505-4

KAO-41C/TSEC

REG NO 6283

CRYPTO CRYPTO

OPERATING INSTRUCTIONS
FOR
TSEC/KL-7 — ADONIS OPERATION

HANDLING INSTRUCTIONS

1. This publication consists of a cover and numbered pages 1 through 27 inclusive. Verify presence of each page upon receipt.
2. Formal authorization for access to Cryptomaterial is required for personnel to have access to this document.
3. This publication becomes effective upon receipt and will supersede KAO-41B/TSEC which may be destroyed.
4. Extracts from this publication may be made if necessary. Such extracts will be classified CONFIDENTIAL, marked CRYPTO, and accounted for locally until destroyed.
5. This publication may be carried in aircraft for use therein.
6. ESPIONAGE LAWS, TITLE 18, U. S. C., SECTIONS 793, 794, AND 798 APPLY.

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

September 1966

CRYPTO CRYPTO

ORIGINAL
(Reverse Blank)

RECORD OF AMENDMENTS

Identification of Amendment and Accounting No. (if any)	Date Entered	By Whom Entered (Signature, Rank or Rate; Name of Command)
Amend 1 S/311 1191382 S67	10 June 80	CSE
Amend 2 S1/0071-73	10 June 80	CSE
Amend 3 25 15412 3/80	10 June 80	CSE

s.15(1)

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)
Rec'd, read 10/5/28			

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

CHAPTER 2

CHAPTER 3

TABLE OF CONTENTS (Continued)

CHAPTER 4

CHAPTER 5

CHAPTER 1

1000—INTRODUCTION

1001. ADONIS Cryptosystems.—The mythological designator ADONIS applies to the general cryptosystem produced by the cipher machine TSEC/KL-7 and TSEC/KL-47. Certain ADONIS cryptosystems, designated specifically for tactical use, are referred to as "tactical ADONIS" cryptosystems.

a. Category of Cryptosystems.—Cryptosystems employing the KL-7 are Category A as explained in the effective edition of KAG-1/TSEC.

b. Intercommunicability.—The KL-7 is cryptographically intercommunicable with the cipher machine KL-47, which is designed primarily for US Navy use. The KL-47 will encrypt not only lower case characters (letters) and numbers, but also will encrypt punctuation marks. When it is necessary for stations using the KL-47 to communicate with stations using the KL-7, all punctuation marks will be spelled out, using authorized abbreviations, in order to avoid garbles.

c. KAG-1 Reference.—The effective edition of KAG-1/TSEC or appropriate service directives will be consulted on all general cryptographic procedures such as dividing messages into message parts, codress format, system selection, insertion of classification and special handling instructions, reporting violations, etc.

1002. Amendments.—Amendments to this publication will be issued by means of printed or electrically transmitted amendments, and are to be entered upon receipt. Individuals entering such amendments shall so indicate on the "Record of Amendments" page included herein as page 1.

1003. Authorization for Use.—ADONIS cryptosystems are authorized for the encryption of messages of all classifications. Except in emergency conditions, the classification of messages shall not exceed the classification of the key list or extract to be employed.

1004. Use with Other Equipments.—Through use of the KLX-7 keyboard adaptor, the KL-7 may be operated with the TSEC/HL-1 or TSEC/HL-1B electromechanical tape reader to provide semi-automatic encryption and decryption. When the HL-1 or HL-1B is used, this publication shall be used with the effective edition of KAO-109/TSEC.

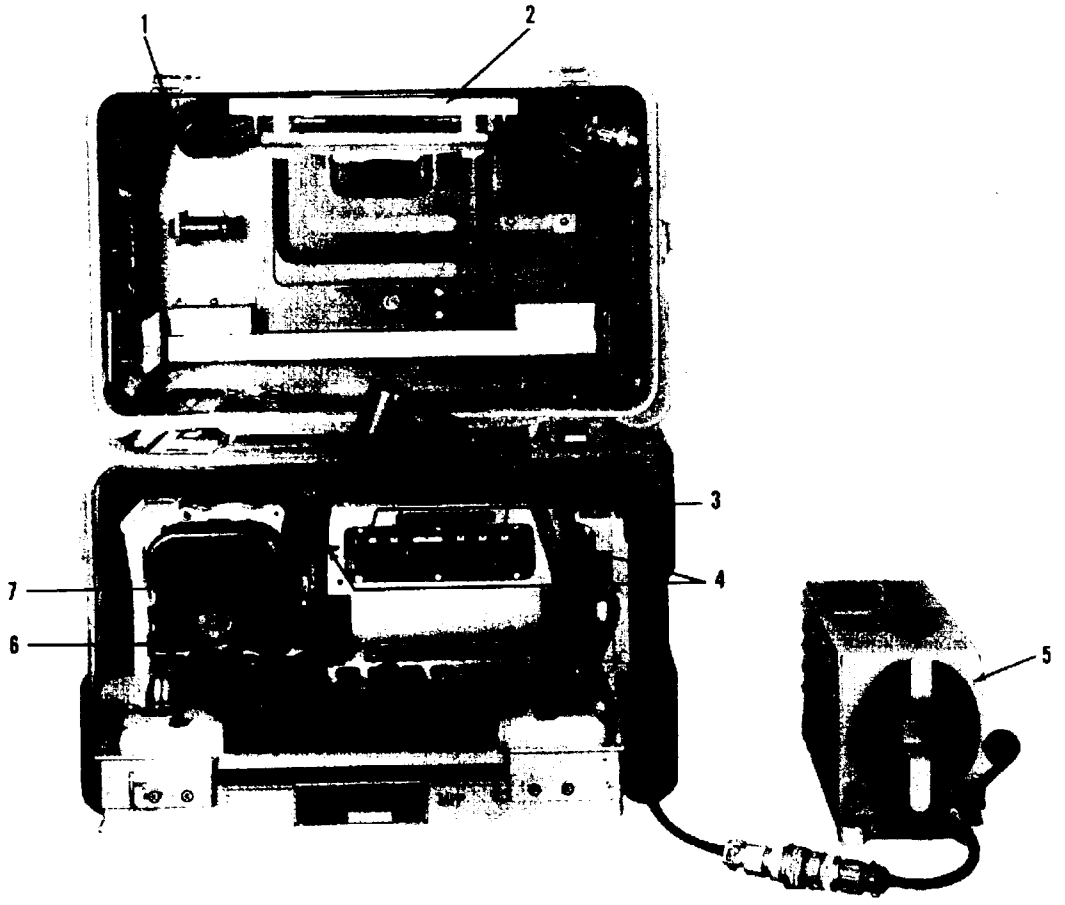
1005. Comments and Recommendations.—Comments and recommendations concerning the instructions contained herein are invited and may be submitted through the appropriate Agency, Department, or Service Cryptologic Agency to the Assistant Director, National Security Agency, 3801 Nebraska Avenue, N. W., Washington, D. C. 20305.

