Operating Instructions for ASAM 1 (a.k.a. ECM Mark II)

Kind readers,

Below is a replica of the instructions for operating the ECM Mark II as written by the Army in 1949. The manual has be input using optical character recognition followed by reformatting to network format (HTML.)

Also see CSP-1100 ECM Instructions from 1944.

By 1949 the designation of the ECM Mark II by the Army was ASAM 1/1. The names of several of its parts were renamed as well, but these are generally obvious in their use. The normal keying shown here is essentially compatible with the final wartime keying. The emergency keying is not the same, during the war a CSP-890 was carried that was used for emergency keying.

Rich Pekelney, Webmaster

CONFIDENTIAL Reg. No. 30

Registered Cryptodocument

DEPARTMENT OF THE ARMY
WASHINGTON

ASAM 1/1

CRYPTO-OPERATING INSTRUCTIONS
FOR
ASAM 1

This document consists of
27 numbered pages
and cover

Verify upon receipt

1

ASAM 1/1

DEPARTMENT OF THE ARMY
Washington 25, D. C.
1 October 1949

1. This document, ASAM 1/1, "Crypto-operating Instructions for ASAM 1," is published for the information and guidance of all concerned.

2. Comments or recommendations concerning the instructions contained herein are invited and may be submitted to the Chief, Army Security Agency, The Pentagon, Washington 25, D. C., Attn: CSGAS-83. Direct communication for this purpose is authorized.

(AG 311.5 (30 Oct 43) OB-S-B)

BY ORDER OF THE SECRETARY OF THE ARMY:

OMAR N. BRADLEY
Chief of Staff

OFFICIAL:

EDWARD F. WITSELL
Major General

RECORD OF CHANGES

Change No.	Date Entered	Entered By
1	1 Nov 1949	M. Fishbow

(BLANK)

TABLE OF CONTENTS

CRYPTO-OPERATING INSTRUCTIONS FOR ASAM 1
SECTION I
GENERAL

1. Introduction.

a. This document, ASAM 1/1, "Crypto-operating Instructions for ASAM 1," is CONFIDENTIAL and registered, and will be handled accordingly. It contains basic instructions for the operation of ASAM 1, formerly Converter M-134-C (short title: SIGABA). Cryptosystems employing ASAM 1 are Category A.

b. Instructions concerning the processing of classified messages in a cryptocenter and information regarding general cryptographic procedures are contained in the document ASAG 2, "Cryptographic Operations."

c. No persons will be permitted to operate ASAM 1 unless they have been properly cleared for cryptographic duties in accordance with the provisions of current directives and have either read this document and ASAG 2 or been instructed by authorized personnel.

d. The document SIGKKK-2 should be consulted for detailed information relative to maintenance and power requirements of the machine and identification of mechanical parts.

2. Distribution.-This document is issued to holders of cryptosystems employing ASAM 1 with ASAM 1A as designated by the Department of the Army.

3. Accounting and Disposal.-Reports of possession, transfer, or destruction of this document will be forwarded as RESTRICTED correspondence, listing the document by the title ASAM 1/1 and register number only, to one of the following, whichever is applicable: (A) the Chief, Army Security Agency, The Pentagon, Washington 25, D. C., Attn: CSGAS-82, (B) the Chief, Army Security Agency, Europe, Pacific, or Hawaii, or (C) the Signal Officer of the major command headquarters which has been

authorized by the Chief, Army Security Agency, Department of the Army, to act as command issuing office for this document in accordance with existing procedures Reports of loss or compromise will be made in accordance with the provisions of Chapter Five of the document ASAG 2. Instructions for the eventual disposal of this document will be issued at an appropriate time by the Chief, Army Security Agency, Washington D. C.

4. Effective Date.-This document is effective 1 October 1949 and at that time supersedes "Crypto-operating Instructions for Converter M-134-C" (short title: SIGQZF-3). One month after the effective date of this publication, SIGQZF-3 will be destroyed by burning and report of the destruction forwarded to the appropriate office of issue.

SECTION II

DESCRIPTION

5. Description and Use.-ASAM 1 is an electromechanical, transportable cipher machine to be used for automatically enciphering and deciphering messages, both tactical and administrative, with speed, accuracy, and security. The machine is CONFIDENTIAL and registered.

6. Component Parts.-The operator is directly concerned with the following component parts.

a. The keyboard resembles a typewriter keyboard and can be operated at a maximum speed of 45 to 50 words per minute (40 words per minute in tandem operation); if this speed is exceeded, characters may fail to print. The keyboard consists of 26 alphabet keys, 10 numeral keys, a "Repeat" key, a "Blank" key, a "Dash" key, a space bar and a dummy key. The "Blank" key permits advancing of the rotors without causing any resultant to be printed. The

"Repeat" key permits continuous operation of the machine with or without printing.

b. The positions of the controller and their effect on the operation of the machine are as follows:

(1) *Off Position* ("O").-The power supply line is open and no current is supplied to the machine.

(2) *Plain-text Position* ("P").-All keys of the keyboard (except the dummy key) and the space bar are operative, and the machine will print plain text exactly as typed. The rotors remain motionless during typing.

(3) *Reset Position* ("R").-Only the numeral keys 1 to 5, inclusive, and the "Blank" and "Repeat" keys are operative. The rotors may be zeroized with the controller in this position and the zeroize-operate key in the "Zeroize" position (see par. 12a(3)). The tape will not feed while the controller is at "R." When the controller is moved to or through the "R" position, the tape-feed ratchet resets so that printing will begin on the first letter of a five-letter cipher group. Therefore, the tape may advance as many as five spaces.

(4) *EnCipher Position* ("E").-The alphabet, "Blank," and "Repeat" keys and the space bar are operative. Numeral and "Dash" keys are inoperative. The machine enciphers the letters struck on the keyboard and prints then resulting cipher text.

