KAO-64C/TSEC

REGISTER NO. 1705

DOWNGRADED TO UNCLASSIFIED - SEE MEMO 1000-80/402 (DCONSEC 5-3) 15 JAN 80.

OPERATING INSTRUCTIONS

FOR

TSEC/KL-4

This publication consists of cover and 25 numbered pages 1 to 25 inclusive.

Verify presence of each page upon receipt.

DEPARTMENT OF DEFENSE
NATIONAL SECURITY AGENCY
WASHINGTON, D. C. 20305

MILITARY C & E MUSEUM
CURATOR
CFB KINGSTON
P O BOX 17000 STN FORCES
KINGSTON ON K7K 7B4

January 1966

ORIGINAL

(Reverse Blank)

CONFIDENTIAL

DEPARTMENT OF DEFENSE
NATIONAL SECURITY AGENCY
WASHINGTON, D. C. 20305

January 1966

OPERATING INSTRUCTIONS FOR THE TSEC/KL-4

LETTER OF PROMULGATION

1. This is a CONFIDENTIAL registered publication and will be handled, stored, accounted for, and destroyed in accordance with the current regulations of the appropriate Department, Agency, or other controlling authority, pertaining to registered cryptomaterial.

2. This publication will become effective upon receipt and will supersede KAO-64B/TSEC, at which time destruction of KAO-64B is authorized. Instructions for the eventual disposal of this publication will be issued at an appropriate time by the Director, National Security Agency.

3. Amendments to this publication will be promulgated by means of a printed or electrically transmitted amendment. Individuals entering such amendments shall so indicate on the "Record of Amendments" page included herein as page 3.

4. This publication will be distributed to authorized holders of TSEC/KL-4.

5. THIS PUBLICATION CONTAINS INFORMATION AFFECTING THE NATIONAL DEFENSE OF THE UNITED STATES WITHIN THE MEANING OF THE ESPIONAGE LAWS, TITLE 18, U. S. C., SECTIONS 793, 794, AND 798. ITS TRANSMISSION OR THE REVELATION OF ITS CONTENTS IN ANY MANNER TO AN UNAUTHORIZED PERSON IS PROHIBITED BY LAW.

6. Extracts from this publication may be made if necessary. Such extracts will be classified CONFIDENTIAL and accounted for locally until destroyed.

7. This publication may not be carried in aircraft for use therein.

MARSHALL S. CARTER
Lieutenant General, U. S. Army
Director

RECORD OF AMENDMENTS

Identification of Amendment and Reg. No. (if any)	Date Entered	By Whom Entered (Signature; Rank or Rate; Name of Command)

RECORD OF PAGE CHECKS

Date Checked	By Whom Checked (Signature; Rank or Rate; Name of Command)	Date Checked	By Whom Checked (Signature; Rank or Rate Name of Command)

RECORD OF PAGE CHECKS

Date Checked	By Whom Checked (Signature; Rank or Rate; Name of Command)	Date Checked	By Whom Checked (Signature; Rank or Rate; Name of Command)

TABLE OF CONTENTS

CHAPTER 1

GENERAL

Section		Paragraph	Page
1000	GENERAL		
	Scope	1001	7
	Use	1002	7
	Associated Materials	1003	7
	Procedure	1004	7-8
	Derivation of Intermediate Groups	1005	8-9

CHAPTER 2

TSEC/KL-4

2000	GENERAL		
	Usage and Operation	2001	11
	Authorization for Use	2002	11
	Clearance Requirements	2003	11
	Training Requirements	2004	11
	Comments and Recommendations	2005	11
	Destruction of Used Keying Material	2006	11
2100	DESCRIPTION		
	General	2101	11-13
2200	PHYSICAL SECURITY		
	General	2201	13
	Accounting	2202	13
	Storage and Shipment	2203	13
	Emergency or Precautionary Destruction	2204	13-14
2300	KEYING MATERIALS		
	General	2301	14
	PENELOPE Call Sign Cipher Key Lists	2302	14
	Keying Material	2303	14
	Key Strips	2304	14-16

CHAPTER 3

OPERATION

3000	KEYING INSTRUCTIONS		
	Drum Loading	3001	17-18
3100	NORMAL KL-4 ENCRYPTION AND DECRYPTION		
	General	3101	18
	Sequence of Operations in Encryption	3102	18-20
	Encryption Check	3103	20
	Sequence of Operations in Decryption	3104	20-21
	Stacking Call Signs	3105	21

Section		Paragraph	Page
3200	ENCRYPTION-DECRYPTION, ALTERNATE METHOD		
	General	3201	21–22
	Encryption	3202	22
	Decryption	3203	22–23
	Encryption/Decryption Check	3204	23

CHAPTER 4

CRYPTOSECURITY

4000	GENERAL		
	Possible Compromises	4001	25
	Practices Which are Prohibited	4002	25

LIST OF ILLUSTRATIONS

Figure	Description	Page
1	KL–4, Open Cover	12
2	KL–4, Closed Cover	15
3	KL–4, Side View	19

CHAPTER 1

1000—GENERAL

1001. Scope.—This publication contains information relative to the use of the TSEC/KL-4 in association with PENELOPE keying material.

1002. Use.—The TSEC/KL-4, in conjunction with PENELOPE key lists, is used for the encryption of call signs and address groups used on radio circuits, both CW and Voice.

1003. Associated Materials.—KAL-9, KAL-15, AMSP 1103, AMSP 298, and ACP-119.

1004. Procedure.

a. General.—Approved plain callsigns/address groups taken from the appropriate ACP's are used with Table A from KAL-15 (digraph substitution table) to obtain intermediate groups, which are in turn enciphered on the KL-4 using key strips from KAL-9. Secure Voice callsigns may be transmitted phonetically, or may be converted to a pair of words using the non-changing word square contained in ACP-119. (Note: KAL-15 and AMSP 298 are parallel documents. They share the same format and may be used with the same equipments. KAL-9 and AMSP 1103 are also parallel documents except that AMSP 1103 contains the digraph substitution table and the non-changing word square, and KAL-9 does not. For users of these instructions that do not hold KAL-9 and KAL-15, substitute AMSP 1103 and AMSP 298, respectively).

b. Task Element Call Signs.—Task Element call signs may be obtained by encrypting the Task Unit call sign in the prescribed manner, then appending a hyphen (-) as the fifth character and the Task Element number as the sixth and final character of the encrypted callsign. An alternative method is to encrypt a Task Element call sign which has been assigned by the Officer in Tactical Command (OTC) from the block of calls provided in the appropriate Task Organization Call Sign Publication. The latter method should be used when it is necessary to conceal the existence of Task Elements. (Note: When Task Element Call Signs are being encrypted in AMSP 1103, a slant sign (/) rather than a hyphen must be appended as the fifth character, except as noted in subpar. 1005*g*, below.)

c. Retarding Voice Call Sign Changes.