1100—DESCRIPTION

1101. General.—The KL-7 is a keyboard operated, tape printing cipher machine which consists of three major components; KLA-7/TSEC, rotor stepping unit, KLK-7/TSEC, cipher unit, and KLB-7/TSEC, base. The KLK-7 has a shaft on which eight rotor assemblies are mounted and is removed from the machine by lifting the latches on both sides of the unit (see figs. 1 and 2).

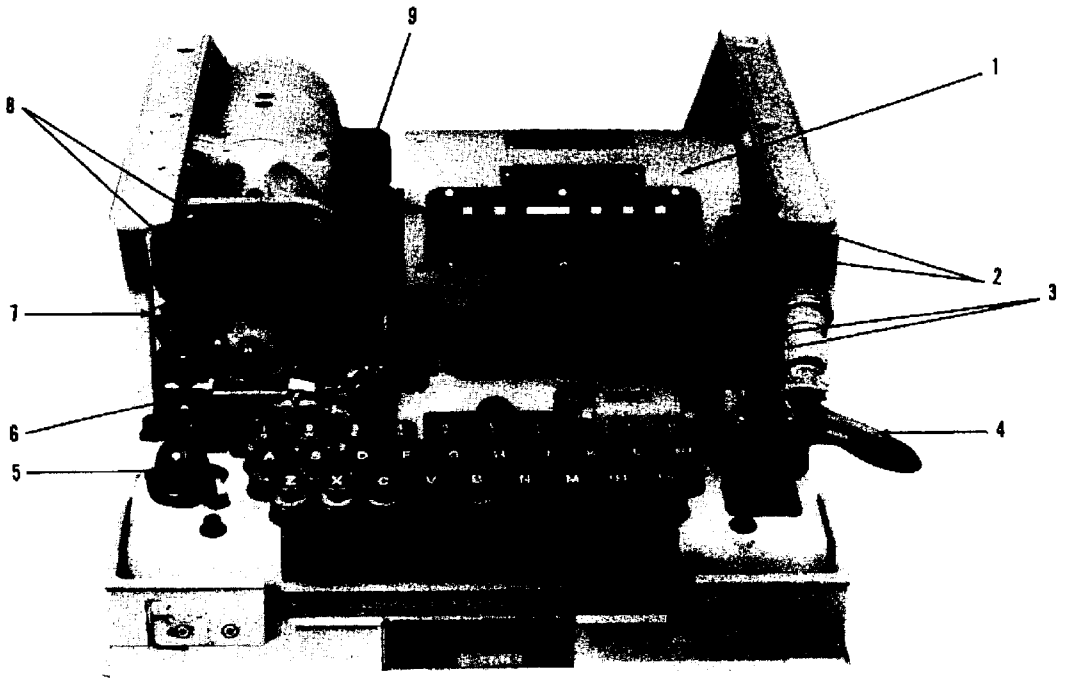
1102. Keyboard.—The keyboard resembles a teletypewriter keyboard and has a FIG (Figures), LET (Letters) and RPT (Repeat) key. When the RPT key is depressed together with any operative key, the unit will operate continuously until the RPT key is released. Depressing the FIG key causes the printer to shift to upper case so the keys in the top row will print figures. The LET key causes the printer to return to lower case and print only letters. The neon glow lamp at the rear of the keyboard lights when the FIG key is depressed and is extinguished when the LET key is used.

1103. Power Requirements.—The KL-7 is operated from a 21-31 volt DC power supply. A power converter may be obtained for 100-125 volt or 200-250 volt (50-60 cycle) alternating current.



1. Carrying Case Cover
2. Copy Holder
3. Cipher Unit Assembly Index Marks
4. Cipher Unit Latch Assemblies
5. AC Power Converter Assembly
6. Tape Release Lever
7. Paper Tape Container

Figure 1.—TSEC/KL-7, with Carrying Case.



1. Cipher Unit Assembly
2. Cipher Unit Latch Assemblies
3. Set Keys
4. Power Cable
5. Selector Handle
6. Paper Tape Holder
7. Tape Release Lever
8. Ribbon Spools
9. Swivel Pin (For Changing Tape)

Figure 2.—TSEC/KL-7, Top View.

1200—PHYSICAL SECURITY

1201. General.—The KL-7 has been approved for use in both mobile and fixed station environments.

1202. Access Requirements.—Operators must have a clearance at least as high as the level of classified traffic to be passed, with a minimum of CONFIDENTIAL. The following table is to be used as a guideline for personnel responsible for the KL-7 and associated publications. For exceptions in using KL-7 in Forward Areas, see paragraph 1300.

1203. Telephone Handsets.—No telephone handsets shall be operated within sound range of the KL-7 during setup, check, encipher or decipher operations unless the telephone is approved for transmission in the clear of information classified at least as high as that of the key lists in use.

1204. Emergency Actions.—Holders of classified cryptomaterial and equipment will prepare an emergency plan in accordance with effective edition of KAG-1 or separate service instructions (see also par. 1305).

Item	Classification	Crypto Access Auth	Remarks
KL-7 External Viewing			See para. 1304*c*.
KLA-7 Rotor Stepping Unit	CONFIDENTIAL	YES	
KLB-7 Base	UNCLASSIFIED	NO	
KLK-7 Cipher Unit	CONFIDENTIAL	YES	See Note 1.
KAR- Rotor Set	SECRET/ CONFIDENTIAL	YES	See Note 2.
KAK- Key Lists	All Class.	YES	
KAO-41C Operating Instructions	CONFIDENTIAL	YES	
KAM-1 Maintenance Manual	CONFIDENTIAL	YES	
Accessories Case (Complete)	CONFIDENTIAL	YES	See Note 3.

Note 1: A cipher unit with rotor maze installed assumes the same classification as its key list.

Note 2: Tactical ADONIS rotors are CONFIDENTIAL; all others are SECRET.

Note 3: Only the spare KLK-7 is classified; if removed, case is UNCLASSIFIED.

1300—FORWARD AREA USE

1301. General.—The following modified procedures for handling and safeguarding the KL-7 and associated materials may be applied when the KL-7 is using "tactical ADONIS" rotors and key lists and is issued for mobile or forward area use.

1302. Keying Material.—See chapter 2 for further information on the classification of "tactical ADONIS" rotors and extracts from "tactical" key lists.

1303. Access.

a. Operators must have a clearance at least as high as the level of classified traffic to be passed, with a minimum of CONFIDENTIAL. Only those individuals whose duties require detailed and continuing access to keying material must have formal authorization for access to cryptomaterial.

b. Up to seven day's extracts of tactical keying material may be provided to personnel not having formal CRYPTO authorization.

c. Personnel assigned to guard vehicles, ships, or aircraft containing KL-7's do not require clearance or formal CRYPTO authorization but they must be responsible and trustworthy U. S. Military personnel or U. S. Government employees. (Contract personnel who are assigned to this duty must have an appropriate clearance.)