(5) *Decipher Position* ("D").-The alphabet, "Blank," and "Repeat" keys are operative. Numeral and "Dash" keys and the space bar are inoperative. The machine deciphers the letters struck on the keyboard and prints the resulting plain text.

---

c. The key located on the left front of the machine is the zeroize-operate key. The key is positioned at "Zeroize". when it is desired to align automatically all alphabet and stepping control rotors to the letter "0." The key is positioned at "Operate " at all other times.

d. The cipher unit ASAM 1A is detachable and consists of six upright bakelite separators which form a support for three rotor shafts. The unit supports the index, stepping control, and alphabet rotors in such relative positions that electrical circuits are formed through each row of rotors. The cipher unit, exclusive of rotors, is CONFIDENTIAL and registered.

e The cipher unit ASAM lB is detachable and consists of six upright bakelite separators which form a support for one rotor shaft. Positions for five rotors are thus provided. The cipher unit, exclusive of rotors, is CONFIDENTIAL and registered; Instructions for the operation of ASAM 1 with cipher unit ASAM lB are contained in ASAM 5/1, "Crypto-operating Instructions for ASAM 5." The ASAM 1 with ASAM lB is referred to as the

Combined Cipher Machine.

7. Rotors.

a. Sets of ten large rotors are issued for use with cryptosystems employing ASAM 1. The rotors are SECRET and registered. Each set of rotors is identified by a title and a number. In addition, each rotor is identified as belonging to a specific series by means of a letter-number pattern stamped on the rotor, usually opposite the letter "0." The pattern consists of any letter or any two-letter combination plus the numbers 1-10, 11-20, 21-30, etc. Each rotor bears a complete alphabet engraved in normal sequence on its periphery. The large rotors are all interchangeable and reversible.

(1) Five rotors are arranged in the middle row of the cipher unit and are known as the stepping control rotors. The two end rotors remain stationary during encipherment and decipherment.

(2) Five rotors are arranged in the rear row of the cipher unit and are known as they alphabet rotors. All five rotors advance in an irregular manner during encipherment and decipherment.

b. The five small rotors positioned in the front row of the cipher unit are known as index rotors. These rotors are a permanent part of the cipher unit and can be moved manually only. Each of the index rotors bears engraved on its periphery a sequence of numbers. One rotor is marked with the sequence 10 to 19 inclusive; another, the sequence 20 to 29 inclusive, etc. The complete set of five index rotors is numbered from 10 to 59 inclusive. The index rotors are always used in a fixed order in the five rotor positions (10-19, 20-29, 30-39, etc.). The index rotors are classified CONFIDENTIAL.

8. Power Requirements.-The machine is normally operated from a 105-125-volt a. c. (50 or 60 cycle) or d.c., power supply. Interchangeable motors are provided to utilize either type of power.

SECTION III
KEYING INSTRUCTIONS

9. Key List.-A key list, prepared in monthly editions and containing data essential to operation of ASAM 1, is used with each cryptosystem. The key list contains the following information:

a. Arrangement of the stepping control and alphabet rotors for each day of the month.

b. Alignment of index rotors for SECRET, CONFIDENTIAL, and RESTRICTED messages for each day of the month.

c. 26-30 check groups for SECRET, CONFIDENTIAL, and RESTRICTED classifications.

d. System indicators for SECRET, CONFIDENTIAL, and RESTRICTED messages.

Day of Month	ROTOR ARRANGEMENT (for all classifications)		SECRET	
	Stepping Control (Middle)	Alphabet (Rear)	Index(Front) Alignment	26-30 Check Group
1	0R 4 6 2R 7	1 8 5 9 3R	10 23 31 49 5	R N H V C
2	2 3R 9R 1 5	6 4R 8 7 0	14 25 33 46 59	S E M N O

Figure 1.-Sample Key List

Day of Month	CONFIDENTIAL		RESTRICTED	
	Index(Front) Alignment	26-30 Check Group	Index(Front) Alignment	26-30 Check Group
1	12 28 31 44 53	P W V M T	17 25 36 43 58	M C S D T
2	15 20 32 48 56	E H E W B	10 27 34 42 56	R S T H H

Figure 2.-Sample Key List

---

10. Rotor Arrangement.-The ten rotors used each day are arranged in the middle and rear positions of the cipher unit in accordance with the key list applicable to the cryptosystem.

(See sample key list in fig. 1.) Single-digit numbers in the ROTOR ARRANGMENT column of the key list refer to the units digit of the number on the periphery of the rotors. The number 1 indicates that rotor number 1 (or 11 or 21, etc.) is to be used; the number 5, rotor number 5 (or 15, or 25, or 35, etc.); the number 0, rotor number 10 (or 20, or 30, etc.). The letter "R" appearing after a 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 on the rotor appearing upside down to the operator as he faces the machine. Arrangement of the rotors may be illustrated by means of an example: In the sample key list, the rotor arrangement for the 2d of the month is 2 3R 9R 1 5 for the stepping control rotors and 6 4R 8 7 0 for the alphabet rotors. Rotors marked 2, 3, 9, 1, and 5 (disregarding the tens digits) will be inserted in the control position in that order, from left to right, as the operator face the converter, with rotors number 3 and 9 reversed. The remaining five rotors marked 6, 4, 8, 7, and 0 will be inserted in the alphabet position in that order from left to right, with rotor number 4 reversed.

CAUTION: Do not touch rotor contacts when arranging the rotors.