(1) *General.*—A Procedure known as MISFIT has been established for retarding voice call sign changes when a force is engaged in action at a time scheduled for a call sign change. Implementation of MISFIT procedure merely continues the use of voice call signs already in effect past the time scheduled for their supersession; it has no effect on the supersession of RATT/CW call signs. Thus, when MISFIT is declared and the time scheduled for normal call sign change is reached, KAL-9 key card supersession will take place, new call signs (RATT/CW and voice) will be derived, and all but the newly derived voice call signs put in use. (The derivation of new voice call signs may be delayed until the time for rescission of MISFIT is known.) As long as MISFIT is in effect, the voice call signs already in use, derived by means of the superseded key card, will remain in effect.

(2) *Description and Instructions.*—The terms "MISFIT" and "CHARTER" have been selected to mean "Implement" and "Rescind" MISFIT Procedure, respectively. They are used in the following manner:

(a) *MISFIT.*—When it is considered expedient to retard a voice call sign change, the OTC may do so by ordering transmission of the term "MISFIT," followed by the random designator (e.g., DH), which appears on each page of the KAL-9 key strip

in use at the time, to all Force units using voice radio communications. This order will inform all units concerned that the voice call signs derived by means of the designated key strips will remain in use until further notice. Transmission of the order will be by the most expeditious means possible, in accordance with standard signal and communications procedures, *and with the security restrictions in paragraph 4, below.* (It is assumed that MISFIT procedure will normally be ordered into use over the voice radio circuits it will affect.)

Example: A force is engaged by the enemy at 2330Z, and has a call sign change scheduled for 0001Z. The Force OTC feels that conducting the call sign change as scheduled on the Force's voice radio circuits will be deleterious to his tactical control. KAL–9 key strips with the designator "DH" are in use by the units of his Force. The OTC orders the following transmission made to all Force units concerned:

"MISFIT DELTA HOTEL"

As transmitted, this order means "continue using voice call signs encrypted by means of KAL–9 key strips having the random designator "DH" until further notice."

(b) *CHARTER.*—When the situation requiring retardation of the voice call signs change has passed, replacement of the superseded voice call signs will be effected as soon as possible. The OTC may accomplish this by ordering transmission to units concerned of the term "CHARTER," followed by the designation of the effective KAL–9 key strips with which the new voice call signs will be derived, and a time (transmitted in Numeral Code) indicating when that key is to be put in use.

Example: The action which caused the OTC to order MISFIT has ended at 0700Z. The OTC wishes to allow time for regrouping before changing call signs, so decides to wait until 0800Z to put the deferred key strips (e.g., DZ) into effect. The OTC orders the following transmission made to all Force units concerned:

"CHARTER DELTA ZULU NUCO ALFA KILO FOXTROT VICTOR LIMA KILO UNUCO"

As transmitted, this order means "Change to call signs encrypted by means of KAL–9 key strips having the random designator "DZ" at 0800Z."

(3) *Promulgation.*—The OTC will ensure simultaneous promulgation of MISFIT procedure on all voice radio circuits under his control.

(4) *Security.*—Ordering MISFIT procedure into effect in the manner described above before engagement in action has occurred, could betray to opposing forces that an operation is impending. Therefore, any orders issued prior to engagement in action which indicates that MISFIT procedure is to be implemented will be afforded physical or cryptographic security in their transmission.

1005. Derivation of Intermediate Groups.

a. Secure call signs/address groups will be based on plain call signs listed in a single column of the appropriate call sign/address group publications.

b. Using a plain call sign, an intermediate group is derived from the ENCODE section of Table A in KAL–15. The intermediate group derived from this table is encrypted using the appropriate pages of keying material from KAL–9 to produce a daily changing call sign or address group. On voice circuits, the secure call sign thus produced may be transmitted phonetically, or it may be converted to a pair of words using the nonchanging Word Square from ACP–119.

c. Only four-character groups will be applied to Table A. Similarly, only four-character groups can be converted to a pair of words using the Word Square. The first two characters of the four-character group are called the first digraph, and the last two characters are called the second digraph.

d. A plain call sign is converted to an intermediate group by a process of digraph for digraph substitution. An intermediate group is converted to a plain call sign by the same process. A call sign encrypted for transmission over voice circuits is converted to a pair of words by a process of word for digraph substitution.

e. The substitution for the first digraph is always from the UPPER HALF of a cell, and the substitution for the second digraph is always from the LOWER HALF of a cell. Table A and the Word Square are always entered on the row (horizontal) corresponding to the first character of the digraph being processed. The substitute digraph is located in the cell formed by the intersection of this row with the column (vertical) corresponding to the second character of the digraph being processed. For example, in the four character group ABRD, AB is the first digraph and RD is the second digraph. The substitute for AB would be located in the UPPER HALF of the cell at the intersection of Row A with Column B. The substitute for RD would be located in the LOWER HALF of the cell at the intersection of Row R with Column D.

f. A pair of words can be converted back to the original encrypted call sign by locating the words in the Word Square and reading off the Row-Column coordinates of the cells in which the words were located. The first words of these call signs are listed alphabetically in the UPPER HALVES of the cells. The second words of the call signs are listed alphabetically in the LOWER HALVES of the cells. The two distinct alphabetical lists read down columns, commencing with Column A and continuing to Column B, and so on through the 37 columns.

g. Example of Digraph Substitution: The plain call sign for the U. S. S. Franklin D. Roosevelt, as listed in ACP–113, is L4Y4. To change this plain call sign to an intermediate group, refer to the ENCODE section of Table A in the effective edition of KAL–15. Assume, in the UPPER HALF of the cell at the intersection of Row L with Column 4, is the digraph 6D. Assume, in the LOWER HALF of the cell at the intersection of Row Y with Column 4 is the digraph A3. The two digraphs form the intermediate group 6DA3, which is then encrypted using the KAL–9 keying material effective for that date to obtain the daily changing call sign to be transmitted. REMEMBER THAT INTERMEDIATE GROUPS ARE NEVER TO BE TRANSMITTED. The transmitted call sign will decrypt on the KL–4 to 6DA3 which can then be converted back to the plain call sign by using the DECODE section of Table A. In the UPPER HALF of the cell at the intersection of Row 6, Column D will be the digraph L4. In the LOWER HALF of the cell at the intersection of Row A with Column 3 is the digraph Y4. The two digraphs form the plain call sign L4Y4. (Note: AMSP–1103 contains an extra set of key strips which are entitled "Supplemental Key Strips Number 32" and which are used to derive monthly changing encrypted call signs for individual merchant ships in wartime or during Exercises, and for warships simulating merchant ships during Exercises. Encryption and decryption procedures are the same as described in chapter 3 of this publication. These key strips will be used only for the purpose stated above unless authorized by appropriate authority for additional use. Task Element call signs encrypted with these strips must have the discriminant $\overline{P}$ (transmitted .--.-) appended as the fifth character, rather than the normal slant sign (/).)

