Copy No. 0102

AROFLEX

OPERATING INSTRUCTIONS

AMSO-762(A)

Copy No. 0102

AROFLEX

OPERATING INSTRUCTIONS

AMSO-762(A)

HOLDERS OF THIS DOCUMENT ARE WARNED THAT THIS DOCUMENT CONTAINS INFORMATION AFFECTING THE MUTUAL DEFENSE OF THEIR NATION AND THEIR ALLIES. THE TRANSMISSION OF THIS DOCUMENT OR THE REVELATION OF ITS CONTENTS IN ANY MANNER TO AN UNAUTHORIZED PERSON IS PROHIBITED.

September 1987

TREATMENT OF PERSONS WHO APPEAR DEAD IN ACCIDENTS INVOLVING ELECTRICITY

ESTABLISHING APPARENT DEATH

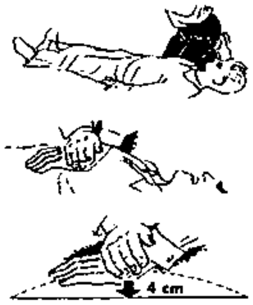
1. **NO BREATHING** (chest does not move, no exhaled air detectable)
2. **NO HEART BEAT** (determined by feeling the pulse)
3. **UNCONSCIOUS** (victim does not react to stimuli of noise or pain)

THEN

1. *Raise the alarm for help*
2. *Begin immediately with:*

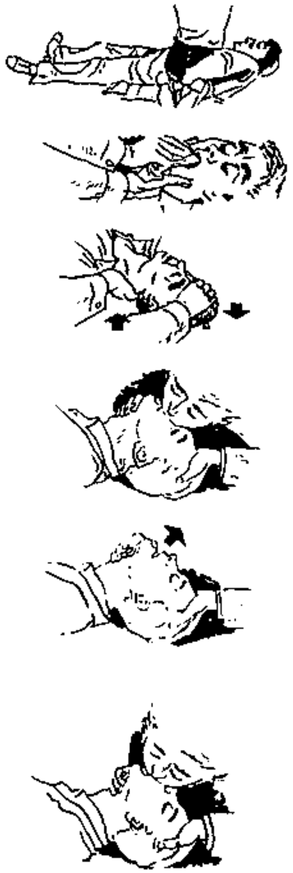
2.1. HEART MASSAGE, 2.2. ARTIFICIAL RESPIRATION

2.1. Heart massage



1. Lay the victim flat on his back on a hard foundation
2. Kneel down beside the victim's trunk
3. Place the palm of one hand on the lower third of the breast bone and press the other hand on top of this hand
4. Using short vigorous actions, press the breast bone down about 4 cm. This causes the heart to empty much like a sponge
5. Perform this pressing action about 60 times a minute.

2.2. Artificial respiration



1. Lay the victim flat on his back
2. Kneel beside the victim's head
3. Clean the mouth and throat if necessary with a handkerchief or something similar
4. With one hand lift the neck slightly, with the other hand on the forehand exert sufficient pressure so that the head is bent far back
5. Close the victim's mouth, inhale more deeply than normal and place the wide open mouth round the victim's nose and blow as much air as possible into the victim's lungs until this is clearly visible at his chest. Keep the head constantly in the sharply bent position
6. Remove the mouth from the victim's nose to allow the air to be breathed out
7. Repeat the procedure in 2.2.5.
8. The rate of resuscitation should be about 15 times a minute
9. If mouth-to-nose resuscitation is not successful (for instance if the nose is blocked) mouth-to-mouth resuscitation must be performed.
   For this, place the open mouth over the victim's open mouth

NOTE

HEART MASSAGE AND ARTIFICIAL RESPIRATION should be preferable carried out by two persons. After every 5 compressions of the chest, blow in air once. If there is only one helper, heart massage 15 times, then artificial respiration 3 times, then heart massage 15 more times, and so on.

Continue with this treatment until the doctor (who has of course been notified immediately) gives other instructions. Any interruption of the heart massage and/or artificial respiration is incorrect and very dangerous to the victim.

FOREWORD

1. AMSO-762 Operating Instructions AROFLEX is a NATO CONFIDENTIAL registered publication and is issued on behalf of the Military Committee. It shall be transported, stored, safeguarded and accounted for in accordance with agreed security regulations for the handling of NATO CONFIDENTIAL registered publications.
   Comments regarding any portion of this publication are invited and should be submitted to the National Distribution Authority who will, if appropriate, make recommendations to the Military Committee Communications Security And Evaluation Agency (SECAN), Washington DC, USA.

2. This publication will become effective upon receipt.

3. This document consists of 65 pages as indicated on the "List of Effective Pages" no. LEP-1. Upon receipt, verify the presence of each page and annotate the "Record of Page Checks" (page X) included herein.

4. Amendments to this publication will be promulgated by means of a printed or electrically transmitted amendment and are to be entered upon receipt. Individuals entering such amendments shall so indicate on the "Record of Amendments" (page IX) included herein.

5. Holders of this document are warned that this document contains information affecting the mutual defense of their nation and of their allies. The transmission of this document or the revelation of its contents in any manner to an unauthorized person is prohibited.

6. It is forbidden to make extracts from or to copy from this publication any material unless the extract is intended for staff guidance on a need-to-know basis or for exclusive cryptocenter use.