11. Alignment of Index Rotors.- The sets of numbers in the key list under INDEX (FRONT) ALIGNMENT designate the alignment of the index rotors. In three separate columns, each headed INDEX. (FRONT) ALIGNMENT, the key list give the daily alignment of the index rotors for each classification. The alignment of the index rotors is determined by the classification of the message and the day of the month. The index alignment for SECRET messages will also be used for messages classified TOP SECRET. Example: According to the sample key list (fig. 1), on the first day of the month the numbers of the index rotors should be aligned from left to right on the white reference mark at 10 23 31 49 50 for SECRET message; at 12 28 31 44 53 for CONFIDENTIAL messages; and at 17 25 36 43 58 for RESTRICTED messages.

12. 26-30 Check.-The key list contains 26-30 check groups by which the correctness of each rotor arrangement and index alignment and the operation of the machine are checked.

a. The 26-30 check is accomplished in the following manner:

(1) Insert the rotors according to the rotor arrangement for the specific date.
(2) Align the index rotors in accordance with the security classification and the specific date.
(3) Zeroize the rotors. This is accomplished by switching the zeroize-operate key to "Zeroize," turning the controller to "R," then pressing down the "Blank" and "Repeat" keys simultaneously until the letter "0" on each stepping control and alphabet rotor comes to rest at the reference mark.
(4) Set the stroke counter at *zero*.
(5) Switch the zeroize-operate key to "Operate" and turn the controller to "E."
(6) Press down the "Repeat" and "A" keys simultaneously and hold until 30 letters are printed.
(7) Compare the 26th through the 30th letters of the resultant encipherment with the appropriate 26-30 check group in the key list. For example, assume that the rotors of an appropriate set had been arranged and aligned in accordance

with the sample key list (fig. 2) for CONFIDENTIAL traffic for the second day of the month. . If the 26-30 check procedure is followed correctly and the machine is operating properly, the 26th, 27th, 28th, 29th, and 30th letters will be E H E W B. Any deviation from the check group in the key list necessitates a complete recheck of the above procedure.

b. If the 26-30 check cannot be obtained, an error in the rotor arrangement, dirty contacts, or faulty mechanical operation may be the cause. If it appears that the error is caused by faulty mechanical operation, the machine should be checked by trained maintenance personnel.

NOTE : Care should be exercised whenever rotors are aligned to insure that the letter to be aligned on each rotor is directly in line with the white reference mark. If a rotor is off center, i. e., aligned halfway between two letters, the machine may not operate or monoalphabetic substitution encipherment may result.

c. The 26-30 check will be accomplished :

(1) After each change of the rotor arrangement.
(2) After each change of the index alignment.
(3) Each time the cipher unit is inserted in the machine prior to encipherment or decipherment.

13. System Indicator.-System indicators are the five-letter groups indicated in the key list for SECRET, CONFIDENTIAL, and RESTRICTED classifications. The system indicator identifies the specific ASAM 1 cryptosystem used to encipher a message, the classification of the message, and thereby the rotor arrangement and index rotor alignment to be used. The SECRET system indicator will also be used for messages classified TOP SECRET. The abbreviation TOPSEC will be buried near the beginning of the plain text during encipherment. The system indicator is *never* enciphered.

14. Message Indicator.-The message indicator consists of five letters selected at random by the operator. Bona fide five-letter words will not be used as message indicators even though such words occur by chance. The message indicator will be different for each message or part. When it is necessary, as in the case of a service, to reencipher a particular message or part, or any portion thereof, a different message indicator will be selected. The message indicator is used to determine the message rotor alignment as shown in paragraph 15.

15. Message Rotor Alignment.-The alignment of the stepping control and alphabet rotors at the beginning of encipherment or decipherment constitutes the message rotor alignment. The message rotor alignment is derived by the following procedure:.

a. Select five letters at random. The five letters will be the message indicator. Letters of the alphabet in proximity to the letter "O" i.e., L, M, N, or P, Q, R, will not be deliberately or consistently selected in the message indicator merely to reduce the number of steps required to align the letters of the message indicator on the stepping control rotors as explained below.

b. Zeroize the rotors(see par. 12a(3)).

c. Leave the controller at "R" and switch the zeroize-operate key to "Operate."

d. Strike the numeral "1" key the number of times required to align the first stepping control rotor (next to the left-end plate) to the first letter of the message indicator. The first stepping control rotor will advance one letter each time the "1" key is depressed.

e. Align the second stepping control rotor by striking the numeral "2" key, the third by striking the numeral "3" key, etc., until all five stepping control rotors are aligned to the five letters of the message indicator. The alphabet rotors will advance in an irregular manner with each operation of the numeral keys.

NOTE : If the letter "0" is to be aligned on any of the five stepping control rotors, it will be necessary to advance that rotor 26 times when setting up the message indicator.

f. If any rotor is advanced past the correct letter or if the rotors are not aligned in proper sequence, the entire process must be repeated from the zeroize position. Do not use the "Repeat" key with the numeral keys in aligning the message indicator and avoid a sharp, quick touch of the numeral keys. It is possible to strike the numeral keys too quickly so that the alphabet rotors will advance but the stepping control rotors will not, thus resulting in an incorrect alignment.

g. After the stepping control rotors have been aligned, check the alignment of the alphabet rotors to insure that all five are not aligned to the letter "0." The alphabet rotors should advance in an irregular manner while the stepping control rotors are being aligned. If all of the alphabet rotors remain aligned to the letter "O" it is an indication that the machine is not functioning properly or that the procedure outlined herein has not been followed correctly.

SECTION IV
OPERATING PROCEDURE

16. Division into Parts.-If the enciphered text of a message will exceed 350 five-letter groups, the plain text will be divided into parts so that no part will exceed 350 cipher- text groups. A different message indicator will be selected for each part.