CHAPTER 2

TSEC/KL-4

2000—GENERAL

2001. Usage and Operation.—The KL-4 is a cryptodevice designed to facilitate the encryption and decryption of 4-character call signs/address groups, when PENELOPE cryptosystems are employed. The device is capable of two different methods of operation, both of which provide an output compatible with that of the KA-2 (CSP 1750), KA-3 (CSP 1756), and the KL-8. The normal method requires keying material produced in a special format; the alternate method permits use of the key lists produced for use with the KA-2, KA-3, and KL-8.

2002. Authorization for Use.—The KL-4 is authorized for use with PENELOPE keying material for the encryption and decryption of 4-character call signs, address groups, and operating signal groups.

2003. Clearance Requirements.—Formal authorization for access to CONFIDENTIAL cryptomaterial is required for personnel to have access to the key lists used with the KL-4. PENELOPE key lists are classified CONFIDENTIAL and are registered. The TSEC/KL-4 is an unclassified, nonregistered equipment.

2004. Training Requirements.—Operators shall be trained in the keying and operation of this equipment before being permitted to use the KL-4 for operational traffic.

2005. Comments and Recommendations.—Comments and recommendations in connection with the equipment or associated cryptomaterials should be forwarded through Service channels to the National Security Agency. Exception: NATO users forward comments and recommendations to SECAN.

2006. Destruction of Used Keying Material.—Used key strips shall be returned to the cryptocustodian after removal from the KL-4 drums. Individual key cards shall be accounted for locally until destroyed. Used key strips must be destroyed within 5 days after normal supersession. The complete publication, KAL-9/TSEC, including unused pages, will be destroyed in accordance with paragraph 2 of its Letter of Promulgation.

2100—DESCRIPTION

2101. General.—The KL-4 is a desk-top, manually operated device of the following dimensions: Length, 14⅞ inches; Width, 11 inches; Thickness, with stand, 4½ inches. (See figs. 1, 2, and 3.)

a. Input Knobs.—Four knobs attached to the left side of the machine control the alignment of the input drums. (See fig. 1, #1.)

b. Input Drums.—Four cylindrical drums (2⅞-inches wide and 7¾-inches in circumference) are located on the left side of the equipment beneath the face cover. The input key strips for the cryptoperiod are displayed on these drums. (See fig. 1, #2.)

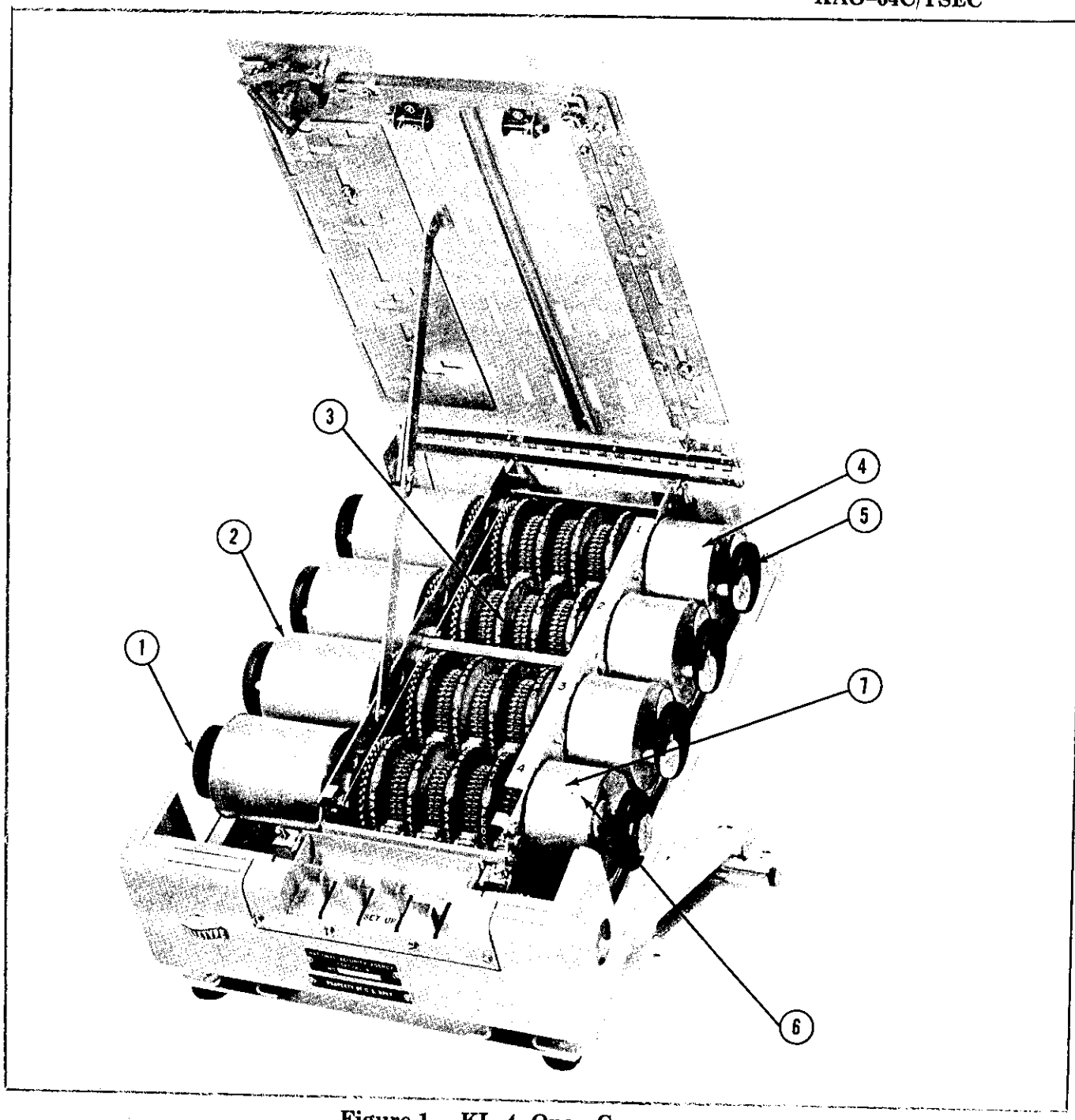

Figure 1.—KL-4, Open Cover

1. Input Knob
2. Input Drum
3. Addition Rotor
4. Output Drum
5. Addition Rotor Setting Knob
6. Horizontal Slot
7. Bench Mark

c. *Addition Rotors.*—Sixteen 37-character rotors, placed in four rows and four columns, are located in the center portion of the equipment. Each row is manipulated by an addition rotor setting knob on the right of the equipment, which performs an addition function. (See fig. 1, #3.)