1304. Physical Safeguarding.

a. For use in mobile or forward area operations where the possibility of loss or compromise is high, sets of rotors must be afforded the same protection as key lists or key list extracts. The KL-7 may be considered to be unkeyed when the rotors and all key settings are removed and separately safeguarded. When the rotors are in place or immediately available, whether they are set to an operational setting or not, the KL-7 must receive the same physical security protection as a keyed equipment.

b. During mobile operations the amount of supporting material carried should be kept to a minimum. Use of brief key list extracts and the exclusion of maintenance manuals unless mobile maintenance facilities are to be established are examples of such reductions. When necessary, the KL-7, key lists, operating instructions and maintenance manuals may be air dropped. Equipment drops should be made so that immediate possession by U. S. personnel is probable on the ground. Key lists, rotors, operating instructions, and maintenance manuals (if carried) should be dropped in the possession of properly cleared and authorized personnel. When the situation will permit, air landing is preferred to an air drop for all cryptomaterial and especially for rotors, key lists and maintenance manuals.

c. External viewing of the KL-7 when not operating is unclassified, but should be prevented to the maximum extent feasible, especially when the rotors are installed. Viewing of the KL-7 in operation may reveal details of cryptographic operating procedures and should be denied unauthorized personnel.

d. When the rotors are removed from the KL-7 it may be stored in an area under control of U. S. Military personnel or U. S. Government employees. For example, the vehicle or aircraft in which a KL-7 is mounted may be parked in a guarded motor pool or airstrip, or the KL-7 may be left in the command post under control of the charge of quarters. The following requirements must be met for such storage.

(1) The individual responsible for the KL-7 must assure himself that protective measures against theft of the equipment have been officially provided before he leaves it, e.g., that the area is guarded.

(2) The KL-7 must be checked at least daily to insure that it is not missing, and if it is missing, immediate action to recover it shall be taken.

(3) A report must be promptly initiated if the equipment is missing. Such reports will be in accordance with established procedures for reporting the compromise of cryptomaterial as modified to meet operational necessity.

(4) KL-7's mounted in vehicles, aircraft or ships for use in maneuvers or in actual combat, need not be removed from such vehicles, aircraft or ships when they are returned to normal garrison type operations. The KL-7's must be provided with at least the minimum physical security required by (1), (2) and (3) above, and all key lists, rotors and associated documents must be removed and placed in separate secure storage (see *f* below). For example, a KL-7 mounted in a van for field maneuvers may be left in the van upon return to garrison duty and protected in a guarded motor pool.

e. Key lists, rotors, and associated materials may be protected in any of the following ways, or in the case of operational necessity, as best feasible under the circumstances.

(1) Kept under the continuous personal control of cleared personnel (formal authorization is not required).

(2) Stored in an approved storage container (see KAG-1).

(3) Stored in a reasonably secure container such as a field safe, secured by an approved three combination padlock inside an area under the control of U. S. Military personnel or U. S. Government employees, for example, a field safe in a van in a guarded motor pool.

(4) Stored in any reasonable container, such as a foot locker, equipped with an approved three combination padlock which is kept under the continuous control of responsible U. S. Military personnel or U. S. Government employees assigned as guards and instructed to prevent direct physical access by unauthorized personnel.

f. The KL-7 must be protected as though keyed whenever the rotors, whether set to an operational setting or not, are installed in the KL-7 or if not installed, are immediately available in the same area. A keyed KL-7 shall be kept under the continuous control of responsible U. S. Military personnel or U. S. Government employees with specific instructions to prevent close inspection or direct physical access to the material by unauthorized personnel.

1305. Emergency Actions.—When necessary to prevent physical compromise or capture of ADONIS cryptomaterials, emergency destruction may be necessary. The following are destruction priorities (consult KAG-1 for approved methods).

a. Destroy superseded key lists and extracts, followed by current and future key lists.

b. Disassemble rotors completely. Remove the wiring of rotors by unplugging and cutting and ripping them loose from their soldered connections.

c. Destroy the notch rings by hammering and crushing or by incendiary means. Scatter remains in dumps, sewers, wooded areas, water, etc.

d. Destroy the operating and maintenance instructions.

e. Render the remaining components unusable. If time permits, the rotor stepping unit (KLA-7), the cipher unit (KLK-7), the stationary (wide) ring assembly, and unassembled rotors should be destroyed by disassembly, hammering, or through the use of thermite incendiary devices.

CHAPTER 2
2000—KEYING

2001. ADONIS Rotors.

a. Each ADONIS rotor set consists of twelve rotor cores, eleven notch rings and a stationary wide ring. An alphabet ring is permanently mounted on each rotor core. When a rotor is assembled, a notch ring (or the stationary ring) is locked on the rotor core in accordance with instructions. Eight rotor assemblies, selected from the set of twelve, are used in ADONIS operation.

b. ADONIS rotor sets are SECRET—CRYPTO and registered, except those specifically designated for tactical use, which are CONFIDENTIAL—CRYPTO and registered. Each set is identified by a short title (KAR followed by a number) and a register number (e.g., KAR-1234 Reg Nr 6). Each core is identified by a single letter from A through L. Each notch ring is identified by a number from 1 through 11. The numbers 1 through 36 appear on the [illegible] side of each alphabet ring and the stationary [illegible] side ring.

2002. Key Lists.

a. Key lists used with the KL-7 bear the designator ADONIS. ADONIS key lists are classified CONFIDENTIAL, SECRET or TOP SECRET and are marked CRYPTO.

b. The system indicator for an ADONIS key list is either a four-digit or a five-letter group which identifies the specific ADONIS key list used in encryption. Digital system indicators are always encrypted. Instructions for the encryption of digital indicators are contained in the separate keying material issued for their encryption. The assignment of digital system indicators to specific key lists is disseminated in the effective edition of KAG-18-1 or by special instructions to key list holders. Key lists employing literal indicators will have either a single indicator assigned for all succeeding editions of the key list or will have daily changing indicators listed for each days key setting. On occasion, key lists with literal indicators may also be assigned digital indicators. When this occurs, holders of the key list will be advised as to which indicator is to be used. Normally it will be the digital indicator.

c. The following information is applicable to extracts from ADONIS key lists.

(1) Regular printed key lists contain keying data for one month. Extracts from these printed key lists shall contain no more than seven days' keying data and will be marked CRYPTO and bear the same classification as the key list from which extracted.