17. Sequence of Operations in Encipherment.-After the message has been divided into parts, if necessary, and bisected, it will be enciphered according to the following sequence of operations.

a. Prepare the machine for operation in accordance with paragraphs 10, 11, and 12, referring to the appropriate effective key list to determine the correct rotor arrangement, the index rotor alignment for the classification of the message, and the 26-30 check.

b. Select at random the message indicator and determine the message rotor alignment in accordance with paragraph 15.

c. With the controller at "P," type the message heading, space several times, and type the system indicator and the message indicator. Phoneticize the message indicator.

d. With the rotors aligned to the message rotor alignment, turn the controller to "E" and set the stroke counter at zero.

e. Type the message text to be enciphered, employing variable spacing. If the last group of cipher text does not contain five letters, strike the space bar once and, if necessary, type enough different letters to complete the group.

f. Turn the controller to "P" and type the system indicator.

g. Press the right tape release marked "PRESS" and withdraw the tape until all printing has cleared the tape chute. Tear off the tape.

18. Sequence of Operations in Decipherment.

a. Prepare the machine for operation in accordance with paragraphs 10, 11, and 12, referring to the effective key list as designated by the system indicator for the correct rotor arrangement, the index rotor alignment for the classification of the message, and the 26-30 check.

b. Determine the message rotor alignment in accordance with paragraph 15.

c. With the rotors aligned to the message rotor alignment, turn the controller to "D" and set the stroke counter at zero.

d. Type the cipher text of the message, exclusive of indicators. Disregard spaces between groups; the space bar is inoperative while the controller is at "D." The

plain text will be printed on the tape in normal word lengths except where variable spacing was employed in encipherment. Note that X will always be printed in the place of Z, e.g.:, ZERO will decipher as XERO, ZONE as XONE. In the event the deciphered text is garbled either from the beginning or after some plain text has been printed, attempt to determine the cause of the trouble by employing the procedure described in section VI.

e. After the cipher text has been completely deciphered, press the right tape release marked "PRESS" and withdraw the tape, until all printing has cleared the tape chute. Tear off the tape.

NOTE: Every message that has been enciphered by means of ASAM 1 will be edited and appropriately marked before delivery to the addressee.

SECTION V
SPECIAL INSTRUCTIONS

19. Hand Operation.

a. If the main power supply fails, or other circumstances make motor operation impossible, the machine can be operated by use of the hand lever. A power supply of 24 volts d. c. is needed to operate the necessary magnets. Sixteen BA-23 cells in series, or equivalent, may be used for emergency power.

b. To shift from power operation to hand operation, proceed as follows:

(1) With the main power lead disconnected, interchange the positions of the motor plug

(marked a. c. or d. c.) and the dummy plug so that the pointer of the dummy plug "24v."

(2) Raise the hand-lever pawl and slip the ring from under the pawl. Release the pawl to engage the hand-lever pinion.

(3) Connect the main power lead to any source of 24-volt d.c. If the voltage falls below 18, the magnet action will be unreliable; if more than 26 volts are used, injury to the magnets may result.

(4) After striking any key or the space bar, depress the hand lever fully and allow it to return completely to the top of its travel.

(5) To encipher or decipher a message, observe the normal operating procedures with the following exceptions:

(a) Zeroizing of the rotors can be accomplished with greater speed by moving the rotors manually to the "0" position.

(b) In determining the message rotor alignment, it is mandatory that each numeral key (1 through 5) be individually held in a depressed position until the downward motion of the hand lever has been completed. Failure to observe this requirement will prevent the stepping control rotors from advancing.

20. Tandem Operation.-Tandem operation provides an immediate automatic check of the encipherment of the message, a check on the operation of the enciphering machine, and an exact copy of the plain text of the message.

a. The machines have been provided with input and output tandem plug receptacles at the rear for tandem operation. Two machines can be connected so that one automatically deciphers the enciphered text produced by the other. When two machines are connected in tandem, errors will occur if only one machine is operated at a time or if the enciphering machine is operated faster than 40 words per minute. Tandem operation cannot be employed when emergency hand operation is used.

b. Two lengths of tandem cables are available. By using the longer cable it is possible to connect two machines in tandem after they have been installed in Chests CH-76

---

if the upper shelves are fully extended. When the shelf of a CH-76 is fully extended, a support should be placed under the front edge of the shelf to prevent its possible collapse.

c. The machines will be prepared for tandem operation as follows:

(1) Determine which machine has the slower speed. This may be accomplished by preparing the two machines for individual operation and turning the controller to the same position on both; i.e., if one machine is set at "P," set the second machine at "P" also. Set the stroke counter on each machine at *zero*. Press simultaneously the "Repeat" and "Blank" keys of both machines, holding them down approximately one minute. Release the keys simultaneously and note the counter readings. The machine showing the higher reading should be chosen as the deciphering machine and should be placed at the right of the other. The SLOWER machine will be the enciphering machine.

(2) Disconnect the power lead of the deciphering machine and tape or tie it so that it cannot accidentally be plugged into a source of power, but leave the ground clip connected. Should both machines be connected to a source of power while operating in tandem, fuses may be blown and damage may result.

(3) Check fuses in the master machine and replace with 10-ampere if equipped with 5-ampere. Five-ampere fuses are insufficient to start both motors at once.

(4) Using the tandem cable supplied, connect from the output on the enciphering machine to the input of the deciphering machine. Plugs are so constructed that they will fit only one way. The plugs must be completely inserted or improper operation may result. Care must be exercised in connecting the tandem cable in order to prevent bending the plug contacts or breaking the fiber insulators on either the tandem cable or the receptacles of the machine. A twisting motion should *not* be used in either inserting the plugs or removing them. A light coat of oil on the contacts will facilitate insertion and removal of plugs without interfering with the operation of the machines.

d. Tandem operation is accomplished as follows:

(1) Turn the controller of the enciphering machine to "R" and the deciphering machine to "P." Determine the message rotor alignment for the enciphering machine in accordance with paragraph 15.
(2) Turn the controller of the enciphering machine to "P" and the deciphering machine to "R" and align the rotors to the same message rotor alignment in accordance with paragraph 15.
(3) Turn the controller of the deciphering machine to "P" and type the necessary plain text, the system indicator, and the message indicator.
(4) Set the enciphering machine at "E" and the deciphering machine at "D." Proceed in accordance with normal operating procedure The enciphering machine will print the enciphered text, while the second machine will print the decipherment of the enciphered text, i.e., a duplicate of the plain text as typed.