d. Output Drums.—Four cylindrical drums (1½-inches wide and 7¾-inches in circumference) are located on the right side of the equipment beneath the face cover. The output key strips for the cryptoperiod are displayed on these drums. (See fig. 1, #4.)

e. Addition Rotor Setting Knobs.—Four knobs on the right side of the equipment are turned to move the addition rotors. (See fig. 1, #5.)

f. Set-Up Blocking Bar.—This button is located on the right side and at the bottom of the equipment. It must be depressed and held to allow the operator to push any of the column set-up levers. (See fig. 3, #1.)

g. Column Set-Up Levers.—Four levers located approximately at the bottom center of the equipment must be pushed down individually to allow a column of addition rotors to be moved. (See fig. 2, #1.)

h. Encrypt-Decrypt Knob.—This knob selects the mode of operation; it has four positions: left encrypt and left decrypt (for past call signs), and right encrypt and right decrypt (for present call signs). The setting of this knob determines the input window which will open to produce the setting for the addition rotors. (See fig. 2, #2.)

i. Numerical Equivalent Reading Knob.—This knob, located at the bottom right of the equipment, may be pulled down to open four windows, adjacent to the output windows, which allow viewing of the four numerical values of the encrypted or decrypted call sign. (See fig. 2, #3.)

j. Cover Release Knobs.—These knobs are located below the bottom row of addition rotor windows and, when squeezed, allow the cover to be raised for keying the equipment. (See fig. 2, #4.)

2200—PHYSICAL SECURITY

2201. General.—The machine and unkeyed drums are unclassified. The equipment when keyed is classified CONFIDENTIAL—CRYPTO.

2202. Accounting.—The KL-4 is not registered but it bears a number on the name plate which can be used for local accounting.

2203. Storage and Shipment.—The storage and shipment of classified PENELOPE cryptomaterial will be in accordance with the procedures outlined in the effective edition of KAG-1/TSEC or AMSP 293, as appropriate.

2204. Emergency or Precautionary Destruction.

a. General.

(1) Each headquarters holding classified cryptomaterial shall have a plan for the destruction of such matter in time of emergency.

(2) Designated cryptopersonnel should be authorized to issue the destruction order on their own initiative in the event that conditions prevent communication with the responsible officer.

(3) Suggested destruction materials and methods are outlined in KAG-1 or AMSP-293, as appropriate, which should be referred to in preparing a destruction plan.

b. Destruction of Associated Cryptomaterial.—The priority for destruction is as follows:

(1) Superseded keying material.
(2) ROB keying material.
(3) Effective keying material.
(4) Operating and Maintenance Instructions for the TSEC/KL-4.

c. *Destruction of Equipment.*—Although the KL–4 is unclassified, it is desirable, if time permits, to render the equipment unusable; this may be accomplished by using an acetylene torch, thermite incendiary, sledge hammer, or other appropriate means.

d. *Destruction Report.*—Accurate information concerning the extent of destruction is second in importance only to the destruction of the material itself. The facts surrounding the destruction shall be reported to the appropriate Service headquarters as soon as possible and by the most expeditious means available. Reports should clearly indicate the material destroyed, the method and extent of destruction, and the extent of destruction of items not completely destroyed and presumed to have been captured or compromised.

2300—KEYING MATERIALS

2301. General.—To obtain maximum benefit from KL–4 usage, keying material has been produced in a special format so that it can be placed on the drums of the device. This keying material has been assigned the short title, KAL–9/TSEC. Each edition of KAL–9 contains the same PENELOPE key values as the corresponding edition of KAL–15 which is currently effective for use with other call sign devices; for example, KAL–9 (E) will produce the same encrypted call sign as KAL–15 (E), when the same intermediate group is enciphered. (Similarly, editions of AMSP 1103 contain the same key values as corresponding editions of AMSP 298.) The digraph square used for enciphering intermediate groups is contained in the KAL–15 key list. This square is used with both KAL–9 and KAL–15 key lists.

2302. PENELOPE Call Sign Cipher Key Lists.—The strips which are used to key the KL–4 are contained in KAL–9, in book form. Each edition of KAL–9 contains 96 pages of keying material. The key for each KL–4 drum loading occupies three pages; two pages contain the key strips for the input (wide) drums and one contains the key strips for the output (narrow) drums. The front cover of each edition contains the following information:

a. The Letter of Promulgation.

b. The classification CONFIDENTIAL.

c. The short title KAL–9 plus the edition indicator, e.g., KAL–9B/TSEC.

d. The mythological designator PENELOPE.

2303. Keying Material.—Each set of three pages of keying material in KAL–9 is effective for two days and is identical in content to that appearing in the corresponding edition of KAL–15. For example, pages 1, 2, and 3 of KAL–9 contain the same keying material as is printed on Key Cards No. 1 and 2 in the corresponding edition of KAL–15. When a page of keying material is cut into strips (see sec. 3000) and placed on the appropriate drums of the KL–4, encipher and decipher values for two successive cryptoperiods can be read in the designated reading windows. Each page contains material effective for the current and preceding days. The numerals printed below the keying material indicate the dates for which it is effective. For the first day of each month, the keying material effective for that day will be used in conjunction with that effective for the last day of the previous month. For example, on 1 May, pages 94, 95 and 96 of the edition effective for April would be used. On 2 May, pages 1, 2, and 3 of the edition effective for May would be used.

2304. Key Strips.—These strips, assigned for a 24-hour cryptoperiod, are of two widths. The wide strips (2⅞ inches) fit onto the input drums 1 through 4 on the left inside of the equipment, and the narrow strips, (1½ inches) fit onto the output drums located on the right inside of the equipment. (See fig. 1.)