(2) Master key lists may contain keying data for more than 31 days. Extracts from master key lists shall contain no more than seven days' keying data and need not be marked CRYPTO. Master key lists are issued for use in tactical ADONIS operation only.

(3) Key list extracts are not registered, but should be assigned copy numbers for local accounting until destroyed.

(4) The short title of the key list may appear on an extract if desired for convenience, but this short title should be preceded by the words "Extract of".

(5) Extracts from SECRET master key lists shall be classified either SECRET or CONFIDENTIAL, depending on the highest classification of the traffic to be encrypted using the keying data involved.

d. Normally, no ADONIS key list or extract thereof will be used for encryption of messages of higher classification than that of the key list or extract to be employed. Except in emergency conditions, TOP SECRET messages shall be encrypted using TOP SECRET key lists only.

e. Key lists specifically designated for training purposes shall not be used for the encryption of operational traffic.

CHAPTER 2

2000—KEYING

2001. ADONIS Rotors.

a. Each ADONIS rotor set consists of twelve rotor cores, eleven notch rings and a stationary wide ring. An alphabet ring is permanently mounted on each rotor core. When a rotor is assembled, a notch ring (or the stationary ring) is locked on the rotor core in accordance with instructions. Eight rotor assemblies, selected from the set of twelve, are used in ADONIS operation.

b. ADONIS rotor sets are SECRET—CRYPTO and registered, except those specifically designated for tactical use, which are CONFIDENTIAL—CRYPTO and registered. Each set is identified by a short title (KAR followed by a number) and a register number (e.g., KAR-1234 Reg Nr 6). Each core is identified by a single letter from A through L. Each notch ring is identified by a number from 1 through 11. The numbers 1 through 36 appear on the side of each alphabet ring and the stationary wide ring.

2002. Key Lists.

a. Key lists used with the KL-7 bear the designator ADONIS. ADONIS key lists are classified CONFIDENTIAL, SECRET or TOP SECRET and are marked CRYPTO.

b. The system indicator for an ADONIS key list is either a four-digit or a five-letter group which identifies the specific ADONIS key list used in encryption. Digital system indicators are always encrypted. Instructions for the encryption of digital indicators are contained in the separate keying material issued for their encryption. The assignment of digital system indicators to specific key lists is disseminated in the effective edition of KAG-18-1 or by special instructions to key list holders. Key lists employing literal indicators will have either a single indicator assigned for all succeeding editions of the key list or will have daily changing indicators listed for each days key setting. On occasion, key lists with literal indicators may also be assigned digital indicators. When this occurs, holders of the key list will be advised as to which indicator is to be used. Normally it will be the digital indicator.

c. The following information is applicable to extracts from ADONIS key lists.

(1) Regular printed key lists contain keying data for one month. Extracts from these printed key lists shall contain no more than seven days' keying data and will be marked CRYPTO and bear the same classification as the key list from which extracted.

(2) Master key lists may contain keying data for more than 31 days. Extracts from master key lists shall contain no more than seven days' keying data and need not be marked CRYPTO. Master key lists are issued for use in tactical ADONIS operation only.

(3) Key list extracts are not registered, but should be assigned copy numbers for local accounting until destroyed.

(4) The short title of the key list may appear on an extract if desired for convenience, but this short title should be preceded by the words "Extract of".

(5) Extracts from SECRET master key lists shall be classified either SECRET or CONFIDENTIAL, depending on the highest classification of the traffic to be encrypted using the keying data involved.

d. Normally, no ADONIS key list or extract thereof will be used for encryption of messages of higher classification than that of the key list or extract to be employed. Except in emergency conditions, TOP SECRET messages shall be encrypted using TOP SECRET key lists only.

e. Key lists specifically designated for training purposes shall not be used for the encryption of operational traffic.

f. Key settings change daily. Each key list contains the following information for each date.

(1) A list of the cores to be placed in the eight positions in the cipher unit.

(2) The settings of the alphabet rings for seven cores.

(3) The setting of the stationary ring on the core in the fourth position.

(4) The notch rings to be used with seven cores (listed in conjunction with the letter of the alphabet ring to which the notch ring bench marks are set).

(5) The 36-45 letter check groups.

(6) The system indicator to be used for the GMT date of encryption for those key lists employing daily changing indicators.

g. Rotor assemblies are listed from left to right in the order in which they are to be inserted in the cipher unit. The arrangement of the keying data in an ADONIS key list is illustrated below.

Note 1: Blank spaces on alphabet rings are indicated in key lists by the letters which precede them in the alphabet printed in conjunction with a plus sign (+). Thus, "J+" indicates the space between the letters J and K, "M+" indicates the space between M and N, etc. There are ten such spaces on each alphabet ring.

Note 2: Some key lists will contain a second column of letter check groups separated by a heavy black line from the other keying data. The KAR on which the additional letter check groups are based is indicated at the top of the column. Ordinarily this KAR will have been superseded. The group in this additional column shall be used only when higher authority directs that the specified KAR will be used beyond its normal supersession date.

Amend 3. (Use of sample Key List is prohibited for on-the-air use)

Sample Key List

POSITION IN MACHINE	1			2			3			4		5			6			7			8			
DATE	CORE	ALPH RING SET	NOTCH RING & SET	CORE	ALPH RING SET	NOTCH RING & SET	CORE	ALPH RING SET	NOTCH RING & SET	CORE	MODE RING SET	CORE	ALPH RING SET	NOTCH RING & SET	CORE	ALPH RING SET	NOTCH RING & SET	CORE	ALPH RING SET	NOTCH RING & SET	CORE	ALPH RING SET	NOTCH RING & SET	36-45 LTR CHECK GRP
	H	24	8- D	A	12																			ATSU/KAH

ND 2

NEW KEY L[redacted]T OF

CCTED ADONIS KEY LISTS HAS BEEN CHANGED. [redacted] FORM

KEY LIST IS A SIX FOUR PAGE BOOKLET CONTAINING THREE ONE

OF KEY WITH A SCRAMBLE DESIGN PATTERN ON THE REVERSE OF

#L PAGES. THE LAST @ PAGES IN THE BOOK ARE BLANK. THE

S ARE ASSEMBLED KEY SIDE DOWN WITHIN A FRONT AND BACK

R THAT CONTAIN HANDLING INSTRUCTIONS AND A DISPOSITION

RD. THE INDIVIDUAL PAGES ARE PERFORATED FOR EASE OF

VAL. NEW KEY LIST PACKAGING FEATURES GLUING THE SIDES OF

BOOKLET TOGETHER WITH A YELLOW GLUE PAINTED OVER WITH

OM STRIPES OF ANOTHER COLOUR, LEAVING ONE CORNER OPEN FO

ER OPENING AND REMOVAL OF PAGES.THE FINISHED BOOKLET IS

OXOMATELY 3 INCHES BY 4 INCHES AND WILL BE PACKAGED IN A

TIC WRAPPER.THIS WRAPPER MUST NOT BE REMOVED FROM THE KE

PRIOR TO 24 HOURS BEFORE IMPLEMENTATION.THE BOOKLET

LD BE OPENED CAREFULLY TO AVOID TEARING PAGES. THE FRONT

R MAY BE LOOSENED BY SLIPPING A SHARP INSTRUMENT SUCH AS

E INTO THE OPEN CORNER OF THE BOOKLET AND RUNNING IT ARO

GLUED EDGES OF THE PAGE. AS NEEDED INDIVIDUAL PAGES MAY

ENED IN THE SAME WAY.