SECTION VI
AIDS FOR DECIPHERING GARBLED MESSAGES

21. Introductory Information.

a. A detailed explanation of certain errors which may occur in messages enciphered by means of ASAM 1 is listed below in paragraphs 22 and 23 under the headings "When No Plain Text Appears" and "When Some Plain Text Appears." The errors are listed according to the frequency of their occurrence and the time necessary to correct them. Corrective measures are given for each error below the listing of the error. It is suggested that the corrections be tried in the order in which they are listed. Before trying any of the suggestions given below, the deciphering operator should check his own work to see that he has not deviated from prescribed procedure or made careless errors.

b. All errors, except typing errors, should be brought to the attention of the crypto-security officer.

22. When No Plain Text Appears.

a. *Missing or additional groups at the beginning of the message*.

CORRECTION PROCEDURE.-If checking the group count given in the message heading against the actual number of groups indicates that one or more groups are missing, or have been added, align the rotors to the message rotor alignment.

(1) If one or more groups are missing, turn the controller to "D" and advance the rotors by striking the "Blank" key as many times as there are missing letters. Decipher, beginning with the first group of the message.

(2) If one or more groups have been added, omit the indicated number of letters and decipher.

b. *Wrong system*.

CORRECTION PROCEDURE.

(1) Try deciphering the message using any other ASAM 1 cryptosystem held in common with the enciphering station.

c. *Failure to zeroize and realign if a rotor is advanced beyond the proper alignment in aligning the message rotor alignment*.

CORRECTION PROCEDURE.

(1) Zeroize the machine.

(2) When beginning to realign the rotors, advance the first rotor 26 characters beyond the letter to which it should be aligned, i.e., if the letter "B" has been selected as the first letter of the message indicator, advance that rotor until "B" appears on the white reference mark a second time and proceed to decipher. (The other four rotors will be aligned to normal positions.)
(3) If plain text does not result, zeroize the machine again and continue the process, advancing each rotor, in turn; an extra cycle. Four of the rotors must always be aligned correctly.

d. Message received with wrong date-time group or without date-time group.

CORRECTION PROCEDURE.

(1) Try the rotor arrangement and the index alignment for the date preceding and the date following the date appearing in the message.
(2) If no date appears in the message, try to decipher the message using the rotor arrangement and index alignment for the date following and the date preceding the date of receipt.
(3) Try the rotor arrangement and index alignment for the same day of the month preceding and the month following the current one.
(4) If the date appearing in the message is different from the date of receipt, try the date of receipt (if not tried in (1) above).

e. Failure to align to message indicator.

CORRECTION PROCEDURE-Zeroize the machine and begin decipherment without aligning the rotors to the indicator.

f. Transposition of letters of message indicator in the alignment of rotors.

Examples:
LEFLU aligned LEFUL
LKMNS aligned MKLNS
ALIFE aligned FAILE

(The enciphering operator is likely to exchange the position of two letters when the result forms a pronounceable group or when the two letters are often seen in reverse.)

CORRECTION PROCEDURE.

(1) Transpose adjacent letters in the message indicator and attempt to decipher the message.
(2) Transpose letters separated by only one letter and attempt to decipher. For example,

transpose the 1st and 3d letters of the indicator and attempt to decipher.
(3) Try aligning the rotors to various other arrangements of the letters in the indicator

g. Incorrect alignment of index rotors.

CORRECTION PROCEDURE.

(1) If the system indicator is for CONFIDENTIAL messages, try the SECRET index rotor alignment, and then the RESTRICTED index alignment. Use the same idea for messages of other classifications.
(2) Use the index rotor alignment for the date preceding and the date following the date appearing in the message.

---

h. Incorrect alignment of stepping control and alphabet rotors.

CORRECTION PROCEDURE.

(1) Decipher, using the system indicator as the message indicator.
(2) Decipher, using the 26-30 check group as the message indicator.
(3) If the message is divided into parts, use as the beginning alignment the reading left on the machine after decipherment of the previous part.
(4) If the letter "0" is to be aligned, do not advance the rotor 26 times in aligning the message indicator
(5) Align stepping control rotors to letters of message indicator which might have been misread, e.g., Q and 0, N and M, W and M (reversed).
(6) Align stepping control rotors to letters which are adjoining letters of message indicator.

i. Incorrect rotor arrangement, the operator having failed to make the 26-30 check.

CORRECTION PROCEDURE

(1) Check the daily rotor arrangement table for "R" (reverse) designations which are faint enough to be overlooked.
(2) Try consecutively each of the reversed rotors in the normal position; then all of the reversed rotors in the normal position.
(3) Exchange positions of the 6 and 9 rotors.
(4) Exchange the positions of the last two alphabet rotors on the right.

j. Additional groups at the beginning of the message when group count checks. (This sometimes occurs when the operator makes an enciphering error and realigns to the message indicator without tearing off the cipher letters already printed on the tape.)

CORRECTION PROCEDURE.

(1) Align the stepping control rotors to the message indicator and decipher, dropping the 1st, 4th, and 7th groups, etc., through approximately the 28th group.
(2) When plain text results, realign the rotors to the indicator and decipher, omitting the same number of groups dropped in the above procedure.

k. An incomplete group or complete groups lost at the beginning of the message when the group count checks.

CORRECTION PROCEDURE.