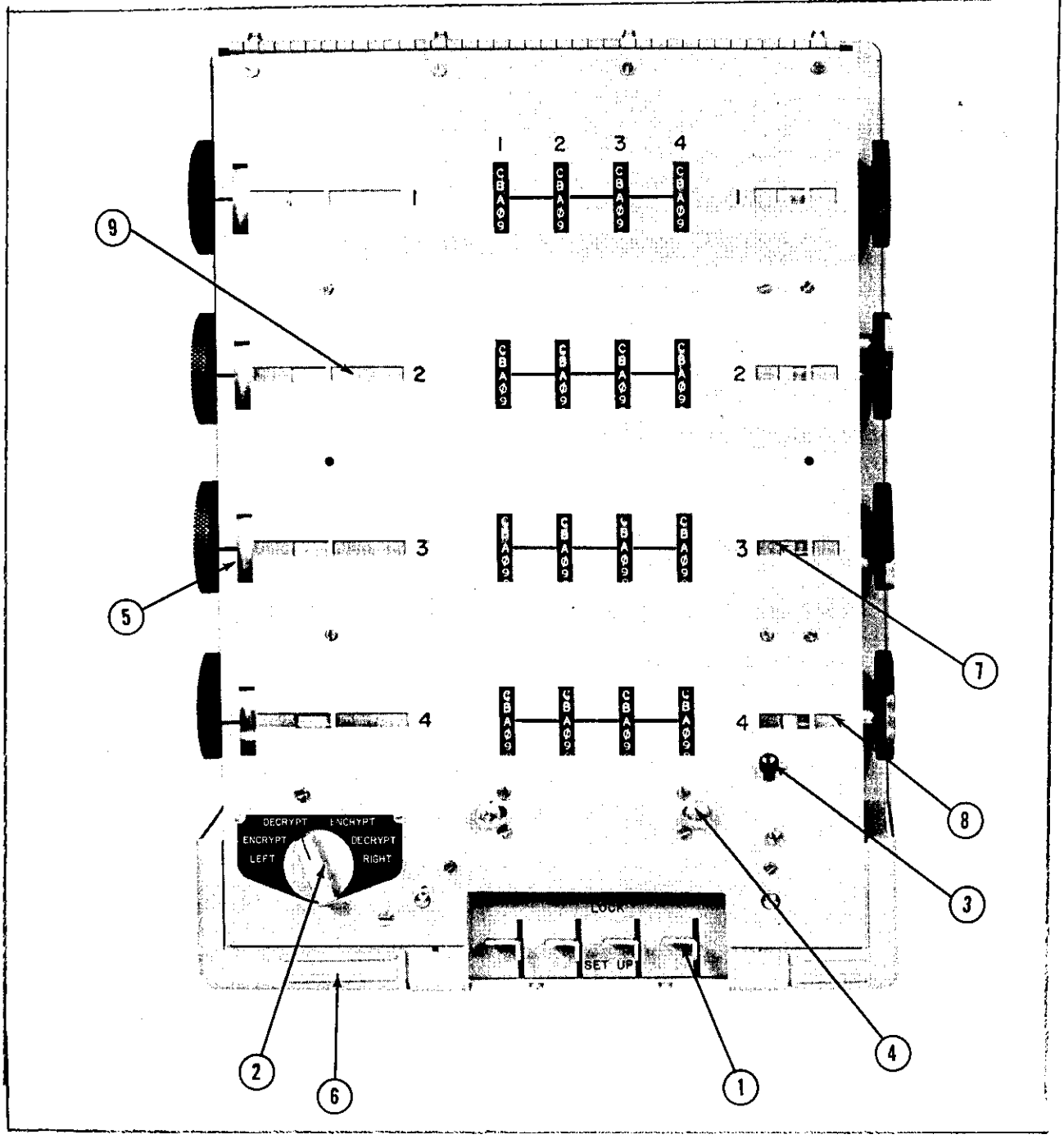

Figure 2.—KL-4, Closed Cover

1. Column Set-Up Lever
2. Encrypt-Decrypt Knob
3. Numerical Equivalent Reading Knob
4. Cover Release Knob
5. Input Window
6. Date Strip Channel
7. Numerical Equivalent Window
8. Output Window
9. Key Value Windows

a. The following information is printed on the wide (input) strips:

(1) At the top of each strip is a number repeated three times which indicates the drum on which that strip is to be placed, e.g., 1 1 1 would be printed on the strip for drum No. 1. The drums are numbered 1 through 4 from top to bottom.

(2) Down the left side of each strip is the PENELOPE alphabet, a 37-character sequence composed of the letters A through Z, the slant sign "/," and the digits 1 through 0, which comprise the input characters.
(3) Adjacent to each input character are four key value groups; each group is composed of four characters from mixed PENELOPE alphabets.
(4) At the bottom of each strip are the short title, and two numbers indicating the crypto-period for the strip's use.
(5) At the top and bottom of each strip, between the second and third columns of key value groups, there are vertical lines (bench marks) which must be used to insure correct horizontal alignment of each strip on the drum. These bench marks are aligned against corresponding bench marks on the drum itself. (See fig. 1, #7.)
(6) A fold line appears at the top of each strip.
(7) The classification CONFIDENTIAL and the designation CRYPTO appear on each strip.

b. The following information is printed on each narrow (output) strip:
(1) At the top of each strip a number, repeated three times which indicates the drum on which that strip is to be placed, e.g., 2 2 2 would be printed on the strip for drum No. 2. The drums are numbered 1 through 4 from top to bottom.
(2) Down the left side of each strip are the numbers 00 through 36 in order.
(3) Adjacent to these numbers are four columns; each column is a mixed PENELOPE alphabet.
(4) At the bottom of each strip are the short title, and two numbers indicating the crypto-period for that strip's use.
(5) At the top and bottom of each strip, between the first and second columns of mixed PENELOPE alphabets, there are vertical lines (bench marks), which must be used to align the strip against corresponding bench marks on the drum.
(6) A fold line appears at the top of each strip.
(7) The classification CONFIDENTIAL and the designation CRYPTO appear on each strip.

c. At the bottom of each input and output strip there are two numbers above the dotted line and two numbers below the dotted line. The section containing the lower pair of numbers must be cut off of one input and one output strip. These sections will be placed in the input and output date strip channels. (See fig. 2, #6.)

d. The margin of each page on which the key strips are printed contains the following information:
(1) The classification of the keying material.
(2) The short title.
(3) The DAY numbers.
(4) The random designators for the two cryptoperiods of key on that page.
(5) The check call for the first cryptoperiod on that page.
(6) Page number.