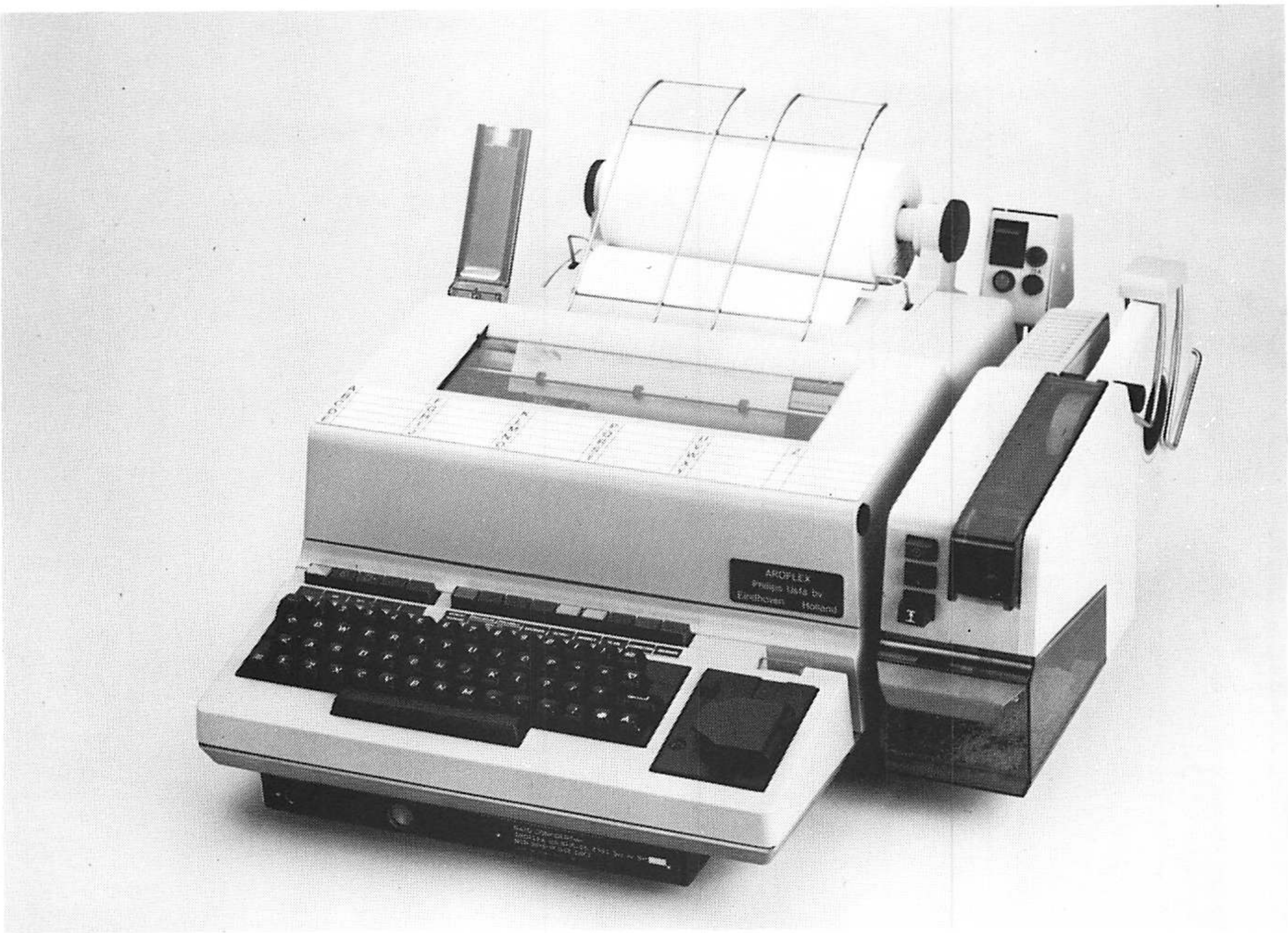


Figure I: Ceroff, Aroflex UA 8116/06

RECORD OF AMENDMENTS

Identification of Change, Reg. No. (if any), and Date	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)

CONTENTS

Page No.

CHAPTER 6 - OPERATION

SECTION 1 - Input/output devices

SECTION 2 - Plain text mode

SECTION 3 - Keysetting

SECTION 4 - Enciphering

SECTION 5 - Deciphering

SECTION 6 - Corrections

Page No.

CHAPTER 7 - OPERATOR MAINTENANCE

LIST OF FIGURES

LIST OF TABLES

ANNEX A - EXAMPLES FOR MESSAGE CORRECTIONS ON CEROFF AROFLEX

ANNEX B - 32 TO 26 CONVERSION OF CCITT CODE

LIST OF EFFECTIVE PAGES

EFFECTIVE PAGES	*PAGE NUMBERS*			
Original	I			(Reverse blank)
Original	III			(Reverse blank)
Original	V			(Reverse blank)
Original	VII			(Reverse blank)
Original	IX	to	XIII	(Reverse blank)
Amend one	LEP-I			(Reverse blank)
Original	1-1	to	1-2	
Original	2-1	to	2-5	(Reverse blank)
Original	3-1	to	3-4	
Original	4-1	to	4-3	(Reverse blank)
Original	5-1	to	5-2	
Original	6-1	to	6-5	
Amend one	6-6			
Original	6-7	to	6-15	(Reverse blank)
Original	7-1	to	7-11	(Reverse blank)
Original	7-13			(Reverse blank)
Original	7-15			(Reverse blank)
Original	A			(Reverse blank)
Original	A-1	to	A-8	
Original	B			(Reverse blank)
Original	B-1			(Reverse blank)

CHAPTER 1

GENERAL INFORMATION

101. Introduction

This publication contains the operating instructions for the AROFLEX off-line equipment UA 8116/06 (figure 1) with the CEROFF algorithm installed. The operator must be thoroughly familiar with the contents of this manual before operating this equipment. It does not discuss installation or maintenance (other than initial troubleshooting procedures) of the equipment.
Operators requiring such information should refer to the appropriate AMSMs listed in the next paragraph.