(1) Align the stepping control rotors to the message indicator; strike the "Blank" key once and decipher the first three groups; strike the "Blank" key again and decipher the 4th, 5th, and 6th groups; strike the "Blank" key and continue this process up to the 13th group. Check the tape for plain text. The number of blanks required to obtain plain text represents the number of missing letters.
(2) If no plain text results from the above procedure, without realigning the rotors, decipher the next group (13th) six or eight times. Check for plain text after each decipherment of the group and if in doubt decipher the next group (14th); if plain text still does not appear, decipher the 14th group six or eight times, checking for plain text.

---

l. Alignment of index rotors displaced.

CORRECTION PROCEDURE.

(1) Turn the index rotors forward one position, one at a time, and attempt to decipher the message each time a rotor is moved. (Four of the rotors will remain in the original position.)
(2) If the above procedure does not result in plain text, turn the index rotors backward one at a time and follow the same procedure

m. Index rotor off center.
(This will result in monoalphabetic substitution cipher text and should be reported to the cryptosecurity officer immediately.)

CORRECTION PROCEDURE.- Place any index rotor in a halfway position, i. e., halfway between two numbers. Align the message indicator and decipher the message. The alphabet rotors will not advance

n. Overstepping of an alphabet rotor.

CORRECTION PROCEDURE.

(1) With the rotors aligned to the message rotor alignment, advance the 1st alphabet rotor one position and decipher the first one or two groups. Check the tape for plain text.
(2) If plain text does not result, retard the 1st rotor one position and advance the 2d rotor one position; decipher the next two groups.
(3) If plain text still does not appear, follow the same procedure for the 3d, 4th, and 5th rotors.
(4) When plain text results, realign the rotors to the message rotor alignment, advance the correct rotor, and decipher.

o Failure of stepping control rotor to advance when a key is depressed during alignment of message indicator on enciphering machine.

CORRECTION PROCEDURE.- Align the rotors to the message rotor alignment, and then advance the alphabet rotors one at a time and in all possible combinations. Each time, decipher one or two groups. . Check the tape for plain text.

23. When Some Plain Text Appears.

a. Deletion of one or more groups.

CORRECTION PROCEDURE.

(1) Check the actual number of groups in the message against the group count appearing in the message heading. Realign to the message rotor alignment. With the controller at "D," advance the rotors to the point of garble by means

of the "Blank" key. Record the rotor alignment and counter reading. Strike the "Blank" key the same number of times as there are missing letters, and then continue with the decipherment of the message.
(2) If the above procedure does not result in plain text, align the alphabet and control rotors manually to the alignment at the point of garble as recorded in (1) above. With the controller at "D," decipher the group following the point of garble as many times as necessary (without realigning the rotors) until plain text appears, checking for plain text after each decipherment. For example, if the garbled text starts at a counter reading of 95 (19 groups), decipher the 20th group as many times as necessary (without realigning the rotors) until plain text appears.

b. Added or repeated groups.

CORRECTION PROCEDURE.

(1) If a check of the group count shows that one or more groups have been added or repeated, realign to the message rotor alignment. With the controller at "D," advance the rotors to the point of garble by means of the "Blank" key. Record the rotor alignment and counter reading. Omit the indicated number of groups and continue to decipher.
(2) If the above procedure does not result in plain text, decipher the 11th group following the garble as many times as necessary (without realigning the rotors) until plain text appears. Check each decipherment of the group for readable text. For example, if the recorded letter count at the point of garble is 205 (41 groups), decipher the 52d group as many times as necessary (without realigning the rotors) until plain text appears. If there are not 11 groups following the point of garble, decipher the next to the last group of the message (exclusive of indicators) as many times as necessary (without realigning rotors) until plain text appears.(3) The number of extra groups can be determined by subtracting from 11 the number of times the 11th group was deciphered to produce plain text.

c. One letter of a six-letter group (made by defective spacing of the machine) is lost in handling.

CORRECTION PROCEDURE.-Realign to the message rotor alignment. With the controller set at "D," advance the rotors to the point of garble, strike the "Blank" key once to replace the missing letter, and then decipher normally.

d. Cipher group consisting of only four letters.

CORRECTION PROCEDURE.-Record the rotor alignment and counter reading immediately before deciphering the four letter group. Strike the "Blank" key once to replace the missing letter, and then continue to decipher.

NOTE: In case an important word remains garbled in C or d above, realign to the point immediately preceding the group yielding garbles and decipher, striking the "Blank" key in a different position until a logical word is obtained. If necessary, consult a Morse error chart for two-letter combinations commonly transmitted as one letter. Substitute such letters in the cipher text and decipher.

e. Cipher group consisting of six letters. (Occasionally a six letter group will be printed because of a machine fault, in which case all six letters will be required to get plain text.)

CORRECTION PROCEDURE.

(1) Record the rotor alignment and counter reading immediately before deciphering the six letter group; then decipher all six letters of the group and continue to decipher several groups. If the result is a garble, decipher only the first five letters of the group, dropping the 6th, and

continue to decipher several groups. If there is still a garble, drop other letters of the group one at a time until plain text results.
(2) Consult a Morse chart, if applicable, for single letters commonly transmitted as two letters, and substitute in the cipher. text.

f. Two or more letters garbled in transmission causing an important word to be partially garbled.

CORRECTION PROCEDURE.

(1) Consult a Morse error chart or a teletypewriter garble table for letters commonly garbled in transmission. Substitute such letters in the cipher text and decipher.
(2) Realign the rotors to the message rotor alignment. Set the counter at zero and the controller at "E," and by means of the "Blank" key, advance the rotors to the point of garble; then encipher the assumed word, Compare the result with the cipher text received. If the difference is justified by common transmission errors, the assumed word is probably correct. (In this event the operator must deliver to the officer in charge of the cryptocenter the text which was actually deciphered as well as the correction.)

g. One hand of the enciphering operator misplaced on the keyboard. (Note that words when deciphered retain their correct length even though garbled) Example: AIRCRAFT REOIRTED IOERATUBG IVER SOUTHERN AREA. (In this example the right hand of the enciphering operator was placed one position over from the correct position.)