CHAPTER 3

OPERATION

3000—KEYING INSTRUCTIONS

3001. Drum Loading.—Remove the pages for the effective cryptoperiod from the key pad by creasing and tearing along the dotted line. Separate the strips by cutting along the lines indicated by the dotted lines between the strips. Care should be exercised not to cut into the strips or to disfigure them so as to make them unusable. Fold the top of each strip at the solid (fold) line. Key the drums using the following procedure:

a. Release the latch on the lid of the equipment and raise the lid to its open position (about 90 degrees).

b. Insert the wide key strip numbered 111 on the drum at the top left of the equipment. This is done in the following sequence:
(1) Hold the key strip in the right hand at the top of the strip, with the printing in normal reading position.
(2) Insert the tab of the folded key strip into the horizontal slot in the drum. Pull the tab into the drum by rotating the pressure roller knob located just to the side of the slot, (see fig. 3), in a clockwise direction. The tab of the strip should be pulled into the drum until the fold is aligned with the bottom edge of the horizontal slot in the drum. The bench mark on the key strip should line up with the bench mark on the drum.
(3) Rotate the strip and drum until the bottom of the key strip meets the tab already inserted in the slot.
(4) Insert the bottom of the key strip into the slot and draw the strip tight on the drum by rotating the pressure roller knob. The bench mark on the bottom of the key strip should be aligned to the bench mark on the top of the strip.

c. The strips for input drums 2, 3 and 4 should be inserted in a similar manner.

d. The narrow (output) strips numbered 1 thru 4 should be inserted on the output drums numbered 1 thru 4 in the same manner as the input strips. The output drums are located on the right side of the equipment.

e. Drum Alignment Check.
(1) Check to determine if the characters of the output strips are properly positioned in the output windows.
(2) If any of the characters are out of line, they can be corrected as follows:
(a) Loosen the vernier adjustment knob on the output knobs affected. (See fig. 3.)
(b) Rotate the drum with the free hand until the characters are correctly aligned below the window(s).
(c) Tighten the vernier adjustment knob.

f. After the drums are keyed, zeroize all addition rotors. To zeroize, push in the set-up blocking bar (see fig. 3, #1) and pull down the column set-up lever (see fig. 2, #1) for column 1 of the addition rotors. The rotors may then be turned manually in either direction by turning the rotor setting knob (see fig. 1, #5). Columns 2, 3, and 4 are aligned in a similar manner. (0 should appear in each of the 16 addition rotor windows in line with the index mark, just as "A" is aligned in fig. 2.) Pull down the numerical equivalent reading lever. If 00 is visible in all four windows, the machine is properly set up and ready for operation.

If not, the machine is off register and must be realigned as follows:

(1) Place all of the set-up levers in the lock position.
(2) Place a finger in the access hole located on the underside of the unit, toward the rear. Move the lock bar tongue fully to the rear.
(3) Rotate the output drum to be realigned to the 00 position. Permit the lock bar tongue to return to its normal position.

g. After the device is keyed, the group ABCD must be encrypted with the Encrypt-Decrypt Knob set to the correct encrypt position to assure that the key has been placed on the drums of the device correctly and that the device is functioning properly. (See pars. 3102*g* thru *i*.) The encrypted value of ABCD is shown in the margin of the effective cryptoperiod of KAL–9 keying material.

3100—NORMAL KL–4 ENCRYPTION AND DECRYPTION

3101. General.—The four-character group to be encrypted (or decrypted) is to be entered vertically in the input windows, at the extreme left of the device, by turning the input knobs on the left side of the device. The first input character should be set to the index mark in Window No. 1 over Drum No. 1 (at the top of the device); the second character is to be set to the index mark in Window No. 2 over Drum No. 2, etc. The sixteen addition rotors are aligned to the appropriate key values appearing in the key value windows adjacent to the input windows. This is accomplished by activating each column of rotors, individually, by pulling down the column set-up lever for that column and rotating the addition rotor setting knobs on the right side of the device. When the key values have been entered on the sixteen addition rotors, the encrypted (decrypted) call sign/address group is displayed vertically in the output windows. CAUTION: When rotating the addition rotor setting knob (see fig. 1, #5) care should be exercised to avoid turning the vernier adjustment (see fig. 3, #2).

3102. Sequence of Operations in Encryption.—After the equipment has been keyed in accordance with the instructions in Section 3000, encryption is accomplished in the following manner:

a. Convert the plain call sign/address group to a four-character intermediate group in accordance with the instructions in Chapter 1.

b. Move the Encrypt-Decrypt Knob to the encrypt position for the cryptoperiod desired, as indicated by the date in the date strip channel. Left windows open for past, right for present period.

c. By turning the input knobs on the left side of the equipment in either direction, set the four characters of the intermediate group to the index marks in the vertical input windows of the equipment, reading from top to bottom. That is, set the first input drum to the first character of the intermediate group, the second drum to the second character of the group, the third drum to the third character, and the fourth drum to the fourth character.

d. Assure that the Encrypt-Decrypt Knob is set to the appropriate encrypt position. This will open the appropriate four encrypt windows, which display the four-character key value groups for each of the input characters.

e. Push in the set-up blocking bar with the right index finger and simultaneously pull down the column set-up lever for Column 1 of the addition rotors. The four key values (reading from left to right) appearing in key value Window No. 1 are to be displayed from top to bottom in the addition rotor viewing windows for Column 1. (See fig. 3.) Similarly set