102. Related publications

The short and long titles of associated publications are given below. The most current edition of each should be referred to.

SHORT TITLE	LONG TITLE
AMSM-763	AROFLEX Field Level Repair Manual
AMSM-764	AROFLEX Depot Level Repair Manual
AMSM-765	AROFLEX Illustrated Parts List

103. Modification of equipment and procedures

Equipment modification and changes to procedures set forth herein must be approved by the SECAN.

104. Comments and recommendations

Users of this publication are encouraged to review it critically. Comments and recommendations concerning it should be forwarded through Department or Agency channels to the SECAN, Washington, DC.

105. Authorization for use

The AROFLEX is approved for the encryption of all categories and classifications of traffic.

106. Qualifications for operator/maintenance personnel

a. Qualifications for operator personnel.

Personnel who have a security clearance at least as high as the classification of the AROFLEX equipment may be qualified by on-the-job training to operate and troubleshoot the AROFLEX in accordance with the instructions outlined in this publication. The operators may also be qualified by on-the-job training to exchange an AROFLEX equipment in the system.

b. Qualifications for AROFLEX Depot Maintenance Personnel.

Personnel who have completed formal training on the depot maintenance of the AROFLEX may perform those procedures specified in the effective edition of AMSM-764. These personnel must possess a certificate of clearance for access to CONFIDENTIAL information.

c. Qualifications for AROFLEX Field Maintenance Personnel.

Personnel who have completed formal training on the field maintenance of the AROFLEX may perform those procedures specified in the effective edition of AMSM-763. These personnel are not authorized to perform higher levels of maintenance, and must possess a certificate of clearance for access to CONFIDENTIAL information.

CHAPTER 2

SECURITY

201. Classification

The classification of the principal components of the AROFLEX cryptosystem is shown below:

Item	Classification	Marking
Unkeyed AROFLEX.	CONFIDENTIAL	
Keyed AROFLEX.	The classification of keyed equipment is at least equal to the classification of the key used but never less than the classification of the equipment when unkeyed (CONFIDENTIAL).	CRYPTO
UA 8485/00 Potted Key Generator.	CONFIDENTIAL	
UA 8482/08 Printed Wiring Board.	CONFIDENTIAL	
Operational and exercise key tapes. (daily cryptovariables)	Same as the highest classification of traffic the key is intended to protect, minimum is CONFIDENTIAL.	CRYPTO
System Indicator (SI) key tapes: AMST-9504.	NATO CONFIDENTIAL	CRYPTO
Maintenance and training key tapes.	NATO RESTRICTED	

202. Physical security considerations

a. Protection of keying material

Individual users are responsible for safeguarding key tapes in their possession, for adhering to prescribed rules for handling, use, and disposition, and for reporting any circumstances, occurences, or acts which could jeopardize the security of such material. The following control procedures apply:

(1) Access may be granted to NATO Alliance citizens whose duties require such access and who possess security clearances equal to or higher than that of the keying material. Contractor personnel who operate the AROFLEX equipment or who have access to operational keying material or traffic must have clearances to the level of the keying material.

(2) Unless in use by, in the physical possession of, or continuously attended by an appropriately cleared person, keying material must be stored in accordance with AMSG-505.

(3) Keying material issued from crypto accounts to users must be transmitted on hand receipts or other formal records. Keying material so issued must be accounted for locally until it is destroyed or returned to the custodian. It must be inventoried by users to assure continuing protection and control. In secure communications centers, daily inventory is required and shall be made a matter of formal record. Keying material stored in security containers which have not been opened since the previous inventory need not be specifically sighted.

(4) At user locations, used key tapes containing daily cryptovariables should be destroyed immediately, if practicable, but in any case within 72 hours; used key tapes containing System Indicator cryptovariables should be destroyed promptly at the end of the cryptoperiod. Unused superseded copies which have been stored in secure areas must be destroyed within five days after supersession. Authorized methods for destroying AROFLEX keying material include complete burning, pulverizing or chopping, and pulping. Destruction must be performed by a suitably cleared individual.

b. Cryptoperiods

The cryptoperiods associated with AROFLEX cryptovariables are as indicated:

(1) **Daily cryptovariable.** Daily cryptovariables are used to encrypt/decrypt messages. The maximum cryptoperiod for daily cryptovariables is 24 hours.

(2) **System indicator (SI) cryptovariable.** SI cryptovariables are used to encrypt/decrypt System Indicators. The cryptoperiod for SI cryptovariables is monthly.

(3) **Maintenance and training cryptovariables.** Maintenance and training cryptovariables are used when there is no intent to transmit or transport AROFLEX encrypted messages (i.e., maintenance cryptovariables are used for in-shop testing and repair of AROFLEX equipment, training cryptovariables are used for classroom-related operations). Maintenance and training cryptovariables have no fixed cryptoperiods, and key tapes which contain them may be used until they become unserviceable.

c. Protection of equipments

The controls specified below apply to the AROFLEX equipment.