2100—KEYING INSTRUCTIONS

2101. Selection, Assembly and Arrangement of Rotors.—The elements of the rotors are selected and assembled to settings appearing in the key list for the GMT date of encryption and are then placed in the cipher unit in the order in which they are listed in the key list. The key list contains eight numbered columns, one for each of the eight rotor assemblies used. Rotors are assembled as shown in figures 3(1) through 3(4) on pages 16 and 17. The example uses the sample key list depicted above and the photographs show the assembly of rotors in the first and the fourth columns of that key list.

a. Each column of the key list designates a rotor core to be used in that position of the rotor maze. An alphabet ring is permanently mounted on each rotor core. The alphabet ring is set by pressing down on the ring and rotating it to align the designated number with the bench mark arrow on the flat side of the rotor core.

b. The notch ring to be used with each core is specified by the key list. The notch ring is placed on the rotor core by aligning the notch ring arrow beside the small hole which appears on the edge of the rotor core on the pressure contact side. The notch ring is set by pressing down on the ring aligning its bench marks until they bracket the designated letter on the associated alphabet ring.

c. The stationary wide ring is placed on the rotor core in the same manner as the notch ring. It is aligned to the proper setting by placing the designated number beside the small hole on the pressure contact side of the rotor.

d. After assembly, check each rotor to insure that it is assembled according to the settings appearing in the key list, and that neither the notch ring nor alphabet ring will rotate relative to the core. Place each rotor in the cipher unit as soon as assembled. ADONIS ROTORS ARE NOT REVERSIBLE, AND MUST ALWAYS BE PLACED IN THE CIPHER UNIT WITH THE FLAT SIDE IN. The stationary wide ring assembly must always be placed in the fourth position in the cipher unit.

e. After insertion of the assembled rotors in the cipher unit, replace the endplate making certain the endplate latch is engaged in the grooves on the shaft and place the cipher unit on the stepping unit. Make certain the two latches are then securely engaged.

f. Rotors are disassembled by reversing the above procedures.

2102. 36-45 Letter Check.

a. The 36-45 letter check groups are provided in the key lists as a means of performing a check on the operation of the machine and upon the correctness of the rotor assembly and arrangement. The letter check is made in the following manner:

(1) After the rotors have been assembled and placed in the cipher unit, and the cipher unit has been placed in the machine, turn the selector handle to "P" (Plaintext). Allow time for the machine to warm up. It is ready for operation when the keyboard will print.

(2) Hold back the tape release lever (see figs. 1 and 2), which is located to the upper left of the paper tape feed roll (to save tape), and align to the white bench marks on the cipher unit the seven visible rotors to AAAAAAA by depressing each of the rotor-set keys. The rotor-set keys are located below the rotor windows when the cipher unit is in place.

(3) Turn the selector handle to "E" (Encrypt). (Note that the rotor maze steps once.)

(4) Set the stroke counter to zero. Press and hold the "L" key; while holding the "L" key, press and hold the "RPT" key until at least 45 letters (nine groups) have been printed on the tape.

CAUTION:

DO NOT USE ANY OF THE FIVE-LETTER GROUPS APPEARING ON THE TAPE AS THE MESSAGE INDICATOR OR THE MESSAGE ROTOR ALIGNMENT.

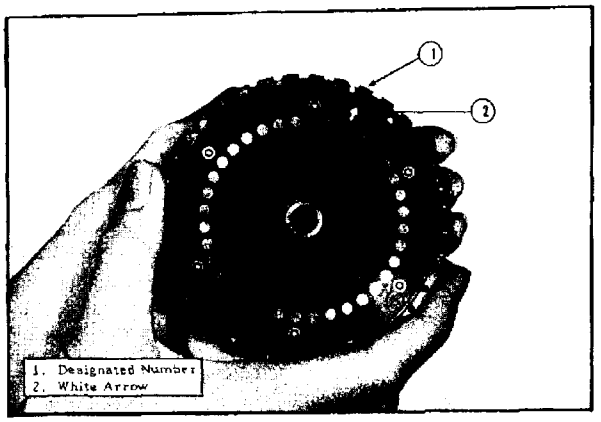


Figure 3(1)

Setting alphabet ring to bench mark arrow on rotor core:

(1) Depress the alphabet ring and rotate the ring until the designated number (24) is beside the white arrow on the rotor core.
(2) Release the alphabet ring and check to insure that it is firmly locked in position and that it will not rotate relative to the core.

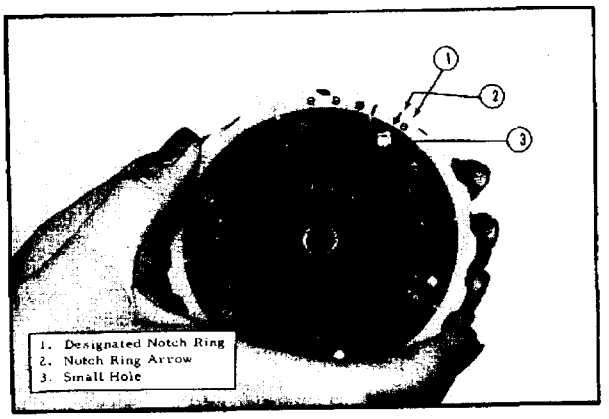


Figure 3(2)

Placement of notch ring on rotor core:

(1) Select the designated notch ring (8) and place it on the rotor core with the black arrow of the notch ring opposite the small hole near the edge of the rotor core.
(2) Depress the notch ring and rotate the ring to lock it in position on the rotor core.

Figures 3(1), 3(2).—Assembly of ADONIS Rotors in Accordance with a Key List.