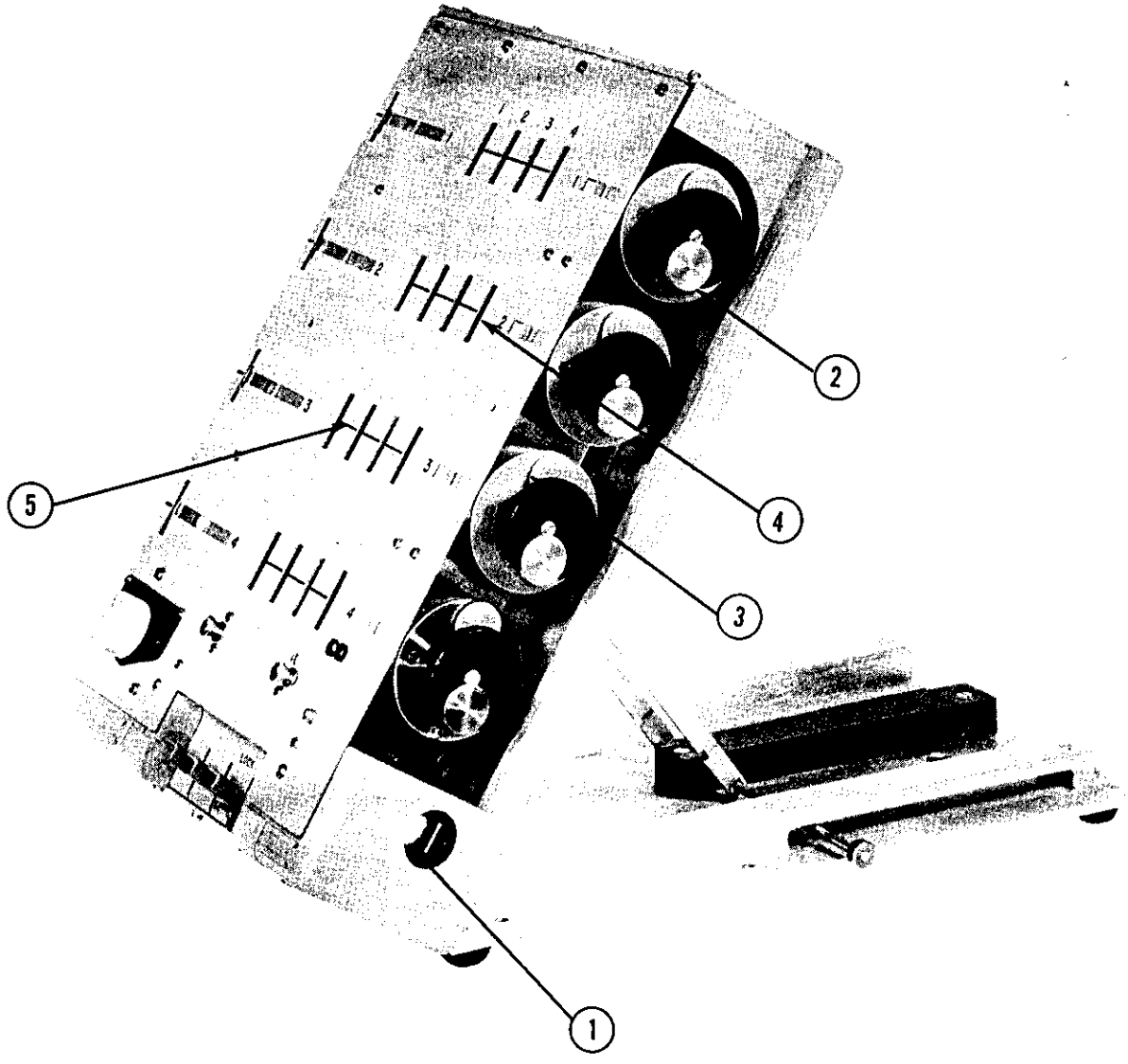

Figure 3.—KL-4, Side View

1. Set-Up Blocking Bar
2. Vernier Adjustment
3. Pressure Roller Knob
4. Addition Rotor Window
5. Index Mark

up the key values appearing in key value Window No. 2 on the addition rotors in Column No. 2, etc. This is accomplished as follows:

(1) Rotate the first (top) addition rotor setting knob in either direction until the addition rotor in Row 1 Column 1 presents the first character of the key value group displayed in key value Window No. 1. (See fig. 2, #9.)

(2) Rotate the second addition rotor setting knob until the addition rotor in Row 2 Column 1 presents the second character of the key value group displayed in key value Window No. 1.

(3) Rotate the third knob until the addition rotor in Row 3 Column 1 presents the third character of the key value group displayed in key value Window No. 1.

(4) Rotate the fourth (bottom) knob until the addition rotor in Row 4 Column 1 presents the fourth character of the key value group displayed in key value Window No. 1.

f. Push in the set-up blocking bar and pull down the column set-up lever for Column 2.

g. Align the addition rotors in Column 2 to the key value characters presented in key value Window No. 2.

h. Follow the above procedures for Columns 3 and 4, using the key value characters for key value Windows 3 and 4, respectively.

i. The encrypted call sign may now be read vertically from the output windows. The first character of the call sign is read from output Window No. 1, second character from output Window No. 2, and so forth.

3103. Encryption Check.—Each time a call sign is encrypted on the KL–4 a check must be made of the accuracy of the encryption. This is done in the following sequence:

a. Check to determine that the correct input characters are aligned against the index marks.

b. Check to determine if the key values in key value Window No. 1 are displayed down the first column of addition rotors.

c. Check to determine if the key values in key value Windows 2, 3, and 4 are displayed down addition rotor Columns 2, 3, and 4, respectively.

d. If any errors are found it is necessary to correct only the particular addition rotor or rotors affected.

3104. Sequence of Operations in Decryption.—Decryption is accomplished in the following manner:

a. Insure that the equipment is keyed for the same cryptoperiod during which the call sign was encrypted. If not, re-key the equipment with the proper key strips or use the alternate procedure (see sec. 3200).

b. Move the Encrypt-Decrypt Knob to the decrypt position for the cryptoperiod required.

c. By means of the input knobs, set up the four characters of the encrypted call sign in the input windows.

d. Push in the set-up blocking bar with the right index finger and simultaneously pull down the column set-up lever for Column 1 of the addition rotors.
(1) Rotate the first addition rotor setting until the addition rotor in Row 1 Column 1 presents the first character of the key value group appearing in key value Window No. 1.
(2) Rotate the second knob until the addition rotor in Row 2 Column 1 presents the second character from key value Window No. 1.
(3) Rotate the third knob until the addition rotor in Row 3 Column 1 presents the third character from key value Window No. 1.
(4) Rotate the fourth (bottom) knob until the addition rotor in Row 4 Column 1 presents the fourth character from key Window No. 1.

e. Push in the set-up blocking bar and pull down the column set-up lever for Column 2.

f. Align the addition rotors in Column 2 to the key value characters presented in key value Window No. 2.

g. Follow the above procedures for Columns 3 and 4, using the key value characters in value Windows 3 and 4, respectively.

h. The decrypted intermediate group may now be read vertically from the open output windows. The first character of the intermediate group appears in output Window No. 1, the second character appears in output Window No. 2, and so forth.

i. This four-character intermediate group must then be converted to the plain call sign/address group in accordance with the procedures in Chapter 1.

3105. Stacking Call Signs.—When a number of 4-character groups are to be encrypted, a savings in encryption time may be obtained through stacking groups having positional characters in common. In the KL–4 operation, each column of addition rotors corresponds to a positional character in the input group. The four key values for the first character of any input group are always aligned on the four rotors in the first column of addition rotors; the key value group for the second input character is always inserted into the second column of addition rotors, etc. For a given cryptoperiod, a given positional input character retains the same key value group, and consequently requires the same alignment for its corresponding column of addition rotors. If input groups (to be encrypted or decrypted) are stacked so that a succession of groups have the same positional character(s), no change of addition rotors in the corresponding rotor column(s) is necessary. For example, if the plain input group ABCD is encrypted followed by an encryption of ABJR, the addition rotors in Columns 1 and 2 would not be changed for the encryption of the latter group. Similarly, if ARDR were encrypted after an encryption of ABJR, addition rotors in Columns 1 and 4 would not be changed. Stacking for encryption is accomplished in the following manner:

a. Convert the call sign/address groups to their appropriate intermediate groups, in accordance with procedures described in Chapter 1, using the digraph table in the effective edition of KAL–15.

b. Arrange the intermediate groups so that there is a maximum number of positional repeats among successive groups. The following example illustrates three different ways of stacking the same five intermediate groups.