(1) Access to keyed equipment may be granted to NATO Alliance citizens whose official duties require such access and who are cleared for access to the keying material employed. Contractor personnel who install or maintain AROFLEX equipment must have at least a CONFIDENTIAL clearance.

(2) No restrictions are imposed upon external viewing of the AROFLEX equipment or on other exposure where no opportunity for use, tampering, viewing of the cryptovariables, or extended internal examination exists. However, the open or public display of the AROFLEX or its classified components at non-NATO symposia, meetings, open houses, tours, or for other non-official purposes is forbidden. Additionally, photographs, drawings, or descriptive information for press release or private use is prohibited.

(3) Unattended, unkeyed AROFLEX equipment must be protected in the manner prescribed for other NATO CONFIDENTIAL material to preclude theft, sabotage, tampering or access by unauthorized persons. When keyed, such equipment must be protected to the degree necessary to prevent their unauthorized use or the unauthorized extraction of their cryptovariables.

(4) Users may be issued AROFLEX equipment on hand receipt, log or other record.

d. Equipment testing

A routine check on the proper operation of AROFLEX is to be carried out at every crypto change period, see par. 702.

e. Emergency procedures

The safeguarding of the AROFLEX equipment and related COMSEC materials under emergency conditions is a responsibility of the holder and should be provided for in the holder's Emergency Action Plans. AMSG-293 should be used in the preparation of Emergency Action Plans.

(1) Reasonable effort should be made to recover the AROFLEX equipment and supporting classified material lost through catastrophe or hostile action. However, human life or personal injury should not be risked in such recovery efforts.

(2) In case of emergency, procedures must be established to provide for both emergency evacuation and/or access by uncleared emergency personnel.

(3) In case of impending seizure or abandonment of an area containing the AROFLEX equipment, procedures must be established to provide for an orderly destruction schedule. By priority, this schedule must include zeroization of keyed equipment (see par. 406), destruction of classified key tape segments and COMSEC maintenance manuals, and the removal and destruction or unrecoverable disposal of classified AROFLEX components and other classified COMSEC materials. Classified AROFLEX components are the boards UA 8485/00 and UA 8482/08 from the crypto module. Emergency destruction can be accomplished by smashing these boards with a hammer, ensuring that they are destroyed to such a degree that they cannot be reconstructed.

203. Reportable insecurities

This section provides specific guidance for identifying those physical, personnel, or crypto-related incidents that are reportable as insecurities in connection with the AROFLEX. The procedures for COMSEC insecurity reporting are prescribed in AMSG-293.

a. Physical insecurities

(1) The physical loss of **any** COMSEC material, or portion thereof (for example, a classified page from a COMSEC maintenance manual).

(2) COMSEC material discovered outside of required physical control or COMSEC accounting channels.

(a) Discovery of COMSEC material which was listed on a destruction report but was not actually destroyed.

(b) Discovery of COMSEC material left unsecured and unattended where unauthorized persons could have access to it.

(3) Unauthorized extraction or loading of cryptovariables.

(4) Failure to remove key from the AROFLEX prior to shipment between crypto accounts or placing into storage.

(5) COMSEC material improperly packaged, shipped, or destroyed. For example:

(a) Receipt of keying material in a package which shows evidence of tampering.

(b) Destruction of COMSEC material by other than authorized means.

(c) COMSEC material not completely destroyed and left unattended when unauthorized persons could have access to it.

(6) Unauthorized access to COMSEC material.

(7) Unauthorized copying, reproducing, or photographing of COMSEC material.

(8) Discovery of a clandestine intercept or recording device in close proximity to AROFLEX equipment.

(9) Any other incident which jeopardized the physical security of COMSEC material.

b. Cryptographic insecurities

(1) Use of crypto keying material which is compromised, superseded, defective, previously used and not authorized for reuse, or in any way incorrect for the cryptoperiod or application in which it is used. For example:

(a) Use of maintenance, test, training, or exercise key for other than its intended purpose.

(b) Use of key which was produced locally without authorization.

(c) Use of any keying material that is not marked "CRYPTO" to protect NATO classified information.

(d) Unauthorized extension of a cryptoperiod.

(2) Discussion, via unprotected telecommunications, of the details of a crypto equipment failure or malfunction.

(3) Failure to test an AROFLEX, as prescribed in par. 202 .d., above.

(4) Transmission of cipher text processed using a defective AROFLEX.

(5) Attempted maintenance of a crypto equipment by unqualified personnel.

(6) Modification of the AROFLEX without the approval of the SECAN.

(7) Suspected tampering with the AROFLEX.

(8) Compromising emanations from a COMSEC equipment.

c. Personnel insecurities

These include actions and circumstances involving persons with access to crypto material, which have jeopardized, or could jeopardize, the security of crypto material. Examples of such actions and circumstances are:

(1) Known or suspected defection, espionage, hostile cognizant agent activity, treason, sabotage, or capture by an enemy.

(2) Theft of COMSEC material.

(3) Falsification of COMSEC records.

(4) Unauthorized disclosure of information concerning COMSEC material or attempts by unauthorized persons to effect such disclosure.

CHAPTER 3

INTRODUCTION AND SUMMARY DESCRIPTION

301. Purpose

AROFLEX - type UA 8116 - is a compact, self-contained and highly automated combination of a Siemens "T 1000Z" teleprinter and a micro-processor-oriented crypto module by Philips Usfa. It is capable of rapid encryption and decryption, with crypto text formatted in 5-letter groups in the English alphabet.
It meets the requirements of MCM 46-72 and its operation complies with the ACP-127 procedures. It operates in the OFF-LINE mode.