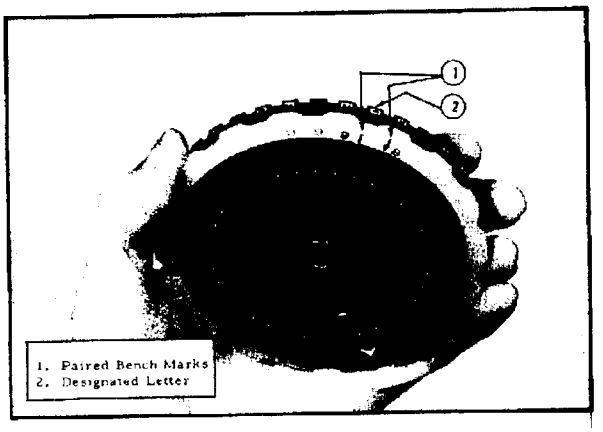


Figure 3(3)

Setting notch ring to designated letter of alphabet ring:

(1) Depress the notch ring and rotate it relative to the core until the paired bench marks (line and arrow) bracket the designated letter of the alphabet ring (D).
(2) Release the notch ring. Check to insure that both the alphabet ring and notch ring are firmly locked in position, and that neither will rotate relative to the core.

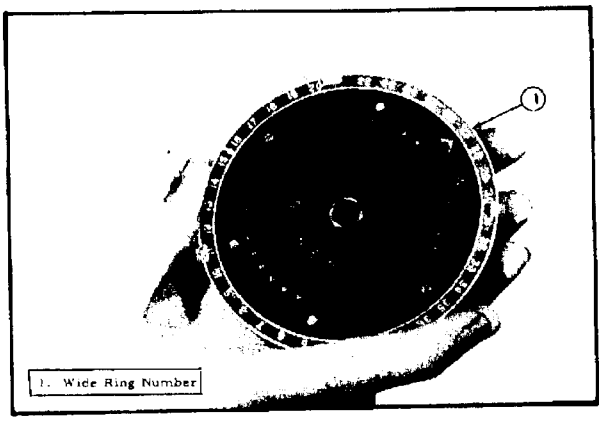


Figure 3(4)

Placement of stationary ring (wide ring) on rotor core:

(1) Select the core listed in the fourth column of the key list (G) and hold it with the spring contacts up.
(2) Place the stationary ring on the core so the arrow on the ring points to the small hole near the edge of the rotor core.
(3) Depress the ring and rotate it until the small hole is opposite the WIDE RING number (27) designated in the key list. Release the ring and check to insure that it is firmly locked in position.

Figures 3(3), 3(4).—Assembly of ADONIS Rotors in Accordance with a Key List.

(5) Tear off the tape and compare the last two encrypted groups with the 36-45 letter check group appearing in the effective key list. The letter check tape must be destroyed immediately after comparison. If the groups are not identical, the above procedures should be repeated, and all steps carefully checked.

b. If the 36-45 letter check cannot be made successfully and rechecks have indicated that the correct rotors, rotor assemblies, rotor arrangements, etc., have been used, dirty rotor or cipher unit contacts, faulty mechanical operation, or an error in the printing of the letter check in the key list may be the cause.

(1) If more than one machine, cipher unit, and set of rotors is available, attempt to produce the letter check using the different equipment. If the same letter check is found consistently with both sets of equipment, it should be assumed that the letter check is incorrectly printed in the key list and normal operation may continue.

(2) If spare equipment is not available, the equipment shall be set up according to the previous day's arrangement. If the letter check for the previous day is made successfully, it may be assumed that the equipment is functioning properly and normal operation may continue. If the letter check for the previous day cannot be made successfully, the equipment shall not be used until maintenance has been performed.

2103. System Indicators.—System indicators are encrypted when prescribed by appropriate Service, Department, or Agency instructions. KAG-18-1 and KAL-11 are used in conjunction for the encryption of system indicators.

2104. Message Indicator.

a. The message indicator consists of five random letters and is used to determine the message rotor alignment as explained in paragraph 2105. THE MESSAGE INDICATOR SHALL BE DIFFERENT FOR EACH MESSAGE OR MESSAGE PART. When it is necessary, as in the case of a service, to re-encrypt a message, or part, or any portion thereof, a different message indicator shall be used. Bonafide five-letter words, abbreviations, etc., will not be used as message indicators.

b. Previously prepared message indicators shall always be used. These shall either be selected from a prefabricated indicator tape or shall be generated on the machine in the following manner.

(1) Place a random assembly and arrangement of rotors in the machine (not an arrangement prescribed in the key list).

(2) Randomly align the rotors, move the selector handle to "E" and by typing letters and words at random, produce a tape of five-letter groups.

c. The random groups should be used, one at a time, as message indicators. As each is used it should be torn off the roll and pasted on the message form, message log, etc., to prevent possible re-use.

CAUTION:

DO NOT DEVIATE FROM THESE PROCEDURES IN SELECTING RANDOM INDICATORS. DO NOT STEP THE ROTORS TO A RANDOM ALIGNMENT AND COPY THE RESULT AS THE MESSAGE INDICATOR.

2105. Message Rotor Alignment.—The alignment of the rotors at the beginning of encryption and decryption is the message rotor alignment. It is derived from the message indicator in the following manner:

a. With the selector handle at "P", align the seven visible rotors to AAAAAAA by depressing, in order, each of the rotor-set keys.

b. Select a random five-letter message indicator as described in paragraph 2104 and paste it on the message form, message log, etc.

c. Turn the selector handle to "E" (note that the rotor maze steps once).

d. With the selector handle at "E", encrypt the five letters of the message indicator. The resulting five encrypted letters printed on the tape forms the five letters of the message rotor alignment.

e. Tear off the tape.

f. Return the selector handle to "P", align the first five rotors to the encrypted

five letters printed on the tape by depressing, in order, the rotor-set keys. Use the alignment of the first and second rotors as the alignment of the sixth and seventh rotors, respectively. This completes the message rotor alignment.

For Example:

Message Indicator (Random) . . . . . DWBRP

Result Printed on Tape (Encrypted Indicator) . . . . . HAFTB

Completed Message Rotor Alignment . . . . . HAFTBHA

CAUTION:

DO NOT TRANSMIT THE COMPLETED MESSAGE ROTOR ALIGNMENT OR ANY PORTION THEREOF AS THE MESSAGE INDICATOR.

g. Destroy the tape on which the encrypted message indicator is printed.

CHAPTER 3

3000—OPERATION

3001. Message Preparation.—Messages to be encrypted with the KL-7 will be prepared in accordance with effective edition of ACP 121 or applicable Department or Agency instructions.

3002. Division into Cryptoparts.—Message length in ADONIS cryptosystems is limited to 900 groups, exclusive of indicators. When the plain text of a message will yield more than 900 groups of cipher text, the following instructions apply.

a. Divide the message between words so that no part will exceed the ~~900~~ 1200 group limitation.

b. Encrypt each part using a NEW MESSAGE INDICATOR.

c. Number each cryptopart in plain language, e.g.,

PART ONE OF THREE PSLAV INDIA TANGO PAPA ALFA TANGO

PART TWO OF THREE PSLAV DELTA ROMEO OSCAR QUEBEC XRAY

FINAL PART OF THREE PSLAV YANKEE TANGO ECHO GOLF KILO

3003. Re-encryptions.—Whenever a message OR ANY OF THE PLAIN TEXT THEREOF was once encrypted and transmitted and is again encrypted by the originator or any addressees, the following rules apply:

a. A different message indicator shall be selected for the re-encryption.

b. A different DTG and a different filing time shall be used with the re-encrypted version. If the original DTG is used for reference purposes, it must be buried in the text of the re-encrypted message.

c. There will be no external linkage between the original message and the re-encryption.