STACK 1	STACK 2	STACK 3	STACK 4
F U 3 2	M V D X	F U 3 2	M V D X
F K 3 1	0 C N X	0 K 5 2	0 C N X
0 K 5 2	0 K 5 2	F K 3 1	
0 C N X	F U 3 2		
M V D X	F K 3 1		

After encryption of the first 4-character group in a stack (using procedures in par. 3100) it is unnecessary to change the four addition rotors in the column(s) of rotors corresponding to the underlined characters. Note that in Stack 1 after encrypting FU32, only the second and fourth column of addition rotors need be changed to encrypt 0K52. To encrypt the five groups in Stack 1, 15 addition rotor columns must be aligned; the same number of columns must be aligned when the five groups are stacked as shown in Stack 2. However, when the same five groups are placed in two stacks as illustrated in Stacks 3 and 4, 17 columns of rotors must be aligned. If the five groups were not stacked, 20 columns of rotors would need to be aligned to encrypt the five groups. If it is anticipated that call sign/address groups to be encrypted will remain fairly constant for a month, care should be taken in stacking their intermediate groups so that a minimum of encryption effort will be required.

3200—ENCRYPTION-DECRYPTION, ALTERNATE METHOD

3201. General.—Provision has been made to permit use of KL–4 with keying material normally used with the KA–2 (CSP 1750). This latter keying material may be used when it is necessary to encrypt/decrypt groups using keying material effective for a cryptoperiod different

from that for which the KL–4 is keyed. (For example, it may be necessary to decrypt a call sign encrypted on the 5th day of the month when the KL–4 is loaded with key effective for the 7th and 8th days of the month.) KAL–15 (or AMSP 298) keying material can be used with the KL–4 by following essentially the same procedures as required for KA–2 operation.

3202. Encryption.

a. Process the plain call sign/address group through the appropriate digraph table in the effective edition of KAL–15 (or AMSP 298) in accordance with instructions in Chapter 1 and obtain an intermediate group.

b. Turn to the ENCIPHER side of the KAL–15 (or AMSP 298) key card effective for the cryptoperiod desired.

c. For the first character of the intermediate group, locate its 4-character key value group in Column 1 of the key card ENCIPHER. Reading the characters of the key value group from left to right enter them from top to bottom (addition rotors 1 through 4, respectively) in the first column of addition rotors, using the procedures described in paragraphs 3102*e* thru *h*.

d. For the second character of the intermediate group, locate its 4-character key value group in Column 2 of the key card, and then insert these key value characters into the second addition rotor column of the KL–4.

e. Continue with the same process for the third and fourth characters of the plain group, placing their key value groups in rotor Columns 3 and 4, respectively.

f. Now push down the numerical equivalent reading lever and read the four 2-digit numbers appearing in the numerical equivalent windows.

g. Return to the ENCIPHER card and locate the four mixed PENELOPE alphabets adjacent to the numbers 00 through 36 on the extreme right side of the key card.

h. In the mixed PENELOPE alphabet immediately adjacent to the column of numbers 00–36 (Col. 1), is found the cipher equivalent for the 2-digit number appearing in the numerical equivalent Window No. 1; this is the first character of the encrypted call sign/address group.

i. In the next succeeding PENELOPE alphabet column, (Col. 2), located on the line corresponding to the number appearing in Window No. 2, is found the cipher equivalent which is the second character of the encrypted group.

j. Continue the process to convert the numbers appearing in Windows 3 and 4, respectively, to their cipher equivalents.

k. The resulting four characters constitute the encrypted call sign/address group.

3203. Decryption.

a. Turn to the DECIPHER side of the appropriate key card.

b. Locate the first character of the encrypted group in Column 1 and obtain the 4-character key value group adjacent to it; reading from left to right enter this group from top to bottom (addition rotors 1 through 4, respectively) in the first column of addition rotors, using procedures described in paragraphs 3104*d* thru *g*.

c. In a similar manner, obtain the key value groups for the second, third and fourth characters of the encrypted call sign/address group from Columns 2, 3, and 4, respectively, of the DECIPHER card and insert these key value groups into addition rotor Columns 2, 3, and 4, respectively, of the KL–4.

d. Now push the numerical equivalent reading lever and read the four 2-digit numbers appearing in the numerical equivalent windows.

e. Return to the DECIPHER card and locate the four mixed PENELOPE alphabets adjacent to the numbers 00–36 on the right side of the card.

f. In the mixed PENELOPE alphabet immediately adjacent to the column of numbers 00–36, (Col. 1), is to be found the decipher equivalent for the 2-digit number appearing in numerical equivalent Window No. 1; this is the first character of the intermediate group.

g. In the next succeeding PENELOPE alphabet column, (Col. 2), located on the line corresponding to the number appearing in Window No. 2, is found the decipher equivalent which is the second character of the intermediate group.

h. Continue the process of converting the numbers appearing in Windows 3 and 4, respectively, to their decipher equivalents.

i. The resulting four characters constitute the intermediate group which must then be converted to a plain call sign/address group by using the digraph table in the effective edition of KAL–15 (AMSP 298).

3204. Encryption/Decryption Check.

a. Locate the respective key value groups; have one operator read the characters of the group which should appear in a specified addition rotor column of the KL–4 while another operator visually checks the rotors to assure that the correct key values appear on the corresponding rotors.

b. If an error is noted, the operator performing the visual check of the rotors can make the correction by activating the rotor column in which the error is located and moving the appropriate addition rotor setting knob in either direction to display the correct key value.

c. The operator then pushes the numerical equivalent reading lever to display the four 2-digit numbers in numerical equivalent windows; he should read these numbers slowly from top to bottom while another operator locates the cipher/decipher equivalents of each number and compares them with the previously obtained encrypted/decrypted intermediate group.

CHAPTER 4

CRYPTOSECURITY

4000—GENERAL

4001. Possible Compromises.

a. The violation listed below is considered a possible compromise and shall be reported in accordance with the procedures outlined in the effective edition of KAG-1 or AMSP 293, as appropriate.

(1) Any improper or erroneous keying of the input or output drums which results in:

(a) the transmission of 6 or more call signs encrypted with improper key, and

(b) the subsequent transmission of the same messages with these same calls correctly encrypted using the proper key.

b. This violation is normally reported by means of a ROUTINE message.

4002. Practices Which are Prohibited.—Extreme caution must be exercised to avoid the following:

a. Any improper or erroneous transmission of 5 or fewer call signs, as outlined in paragraph 4001 above.

b. Transmission of an intermediate group in the clear.

c. Transmission of any of the 4-character key value groups, which appear on the KAL-9 key lists, in the clear.

No reports of violations of these practices are required.

KAO-64C/TSEC

ORIGINAL
(Reverse Blank)