AROFLEX is equipped with 26 separate key stores to wit: 25 "normal" key stores and 1 "indicator" key store. Two principal modes of operation are incorporated. In the DIRECT mode the input is processed immediately to produce the cryptogram or deciphered message. In the INDIRECT mode the input is printed "as entered", stored internally and output (as cryptogram or deciphered message) in a second operation. The input can therefore be monitored and, if necessary, corrected to eliminate errors.

AROFLEX is equipped with a light-weight optical tape reader and a clip-on tape punch to give it maximum applicability.

302. Employment

AROFLEX can be employed for the following purposes:

a. self-contained rapid off-line encryption and decryption

b. message preparation facility with or without instant encryption.

303. Physical data

Input	:	Keyboard, tape reader		
Output	:	Page copy, punched tape		
Operating modes	:	Crypto off-line		
	:	Message preparation facility		
	:	With or without monitoring of input		
	:	Always with automatic decryption		
Formatting arrangements	:	According to ACP-127, viz. Format Lines 1...4 without counting of Line Feeds		
	:	Format Lines 5...11 with counting of Line Feeds		
	:	Automatic paging procedure after every 20 lines		
	:	Automatic termination of messages, maximum 6 pages		
Dimensions	:	Height	:	265 mm without roll of paper, 320 mm with roll of paper
	:	Depth	:	545 mm without roll of paper, 600 mm with roll of paper
	:	Width	:	530 mm including clip-on tape punch
	:	Weight	:	25 kg including tape punch.

Operating temperature range	:	-10° C to +55° C.
Power supply	:	110 Volts AC, or 220 Volts AC -10% to +20%, 50/60 or 400 Hz.
Power consumption	:	150 VA in full operation, 40 VA in standby.
Operating speeds	:	100 Baud in the off-line mode.
Telegraph code	:	ITA Code No. 2 (CCITT Alphabet No. 5).

304. Cryptographic data

The 26 keysetting stores (compartments) of AROFLEX can be filled from the keying lists by means of the keyboard or tape reader; each keysetting results in a check word so that an immediate check on the correct keysetting (and hence the correct operation of the equipment) is provided.
Keysettings cannot be recalled after having been inserted. Hold cells are incorporated to prevent loss of keysettings because of power interruptions.
Keysettings can only be inserted after the code "KEYINSERT" and the store location character have been typed-in.

The keysettings consist of the compartment address (a...z), 5-figure indicator, 24 random characters, and the 5-letter check word. In case of emergency, the keysettings can very rapidly be destroyed by actuating the ZEROIZING push-button (see par. 406).
Each message is provided with an automatically generated random message key which prevents overlap and allows repeated use of one keysetting.

Fail-safe supervisory circuits result in immediate crypto alarm in case of single or multiple component failure in essential circuits.

305. Keying material

a. NATO keying material will be in the form of five-level standard hole tape. Standard hole tapes are standard in the following respects.
   Each tape segment consists of (in order):
   (1) tape leader (blank) - 0.3" long
   (2) print field - 2.0" long containing three lines of printed data with a maximum of 20 characters and spaces per line (see subpar. (b))
   (3) separator space (blank) - 1.8" long
   (4) punched data - 4.8" long (48 punched characters, see subpar. (c))
   (5) trailer (blank) - 0.7" long.

b. The print field normally contains short title, edition suffix, segment number, copy number (if needed), classification and digraph code letters.
   (1) An example of the print field for an AROFLEX tape segment (system indicator key or traffic key) with no repeats is:

	NATO	SECRET	CRYPTO	
	AMST	ED	REG	SEG
xx	xxxx	xx	xxx	xx

(2) An example of the print field for an AROFLEX tape segment (system indicator key or traffic key) with repeats is:

```
      NATO  SECRET  CRYPTO
      AMST    ED       REG   SEG/CY
xx    xxxx    xx       xxx    xx xx
```

The two letters printed to the left of the short title are used to identify the number of unique variables, copies per unique variable, total number of segments and variable cryptoperiod of the tape contained in the canister. There is a digraph printed on the Disposition Record card which is used in conjunction with the two letters. Reading left to right, the first letter identifies the number of unique variables, copies of variables and total segments.
The second letter identifies the variable cryptoperiod.

c. The punched data for an AROFLEX tape segment (one variable) is as follows (in order, no spaces):
(1) one FIGURES character
(2) five digits - the system indicator. The first three digits are the same as the three least significant digits of the key tape short title. The last two digits represent the day of the month and are assigned sequentially from 01 (first segment) through 31 (last segment)
(3) one LETTERS character
(4) 24 alphabetic characters - the cryptovariable, which is randomly generated using 16 letters of the alphabet (A, B, C, E, F, G, H, I, J, K, L, M, O, Q, S, T)
(5) five-letter checkgroup
(6) 12 BLANK characters (this results in no punches on the tape).

d. System Indicator Encryption Key (AMST 9504).
The above description applies specifically to keying material for traffic encryption. AROFLEX also requires variables (Z variables) for system indicator encryption. The format of the Z variable tape segment is identical to the format for tape segments containing variables for traffic encryption. Each Z variable is effective for one month. One edition contains five copies each of six unique variables, packaged in a plastic canister, and is effective for six months.

e. For keying material for traffic encryption, the print field of each segment reflects short title, edition, register number, and segment number.
For system indicator keying material, the print field of each segment reflects short title, edition, register number, segment number and copy number.