CORRECTION PROCEDURE.-Observe the text as it appears on the tape. Fit in probable plain-text words and try to justify them by a particular incorrect position of the operator's hand.

h. One hand of teletypewriter operator misplaced on keyboard in transmission. (Note that words do not necessarily retain their correct length.) Example: BOMBED AIRCLJFTWR GCBRTXDWOPERMXHJTYION GIAVER SOUTHERN AREA.

CORRECTION PROCEDURE.- Assume a specific incorrect position of the operator's hand. Replace the incorrect cipher letters with the assumed correct ones and decipher the result.

i. Stepping control rotors advancing incorrectly on the enciphering machine.

CORRECTION PROCEDURE. - Realign the rotors and decipher slowly, at the point of garble, observing the stepping of the rotors. As "0" on the 3d stepping control rotor passes the white reference mark, the 4th rotor should advance once; as "0" on the 4th rotor passes the white reference mark, the 2d rotor should advance once. In case one of these rotors fails to advance at the proper time move it forward by hand before striking the next key. Then proceed to decipher the message.

j. Stepping control rotors advancing incorrectly on the enciphering machine.

CORRECTION PROCEDURE.

(1) If the 2d, 3d, and 4th stepping control rotors advance at the point of garble, move back the 2d rotor one position, and continue decipherment. If plain text does not result, realign, move back the 2d and 4th rotors when they advance, and continue decipherment. Then realign, move back all three rotors one position, and continue decipherment.
(2) If only the 3d and 4th rotors advance at the point of garble, move back the 4th rotor one position and decipher. Then realign, if necessary, move back both the 3d and 4th rotors one position, and decipher.
(3) If only the 3d rotor advances at the point of garble, realign the rotors. Advance the rotors to the last letter yielding plain text; record the alignment of the rotors. Move back the 3d control rotor one position and decipher, beginning with the last correct letter. Check the tape for plain text.
(4) If plain text does not result, return to the recorded alignment, advance the 4th rotor one position and decipher; if plain text still does not appear, follow the same procedure for the 2d, 1st, and 5th rotors.

k. One alphabet rotor missing a step.

CORRECTION PROCEDURE.-To check for this fault on the enciphering machine, realign the rotors and at the point of garble move back the 1st alphabet rotor one position and decipher three groups. If no plain text results, advance the 1st alphabet rotor one position and move back the 2d alphabet rotor one position . Then decipher three more groups. If no plain text results, repeat this process for each of the five alphabet rotors. (If the last good letter of the text can be determined, only the alphabet rotors which advance during the decipherment of that letter need be tried.)

l. Overstepping of an alphabet rotor on the enciphering machine.

CORRECTION PROCEDURE.-Repeat the process outlined in paragraph 23k above, but this time advance the rotors one at a time and attempt to decipher. (If the last good letter of the text can be determined, only the alphabet rotors which did not advance during the decipherment of that letter need be tried.)

SECTION VII
OPERATION IN AN EMERGENCY

24. General.-The procedure for operation of ASAM 1 during an emergency created by the compromise of all keying materials in use or held in reserve by individual holders is described in paragraphs 25 through 29. The procedure provides a method whereby the data normally contained in the key list is supplied to each holder by a classified message in order that normal communications may be maintained until uncompromised key lists and rotors can be distributed.

25. Notification of Compromise.

a. Upon determination of a compromise the Chief, Army Security Agency, The Pentagon, Washington 25, D. C., or the Chief, Army Security Agency, Europe, Pacific, or Hawaii, whichever is applicable, will inform each holder of ASAM 1 of the compromise by means of an emergency message which will contain keying data for a period of five days. The emergency message will be identified by a special indicator reserved for that purpose only.

b. The emergency message will be enciphered with the currently effective rotors of the system. However, the rotor arrangement and index rotor alignment used will be based upon the emergency key phrase in effect at the time of the compromise.

26. Emergency Key Phrase.

a. Emergency key phrase will be supplied each holder of ASAM 1 in a sealed envelope *which will not be opened before the date indicated on the envelope*. Each emergency key phrase will be effective for a period of two months, at the end of which time a new phrase will become effective. The emergency key phrase will be used only in connection with the encipherment and decipherment of the emergency message. It will be used to determine for that message:

(1) The stepping control and alphabet rotor arrangement.(2) The index rotor alignment.

b. After the sealed envelope is opened, the emergency key phrase will be memorized and the letter containing it will be destroyed. No report of destruction is required. To insure knowledge of the phrase at all times, it will be memorized by the crypto-security officer and each trick chief. *Under no circumstances will the emergency key phrase be recorded nor will the letter be retained*. Written evidence of the phrase would defeat the purpose of the emergency system.

27. Use of the Emergency Key Phrase.-The emergency key phrase will be used for arranging and aligning the rotors as follows:

a. Each key phrase will be at least 16 letters in length, e.g., CAPTAIN JOHN SMITH
b. The first 10 letters will be numbered 1 through 0 according to their relative sequence in the normal alphabet. Thus,
3 1 9 0 2 5 7 6 8 4
C A P T A I N J O H N S M I T H
Note that repeated letters, such as A in this example, are numbered according to the order of their occurrence in the key, from left to right. The last letter to be numbered becomes 0, denoting the rotor numbered 0 in the set.

c. *Stepping control* (middle) rotors will be arranged in the cipher unit according to the first five numbers of the key. Any number associated with a vowel (A, E, I, 0, or U) indicates a "reversed" rotor. In this example, the arrangement of the stepping control rotors would be: 3, 1R, 9, 0, 2R.

d. The *alphabet* (rear) rotors will be arranged in the cipher unit according to the sixth through tenth numbers of the key. Any number associated with a vowel indicates a "reversed" rotor. In this example, the arrangement of the alphabet rotors would be: 5R, 7, 6, 8R, 4.

e. The index (front) rotor alignment will be derived by taking the alternate numbers in the key, beginning with the second number and proceeding through the tenth. In this example, the numbers are 1 0 5 6 4. The numbers indicate the "units" digit of the number to be aligned on each index rotor. Thus the index alignment in this example would be 11, 20, 35, 46, 54.

f. After arranging and aligning the rotors as described above, normal operating procedure for ASAM 1 will be observed in enciphering and deciphering the emergency message.