3004. Cryptoperiod.

a. ADONIS cryptosystems have variable elements, called keying elements, which change on a daily basis; for example, rotor arrangement and rotor assembly. Key changes shall be made at 0001Z (GMT).

b. Messages shall be encrypted using the key for the GMT date indicated by the external date-time group; for example, a message with an external DTG of 240200Z, to be encrypted at 232200R (local time) shall be encrypted using the daily keying elements for the 24th day.

c. When it is determined at the end of a cryptoperiod that a backlog of messages will require more than one hour encryption time and DTGs have already been assigned, a new external DTG should be assigned to each message by the cryptocenter and the original DTG should be buried in the text for encryption.

3005. Sequence of Operations in Encryption. **(see CHECKLIST on page 24)**

a. Prepare the KL-7 rotors for operation in accordance with paragraph 2101 and insure the letter check (par. 2102) agrees with the letter check listed in last column of key list.

b. Align rotors and encrypt message indicator as indicated in paragraph 2105.

c. With the selector handle at "P", type the message heading, space several times, and type the system indicator which identifies the keying data used for encryption, then type the phoneticized message indicator.

d. With the rotors aligned to the message rotor alignment (encrypted message indicator), turn the selector handle to "E" (note the rotor maze steps once).

e. Set the stroke counter to zero.

f. Type the message text to be encrypted.

(1) The KL-7 will cause an encrypted "J" to decrypt as a "Y" and an encrypted "Z" to decrypt as an "X". Phoneticize the letters J, Y, X and Z when encrypting such text as callsigns, proper names, etc.,

which might otherwise be inaccurate when decrypted.

(2) Space normally between words. The cipher text will be printed on the tape in five-letter groups.

(3) The letter "X" may be used in lieu of punctuation in the message text. Punctuation marks, where required for clarity, must be spelled out or abbreviated. Numbers should normally be spelled out in order to prevent garbles in the message text. In certain circumstances where message texts are composed primarily of digits (e.g., weather traffic, logistic traffic, etc.) the encryption of digits may be authorized by higher authority.

(4) If a typing error occurs during encryption of literal traffic which will affect the sense of the message, type the word "ERASE" preceded and followed by a space, repeat the last correct word, NOT A NUMBER, and continue the message from that point. If an error is made during encryption of digital traffic, return to lower case by striking the LET key, type the word ERASE, preceded and followed by a space. Strike the FIG key to return to upper case, repeat the last digital group known or assumed to be correct, and continue the message from that point.

g. If the last group of cipher text does not contain five letters, strike the space bar once and encrypt as many random letters as necessary to complete the group. If the machine is in upper case, first strike the LET key, strike the space bar once, and then encrypt as many random letters as necessary to complete the final group.

h. After the text has been encrypted, move the selector handle to "P" and type the system indicator.

i. Advance the tape until the printing is clear of the tape channel and tear off the tape.

j. The following illustrates the arrangement of system and message indicators which shall be used.

37135 NOVEMBER SIERRA JULIETT
1 2
ALFA PAPA BVPLQ FKROC DLQQO
3
NXMSD ZLDXI 37135
3 1

1. System indicator (repeated at end of text; may also be literal).

2. Message indicator (each letter phoneticized).

3. Encrypted text.

k. Randomly disarrange the rotor alignment reached at the end of encryption.

l. Except under the conditions stated in paragraph 3004*m*, every message shall be completely check decrypted to verify that the operating instructions have been carefully followed and that the encrypted text is decipherable. If two or more operators are available, the check decryption should be performed by an operator other than the one who performed the original encryption. If possible, a different set of cryptomaterials should be used. THE CHECK DECRYPTION SHALL BE MADE BEFORE TRANSMISSION OF THE ENCRYPTED MESSAGE EXCEPT IN CASES OF EMERGENCY. In cases of emergency, the message may be transmitted and then check decrypted. If an error is discovered after an encrypted message has been transmitted, appropriate corrective actions should be taken by means of an explanatory cryptoservice as explained in the effective edition of KAG-1.

m. When a complete check decryption cannot be made because of the urgency of the message or other cogent reason, a partial check decryption of each message or cryptopart will be made as follows:

(1) Examine the message as though it were an incoming message.

(2) Follow the normal sequence of operations for decryption as contained in paragraph 3005.

(3) Decrypt the first ten groups.

(4) Press the RPT and L keys simultaneously and permit the machine to run until the stroke counter reaches 50 characters LESS than the number of characters in the cipher text.

(5) Decrypt the last ten groups.

(6) If all items check properly and the first and last ten groups decrypt correctly, it can be assumed that the message has been correctly encrypted.

n. Randomly disarrange the alignment reached by the rotors on completion of the check decryption.

3006. Sequence of Operations in Decryption.

a. Prepare the KL-7 rotors for operation in accordance with paragraph 2102 and insure letter check agrees with key list.

b. With the selector handle at "P", align the seven rotors to AAAAAAA by depressing the rotor-set buttons.

c. Move the selector handle to "E" and encrypt the message indicator *RECEIVED.*

d. Return the selector handle to "P" and align the five letters printed on the tape on the first five rotors from left to right.

e. Complete the rotor alignment by repeating the alignments of rotors 1 and 2 on rotors 6 and 7 respectively.

f. Destroy the tape containing the first five letters of the rotor alignment.

g. Turn the selector handle to "D" (Decrypt). (Note the rotors step once as the selector passes from "P" to "E".)

h. Set the stroke counter to zero.

i. Type the encrypted text of the message, exclusive of indicators. Disregard the spaces between groups. The plain text will be printed on the tape in normal word lengths. The X will be printed in lieu of Z, and the Y in lieu of J, e.g., XERO for ZERO, and YUMP for JUMP.

j. After completing decryption, advance the tape until the printing is clear of the tape channel, and tear off the tape.

k. Randomly disarrange the rotor alignment reached at the end of decryption.

l. Prior to delivery of the messages to addressees, the message must be edited in accordance with the effective edition of KAG-1.

3007. Degarbling.

a. If no plain text appears:

(1) Compare the group count against the actual number of groups in the message. If different, add random groups to make up the difference or subtract the difference and attempt to decrypt again.