306. Operational features

Decryption is entirely automatic with automatic selection of the correct keysetting. The crypto output, viz. 5-letter groups according the ACP-127 format, is always printable and conforms with the current formatting arrangements with automatic page numbering and group counting, printed at the end of the cryptogram.
The cryptomemory is sufficient for the storing of 6 pages of crypto text or 1200 5-letter groups. Correction of input is possible without losing cryptosynchrony.
When an operator makes a mistake in operation or procedure, AROFLEX gives an automatic warning and blocks the keyboard and tape reader till the mistake has been set right.
The automatic group count, paging procedure, crypto procedure and termination of messages, combined with the possibility of correcting the clear text message preparation, make for a simple, versatile equipment.

307. Comsec officer duties

When receiving a report as meant in Table 6-IV (serial 4-remark 4) or Table 6-V (serial 5-remark 2), the comsec officer is to collect all relevant copies (paper-tapes and print-outs of encrypted and decrypted text) and is to report the incident with full details to the chief of communications for his service by a priority message classified NATO SECRET.

308. General note

Throughout this manual continuous reference is made to Figure II: Operating controls on pull-out sheet Chap. 7.

CHAPTER 4

OPERATING CONTROLS

The serial numbering of the operating controls is shown in Figure II.

	Pos	Name	Function
401.	**ON/OFF Controls**		
	1	--	No function in the OFF-LINE mode. Flashing lamp inside button indicates open cover or end of paper roll.
	2	ON button	Spring-loaded button for putting AROFLEX into the OFF-LINE mode, starting from the standby mode. Lamp is lit when AROFLEX is in the OFF-LINE mode.
	3	OFF button	Spring-loaded button for putting AROFLEX into the standby mode from the off-line mode.
	4	--	Spare button. No function in the off-line mode.
	5	--	Spare button. No function in the off-line mode.
402.	**Crypto Controls**		
	6	MEMORY WARNING	White lamp, lit when text is present in the memory.
	7	PROCEDURE button	Two-position button for starting and terminating the enciphering process. When pushed down, the red lamp is lit and AROFLEX is ready to carry out the crypto procedure as described in Paragraph 615 and 616 below. After the crypto procedure the clear text heading of Format Lines 1 ... 4 (if required) may be put in, without the counting of Line Feeds. Lit lamp denotes Procedure mode. Releasing the button terminates the enciphering. Furthermore the light is lit (together with the light in the DECIPHER button 14 during keyinsertion.
	8	PREAMBLE button	Spring-loaded button for putting AROFLEX into the PREAMBLE mode for inputting of Format Lines 5 ... 11 and 14, 15 before EOM-function if required. The Line Feeds of Format Lines 5 ... 11 are counted for the paging procedure. Lit lamp indicates PREAMBLE mode.
	9	ENCIPHER button	Spring-loaded button for putting AROFLEX into the ENCIPHERING mode, indicated by lit lamp. In the DIRECT ENCIPHERING mode, the printing/punching of the cryptogram commences immediately after the pushing of the ENCIPHER button; the enciphering is terminated by releasing the PROCEDURE button. In the INDIRECT ENCIPHER mode, the pushing of the ENCIPHER button causes the printing of 10 slants (//////////) as an indication of the beginning of the enciphering. The input is printed/punched in clear text. When the enciphering in the INDIRECT mode is terminated, another 10 slants (//////////) are printed.

Pos	Name	Function
10	OUTPUT button	Spring-loaded button for producing the output, prepared in the INDIRECT ENCIPHER or INDIRECT DECIPHER mode. During the production of the output, the lamp is lit. Pushing the lit button stops the output and allows of beginning the output again at the start. The output can be repeated as many times as required. The Procedure signal + blocked keyboard/tape reader + lighting up of the OUTPUT lamp in the ENCIPHER mode indicate the "FULL MEMORY" condition. The enciphering must be terminated in order not to exceed the maximum length of a transmission section according to ACP-127.
11	INDIRECT button	Two-position button for putting AROFLEX in the DIRECT or INDIRECT mode; lit lamp and depressed button indicate the INDIRECT mode with monitoring of the input and production of the output after pushing the OUTPUT button. The mode of operation must be selected before starting with the enciphering or deciphering. The lit lamp inside the INDIRECT button signifies: "TEXT IN MEMORY". A change from INDIRECT to DIRECT or vice versa resets the memory and extinguishes the lamp.
12	PLAIN button	Two-position button for putting AROFLEX in the PLAIN text mode: lit lamp and depressed button indicate mode. Pushing and releasing the PLAIN button clears and resets the crypto/message memory.
13	CORRECTION button	Spring-loaded push button for character-by-character correction of: - input in the INDIRECT DECIPHER mode - input in the INDIRECT ENCIPHER mode - input for paging information The lamp inside this button has 2 functions: - steady burning in the DECIPHER mode indicates incorrect format - slow blinking + procedure signal in the DECIPHER mode after the 11th group indicates the "NO KEY" condition.
14	DECIPHER button	Two-position push button for putting AROFLEX in the DECIPHER mode; lit lamp indicates mode. Light is lit as well during Key inserting.

403. Punch Controls

15	TAPE PUNCH ON/OFF	Spring-loaded push button for switching the tape punch on and off; lit lamp inside the button indicates that the punch is switched on.
16	TAPE run out	Spring-loaded button for punching "Letters" continuously, regardless of operating mode or punch activation.
17	TAPE backspacer	Spring-loaded button for backspacing the tape for correction ("lettering out"); tape is backstepped one character when the button is pressed firmly.
18	TAPE Retaining Catch	Small two-position catch under the plastic cover to be used for lifting the tape retaining pad when a new tape must be inserted; when catch is pressed home, the punch automatically punches 32 "Letters".