28. Emergency Message.

a. An emergency message, enciphered according to the above outlined procedure, will be sent to all holders of the compromised system. It will contain keying data for a five-day period and will bear three indicators, as follows:

(1) *A special indicator* which will indicate that it is an emergency message. This indicator will be KINSL.
(2) *The system indicator* for the SECRET classification of the compromised system.
(3) *The message indicator.*

b. The message will include the following items:

(1) Identification of the compromised system.
(2) Keying data arranged in the following order: date of the month; stepping control rotor arrangement; alphabet rotor arrangement; SECRET index rotor alignment and 26-30 check; CONFIDENTIAL index rotor alignment and 26-30 check; RESTRICTED index rotor alignment and 26-30 check.

c. A sample emergency message is illustrated below. "REV" appearing *after* a rotor number indicates that rotor is to be inserted in a reversed position.

SYSTEM NINE SIX FIVE THEEE COMPROMISED PD FIFTEENTH MIDDLE
FIVE TWO SIX NINE ZERO REAR SEVEN ONEREV EIGHT FOUR THE SEC

FOUR EIGHT FIVE ZERO ONE CHECK MIKE KING LOVE OBOE CHARLIE CONF
THREE SEVEN FIVE FOUR ONE CHECK NAN GEORGE TARE VICTOR ZEBRA
RESTR FOUR EIGHT TWO ZERO SEVEN CHECK DOG GEORGE OBOE WILLIAM
YOKE PD SIXTEENTH MIDDLE TWOREV NINE SEVEN FOUR ONE REAR THREE
FIVE SIXREV EIGHT ZERO SEC FOUR TWO EIGHT SEVEN ONE CHECK
CHARLIE BAKER FOX WILLIAM VICTOR CONF EIGHT TWO SIX FIVE THREE
CHECK TARE UNCLE OBOE PETER KING RESTR ZERO NINE TWO EIGHT SIX
CHECK QUEEN ZEBRA FOX UNCLE NAN PD SENTEENTH MIDDLE ONEREV
SEVEN NINE FOURREV TWO REAR EIGHT THREE SIXREV FIVE ZERO SEC
SEVEN FIVE TWO ONE SIX CHECK GEORGE VICTOR BAKER JIG QUEEN CONF
ONE FIVE ZERO EIGHT TWO CHECK TARE SUGAR UNCLE OBOE DOG RESTR
FIVE TWO NINE THREE SEVEN CHECK OBOE FOX CHARLIE KING PETER PD
EIGHTEENTH MIDDLE FOUR SEVENREV TWO FIVE ZERO REAR THREE NINE
SIX EIGHT ONE SEC TWO THREE EIGHT ZERO FOUR CHECK HOW YOKE FOX
CHARLIE JIG CONF FIVE NINE TWO ONE ZERO CHECK GEORGE WILLIAM
PETER OBOE ITEM RESTR SEVEN ONE FIVE EIGHT NINE CHECK DOG ITEM
KING ROGER BAKER PD NINETEENTH MIDDLE SIX TWOREV EIGHTREV ONE
FOURREV REAR FIVE ZERO SEVEN THREE NINE SEC NINE FOUR SEVEN ZERO
ONE CHECK JIG HOW DOG FOX ITEM CONF SEVEN ZERO FIVE THREE EIGHT
CHECK LOVE GEORGE MIKE PETER EASY RESTR NINE THREE SIX ONE FIVE
CHECK MIKE LOVE HOW GEORGE LOVE

d. The enciphered message, including the indicators, will be arranged as follows:

EXAMPLE: KINSL RLMCR DOG TARE JIG XRAY LOVE MRWTX ..... GDLJC

1 2 3 4

1. Special indicator for Key-changing message.
2. System indicator for SECRET classification of the compromised system.
3. Message indicator.
4. Text.

e. The emergency message will always contain keying data for the day on which it is sent, regardless of the time.

f. The keying data derived from the emergency key phrase will not be employed for enciphering or deciphering any other message. After deciphering the emergency message, each holder will prepare the ASAM 1 for operation using the data supplied in the message in conjunction with the currently effective rotors of the compromised system.

g. The deciphering copy of the emergency message will be retained in the cryptocenter where it will be safeguarded in the manner prescribed for registered SECRET material. It will be destroyed five days after the last date for which the keying data is contained therein. In the event that an emergency destruction of crypto- material is necessary, the plain text of the emergency message will be the first item destroyed.

h. In the event that replacement key lists and rotors cannot be distributed to all holders within five days, additional keying data will be supplied each holder by classified message. This message will resemble a normal message and will be enciphered by means of the keying data supplied for the last date in the emergency message.

---

29. Normal Traffic.

a. The system indicators contained in the key list will be used for all ASAM 1 traffic enciphered during the emergency period. The special indicator KINSL is reserved for the original emergency message only.

b. Operation of the ASAM 1 employing the keying data supplied in the emergency message will conform to the normal operating procedure for the machine.

REFERENCES:

The information enclosed here relating to the ECM Mark II was OCR scanned and reformatted for the Internet from:
Department of the Army (1949) ASAM 1/1 Crypto-Operating Instructions for ASAM 1.

Return to the ECM Mark II page.