(2) The Message Rotor Alignment may be incorrect. Attempt to decrypt using the 36-45 letter check alignment, then using AAAAAAA and finally the alignment reached by the rotors *AFTER* derivation of the correct rotor alignment.

(3) The DTG may be in error. Try to decrypt using the key for the day before and the day following the DTG. Try the key list for the previous month and the following month.

b. If some plain text appears: Write down the rotor alignment at the "point of garble". The "point of garble" is the fourth character of the last group known to be correct. The fifth character of this group must not be used since the stepping of the rotors as the selector handle passes from "P" to "E" or "D", will make up for that missing fifth character. Compare group count against actual number of groups. If not the same, add or delete characters or groups at the "point of garble" to make up the difference.

c. If the message cannot be decrypted, a cryptoservice request for re-encryption must be sent and the undecipherable message brought to the attention of the officer-in-charge. He will determine how much time, if any, should be spent in attempting to degarble it and if any special action should be taken.

CHECK-DECRYPTION LIST

DATE_____

Msg. No.	1	2	3	4	5	6	7	8	9	10	11	12
a. Correct Cryptosystem used.												
b. Correct key list and system indicator for system, month and day.												
c. Letter check made. (Tape destroyed.)												
d. Message indicator selected at random and not previously used in this crypto-period.												
e. Message rotor alignment derived correctly.												
f. Message or part does not exceed ~~900~~ 1200 groups.												
g. Complete check decryption performed by different operator if possible, (1) using only the copy of the message as prepared and ready for transmission;												
(2) using different crypto-equipment, if possible;												
(3) none of the groups obtained in making the letter check used as message rotor alignment or message indicator (tape destroyed).												
OPERATOR'S INITIALS												
CHECK OPERATOR'S INITIALS												

Note: Extracts of this page need not be marked CRYPTO.

CHAPTER 4

4000—SURVEILLANCE

4001. General.—The specific physical and cryptographic insecurities applicable to the ADONIS cryptosystems are described below. Whenever an insecurity is detected, the cryptosecurity officer or officer in charge should be notified. He will prepare the necessary report and submit it in accordance with the effective edition of KAG-1 by the means shown.

a. Physical Insecurities.—Any physical insecurities pertaining to the KL-7, rotors, classified components, printed key lists, or extracts of printed key lists, maintenance manuals, operating instructions, or pages thereof, will be reported by message in accordance with the effective edition of KAG-1.

b. Locally Extracted Keying Material. All known or suspected physical compromises of master key lists or locally extracted keying material from master key lists will be reported to the commander issuing the keying material. He will take the necessary action to evaluate the compromise and notify holders in event supersession is warranted.

c. Cryptographic Insecurities.—Cryptographic insecurities shall be reported by letter (except (3) below which must be reported by message), together with a copy of the cipher text of the message involved, directly to the Assistant Director, National Security Agency, 3801 Nebraska Avenue, N. W., Washington, D. C. 20305, ATTN: S13.

(1) Any reuse of a message indicator on the same daily key list setting. Specify if the reused indicator was for a re-encryption of the same message or for encryption of two or more different messages or cryptoparts. Notify the originator by message that the messages involved must be paraphrased in accordance with the appropriate paragraph of KAG-1.

(2) Encryption of a message or any part of the plain text thereof in which a rotor is discovered to have missed two or more scheduled steps, or to step two or more times when not scheduled. If there are more than two improper steps of a rotor, *the originator shall withdraw the faulty machine from use until it has been repaired.*

(3) Faulty encryption resulting in monoalphabetic substitution. This fault is the result of encryption in which none of the rotors step. The easiest way to recognize this is by noting that a particular letter in cipher text, the monoalphabetic version of the encrypted spaces in the message, will recur at word-length intervals. Describe in detail the cause of the monoalphabetic substitution. Action to be taken is:

(a) If the originator notes this fault, he shall send a cryptoservice message to all addressees which states that the original message will not decipher due to faulty encryption which resulted in monoalphabetic substitution and that the original message must be considered compromised and will not be serviced. The originator must also provide addressees with a re-encryption of the original message, if the information is still required.

(b) If an addressee notes the fault, he shall notify the originator and all addressees by encrypted message. The originator must then take the action outlined in (a) above.

(4) Transmission of a message having more than ~~250~~ 1300 groups to a cryptopart. State the number of groups sent.

(5) Transmission in the clear of any alignment reached by the rotors during or at the end of a previous transmission.

(6) Transmission in the clear of any portion of the 36-45 letter check sequence.

(7) Message indicator obviously not selected at random (bonafide words, abbreviations, use of any five letters which appear on the rotors at the end of a previous message or cryptopart).

(8) Transmission in the clear of the message rotor alignment or any five consecutive letters thereof (for example, use

of the first five letters of the rotor alignment as the message indicator).

(9) Encryption of a message using AAAAAAA as the message rotor alignment.

(10) Use of the alignment reached by the rotors after encryption of the message indicator as the message rotor alignment, i.e., failure to align the message rotor alignment after its derivation.

CHAPTER 5

5000—CLEANING

5001. General Instructions.—Care must be taken not to disturb springs or adjustments when performing first echelon maintenance. Dirt and dust are to be removed from the exposed surfaces of the machine with the sash-brush-type cleaning brush. Troubles frequently develop later as a result of careless cleaning. Cleaning should be carried out as prescribed in these instructions and should be confined to the following items:

a. Contacts on bottom and side of KLK-7 endplates.

b. Contacts on stepping unit where KLK-7 rests.

c. Rotors.

Note: Definite cleaning schedules should not be prescribed since such factors as dust, humidity, temperature, and the volume of traffic must be the determining factors.

5002. Flat Head Contacts.—If the flat head contacts on the bottom of the KLK-7 endplates, inside the removable KLK-7 endplate, or the rotors themselves appear black or badly corroded, thoroughly clean them with the eraser provided in the accessories kit. Put a medium coating of cleaner-lubricant on the surface of those contacts which are subject to friction and spread the lubricant with twilljean cloth. Under normal operating conditions, the eraser should not be used more than once every 30 days to clean the rotor contacts. Also clean and put a medium coating of cleaner-lubricant on all rotor brushings (hole in center of rotor) and the shaft of the KLK-7 on which they are inserted.

5003. Pressure Contacts.—Clean the pressure contacts by polishing them with the canvas cleaning block assembly. DO NOT PUT LUBRICANT ON THE PRESSURE CONTACTS. All flat head and pressure contacts on endplate *inside* KLK-7, on stepping unit beneath KLK-7, and on the rotors themselves, should be thoroughly cleaned with a clean lint-free cloth or canvas cleaning block whenever a component assembly is replaced.

~~CONFIDENTIAL—CRYPTO~~

KAO-41C/TSEC

~~CONFIDENTIAL~~

ORIGINAL
(Reverse Blank)