	Pos	Name	Function
404.		**Mains ON/OFF switch**	
	19	Mains Switch	To switch the mains supply on and off; lit indicator **26** denotes mains present.
	20	Fuse	Slow, 2.5 A fuse.
405.		**Tape Reader Controls**	
	21	TAUT TAPE contact	Tape for reader must be passed upwards over this contact so that a stuck tape will stop the reader.
	22	TAPE READER ON/OFF	Spring-loaded button for starting and stopping the tape reader; when a tape has been inserted and the cover **23** is closed, pressing the button for a very short time (less than $^{1}/_{4}$ second) will advance the tape one character. Pressing the button for a longer time (about $^{1}/_{2}$ second) will make the reader step continuously. Pushing the button whilst the reader is stepping will stop the reader.
	23	TAPE READER cover	Catch-retained cover for opening the tape reader so that a tape can be inserted, engaging the transport holes in the sprocket wheel.
406.		**Keying Controls**	
	24	ZEROIZE button	Red spring-loaded button for zeroizing the key stores and crypto memory in case of emergency. The button must also be used for switching off the hold batteries when AROFLEX is removed from the mains and the contents of the crypto memory are to be zeroized. Pushing the ZEROIZE button **24** extinguishes the drain indicator **25**.
	25	Battery Drain Indicator	Red light emitting diode, lit when the "hold" batteries are being drained to retain the contents of the key stores and crypto memory, for instance during interruptions in the power supply. The indicator lights up as soon as the mains switch is switched "off" or, the plug is pulled from the mains. The hold batteries are switched off automatically when the output voltage drops below a certain threshold. The hold batteries are constantly trickle-charged as long as the mains is connected to AROFLEX. The indicator is extinguished when the ZEROIZE button **24** is pushed.
407.		**Notes**	
	26	Power on indicator	Lit indicator denotes mains present.
	27	"Here is" button	◇ button inactive.

ORIGINAL
(Reverse blank)

CHAPTER 5

INSTALLATION

501. Unpacking

a. Lift the AROFLEX out of the wooden transport box with the aid of the two ropes, taking care that the right-hand rope does not become entangled with the tape holder of the tape-punch.

b. Remove the four M8 bolts and large washers from the underside of the padded wooden base plate.

c. Store the packing material for future use.

502. Installation

a. For stationary use inside a building:

Place AROFLEX on a non-metallic desk or table.
Set the mains "ON/OFF" switch in position OFF and put the mains plug into rim-earthed socket.

b. For mobile use in ships and vehicles, the use of special shock mounts is recommended.

(1) Place AROFLEX on rubber cushion on top of metal base plate and secure by means of four bolt-assemblies (see Figure III). Make sure that all rubber washers and spacers fit snugly into the holes provided on the base plate and the rubber cushion.

(2) Fix metal base plate (mounting support) to the operating surface by any convenient means using the holes provided for this purpose. For mobile use in ships a metallic surface is allowed.

c. The equipment must be installed in accordance with AMSG-719.

503. Mains supply

a. The equipment is set in the factory for operation off a 220 Volts, 50/60 Hz mains.

b. To operate AROFLEX off a 110 Volts mains, the entire power supply unit must be removed and a voltage adapter (drum switch) must be set to 110 Volts.

c. To operate AROFLEX off a DC supply, a DC to 220 Volts AC convertor must be used.

504. Preparation of AROFLEX

a. Release the printing assembly by withdrawing the metal latch, inserted between the rail and the notch in the printing head, see Figure IV.

b. Insert a roll of paper as per drawing under the hood, see Chapter 7, Operator Maintenance.

c. Put the mains plug into the socket and set the mains switch **19** in the ON position: a relay will be heard to be energized and AROFLEX is now in the STAND BY mode, consuming about 40 VA.
An automatically switched fan will control the cooling of the power supply unit.

d. Insert a roll of tape in the punch as per drawing on the side of the equipment, see also Chapter 7, Operator Maintenance.
Release catch **18** under the punch cover so that the tape can be slided in easily. Snap catch **18** into position after the tape has passed underneath it; a number of "Letters" will be punched automatically.

e. Blinking of the lamp **1** indicates that there is no paper for the page copy or that the hood is not closed.

f. AROFLEX is switched into the OFF-LINE mode by pushing the spring-loaded ON button **2** so that the lamp inside this button is lit.
To switch AROFLEX back into the STAND BY mode, with the contents of the memory still alive, push the OFF button **3**. All lamps will now be extinguished.

g. Carry out tests as detailed in par. 702 below.

h. AROFLEX is switched off completely only when the mains supply is withdrawn or when the mains switch **19** is at "OFF".
As soon as AROFLEX is switched off, the Battery Drain Indicator **25** lights up, denoting that the hold batteries are switched on to keep the contents of the memory alive.
The batteries can supply the memories for 15 minutes and are switched off automatically as soon as the battery voltage drops below a pre-set threshold value. To stop the drain (and to reset all memories to zero and to kill all keysettings at the same time) push the red ZEROIZE button **24** thereby extinguishing the Battery Drain Indicator **25**.

