Throughout the remainder of paragraph 4 and paragraphs 5 and 6 the term "combined" includes "limited combined" systems and "full combined" systems.

\*\* Converter M-134-C refers to Converter M-134-C with SIGIVI, throughout paragraphs 4, 5, and 6.

\*\*\* In addition to the systems named, exception is also made in the case of any other system when War Department instructions for the system contain provisions similar to those in paragraph 5 of this appendix.

- (2) When a message enciphered in any system employing a combined cipher machine, Converter M-134-C, one-time tapes, or literal or numerical one-time pads\*\*\* is re-enciphered in a combined system employing a combined cipher machine *unless* the message as originally enciphered contained the phrase CRYPTO SECURITY APPLIES. (See par. 6.)
- (3) When a message enciphered in a combined system employing a combined cipher machine is re-enciphered in any system employing a combined cipher machine, Converter M-134-C, one-time tapes, or literal or numerical one-time pads\*\*\* *unless* it is known that the re-enciphered message will be further re-encrypted by the receiving headquarters in a system not employing a combined cipher machine, Converter M-134-C, one-time tapes, or literal or numerical one-time pads.\*\*\*
- (4) When a message enciphered by a combined cipher machine in a system other than a combined system is re-enciphered in any combined system *unless* the message as originally enciphered contained the phrase CRYPTO SECURITY APPLIES.
- (5) When a message enciphered in any combined system is re-enciphered by a combined cipher machine in a system other than a combined system *unless* it is known that the re-enciphered message will be further re-encrypted by the receiving headquarters in a system not employing a combined cipher machine, Converter M-134-C, one-time tapes, or literal or numerical one-time pads.\*\*\*
- (2) When a message enciphered in a system employing a combined cipher machine, Converter M-134-C, one-time tapes, or literal or numerical one-time pads\*\*\* is re-enciphered in a combined system employing a combined cipher machine *if* the message as originally enciphered contained the phrase CRYPTO SECURITY APPLIES.
- (3) When a message enciphered in a combined system employing a combined cipher machine is re-enciphered in a system employing a combined cipher machine, Converter M-134-C, one-time tapes, or literal or numerical one-time pads\*\*\* *if* it is known that the re-enciphered message will be further re-encrypted by the receiving headquarters in a system not employing a combined cipher machine, Converter M-134-C, one-time tapes, or literal or numerical one-time pads.\*\*\*
- (4) When a message enciphered by a combined cipher machine in a system other than a combined system is re-enciphered in any combined system *if* the message as originally enciphered contained the phrase CRYPTO SECURITY APPLIES.
- (5) When a message enciphered in any combined system is re-enciphered by a combined cipher machine in a system other than a combined system *if* it is known that the re-enciphered message will be further re-encrypted by the receiving headquarters in a system not employing a combined cipher machine, Converter M-134-C, one-time tapes, or literal or numerical one-time pads.\*\*\*

---

\*\*\* See footnote, page iii.



- (6) When a message enciphered by a combined cipher machine in a system other than a combined system has been or is to be cryptographed in any U. S. system (intra-Army or joint Army-Navy).
  - c. External linkage of different encipherments of the same message is not permitted.
  - d. When a message enciphered in any system employing a combined cipher machine is re-enciphered in a system employing Converter M-134-C, and when a message enciphered in a system employing Converter M-134-C is re-enciphered in any system employing a combined cipher machine, the point of bisection and the consonant group, or the amount and type of words used for padding, and the variable spacing will be completely different for each encipherment.
5. **Plain-Text Copies of Messages.**—Except as provided in paragraph 6 below, plain-text copies of combined cipher machine messages may be handled and transmitted in unparaphrased form.
- a. They may be sent by any means, provided regulations are followed governing the handling and transmission of correspondence of the same classification as that of the message.
  - b. They will be marked substantially as follows: "Handling and transmission of literal plain text of this message as correspondence of the same classification has been authorized by the War Department in accordance with the provisions of paragraphs 44g and 53a(3) (Changes No. 3), AR 380-5, 15 March 1944."
  - c. They may be released without paraphrasing to nonmilitary agencies, Allied Governments, or any other agencies or persons, when such agencies, governments, or persons are specifically authorized to receive the classified information therein, provided that the plain text which is so released does not contain information or references which would associate it with the plain text or cryptographed text of any message not marked as indicated in subparagraph *b* above.
  - d. If the information in the message becomes unclassified, the information may be released to the general public without paraphrasing, provided that the plain text so released does not contain information or references which would associate it with the plain text or cryptographed text of any message not marked as indicated in subparagraph *b* above.

**CAUTION:** If through error a message enciphered by means of a combined cipher machine has *not* been variably spaced and bisected or padded, normal requirements for paraphrasing will be observed in handling and transmitting plain-text copies of the message. Plain-text copies of such messages will be marked to indicate that paraphrasing and all other security safeguards must be afforded the message.

6. **Indication of Normal Paraphrasing Requirements for Plain-Text Copies of Messages.**—If a message enciphered by a combined cipher machine in a system other than a combined system has been cryptographed, is simultaneously cryptographed, or is to be recryptographed in some system other than one employing a combined cipher

machine, Converter M-134-C, one-time tapes, or literal or numerical one-time pads,\*\*\* the phrase CRYPTO SECURITY APPLIES will be inserted in the body of the message when it is enciphered by the combined cipher machine in the system which is not a combined system. This phrase will indicate that normal requirements for paraphrasing will be observed in handling and transmitting plain-text copies of the message. However, this phrase will be deleted before the plain text of the message is delivered to the addressee. Plain-text copies of such messages will be marked to indicate that paraphrasing and all other security safeguards must be afforded the message.

NOTE: The phrase CRYPTO SECURITY APPLIES will never be included in a message when it is enciphered in a *combined* system employing a combined cipher machine.

---

\*\*\* See footnote, page iii.