505. Packing

As unpacking, in reverse order. Do not forget to secure the printing head assembly by inserting the small metal latch at the left side of the rail in the notch between the printing head and the rail itself.
Push the red ZEROIZE button **24** to make sure that the Battery Drain Indicator **25** is switched off and that all memories are reset.
The base plate can be fixed to AROFLEX when the equipment is tilted to one side, with the punch uppermost. Do not forget to use the plywood container for storing the roll of paper and securing AROFLEX in the transport box.

CHAPTER 6

OPERATION

SECTION 1 - Input/Output devices

601. Keyboard

a. The keyboard is equipped with a special key for the Nabla sign (Message Validation Signal, figs. H), top row, extreme right key.

b. The keyboard contains an automatic Figures/lettersshift, coming into action when it is needed. The actuation of the "Letter" or "Figures" buttons is no longer required.

c. The input/output device is equipped with a keyboard memory of 10 characters, allowing several characters to be stored simultaneously.

d. The keyboard has a "New Line" key.

602. Page printer

The page printer is equipped with an automatic New Line Function (C.R. + L.F.) which comes into action after the typing of the 69th character on a line.
This New Line Function is not punched or stored in the message memory and solely serves to avoid the typing of a complete line on a single spot in case a Carriage Return is omitted or garbled.

603. Tape reader

The tape reader is controlled by one single control: tape reader on/off button **22**. When a tape has been inserted and the cover closed, pressing the push button for less than $^1/_4$ second will advance the tape one character. Pressing the button for longer than $^1/_2$ second will make the tape reader step as long as tape is being transported. Pushing the button whilst a tape is being advanced through the reader will stop the reader.
This allows for character by character printing. The lid **23** can be lifted from the tape reader so that the tape can be put into place, passing over the taut tape contact **21** and engaging the sprocket wheel with the transport holes.

604. Tape punch

The tape punch is switched on and off by push button **15**; when the lamp inside this button is lit, the punch is switched on. Push button **16** is used for running out tape with punched characters "Letters". Pushing the tape backspacing button **17** makes the tape step back one character so that mistakes can be lettered out.

605. Signals

A procedure signal (3 bells) sounds when buttons are pushed at the "wrong" moment or when the operator makes a mistake. In most cases, the procedure signal is accompanied by blocking of the keyboard and tape reader.
When the sequences as described below are followed, no procedure signal will be given.

SECTION 2 - Plain text mode

606. Application of general crypto procedures

Instructions regarding the application of general crypto procedures, such as arrangement of indicators and text, and the use of codress procedures are contained in the effective edition of AMSG-293. When AMSG-293 is not available, the officer in charge of the crypto center shall be responsible for issuing instructions concerning general crypto procedures. Exclusive of indicators, message length in CEROFF cryptosystem is limited to 1200 groups.

When the plain text of a message or message part will yield more than 1200 groups of cipher text, it must be divided into cryptoparts, each of which contains no more than 1200 groups.

Bisection and variable spacing are not required.

607. General note

In each of the following Sections, it is assumed that the operator starts with all push buttons released and lamps off.

608. Plain text mode

a. Push ON button **2** and press PLAIN button **12** down. Switch on tape punch. Push TAPE PUNCH button **15**.
   The lamps inside both buttons are lit. Text, put in via the keyboard or tape reader is printed and/or punched. Plain text, put in this mode, is not stored in the crypto/message memory.

b. As long as PLAIN button **12** is pressed, any other mode of operation is inhibited. Attempts to assume other modes of operation result in the procedure signal only (the procedure signal does not sound when the buttons OUTPUT INDIRECT or CORRECTION are pushed); the plain text mode overrides any other mode as long as the button **12** is pressed home.

c. Pushing the PLAIN TEXT button **12** after enciphering or deciphering resets the message memory but leaves the keysettings intact.

SECTION 3 - Keysetting

609. Keysetting general

AROFLEX keysetting is accomplished by filling 26 keysetting storage compartments from the key lists. The keyboard is used to gain entry to the key storage at the user's option, by assigning an alphabetical letter to each compartment. This identification is necessary for recalling the keys for enciphering and deciphering procedures. Z for the system key and A through to Y for daily keys.

610. Keysetting operation

See Table 6-I: Keysetting Operation.

611. Keysetting restrictions

Future keys may be stored in the AROFLEX equipment to facilitate communications when hard-copy keying material is not readily accessible, e.g. weekends or holidays, and should only be stored until hard-copy keying material is readily accessible again.

Keys may only be stored in the AROFLEX equipment while it is under continuous custody of cleared personnel authorized access to keying material.
Keys may not be stored in the AROFLEX equipment while it is left unattended, unless it is stored in a security container or vault area approved for the open storage of keying material of the appropriate classification.

612. Use of the System Indicator Key

In the CEROFF-system, the use of the System Indicator Key (AMST-9504) is mandatory from a transmission security point of view. Non-use of the System Indicator Key will result in the encrypted text starting and ending with the group ZZZZZ.
Such occurences should be reported as practice dangerous to security in accordance with Command or Service Instructions.

613. Zeroizing key compartments

a. *Total zeroizing*
Zeroizing of all key compartments can easily be accomplished by pushing the red zeroize button **24** on the front of the crypto module.

b. *Zeroizing individual key compartments*
Zeroizing an individual key compartment can be accomplished by using the keysetting procedure in accordance with Table 6-I for the key compartment concerned, by inserting the following characters after "SELECT" has been printed:
(1) relevant key compartment letter
(2) five digits 1 2 3 4 5 to delete the system indicator of the key to be zeroized
(3) at least 10 characters "A" to render the key to be zeroized useless.

Table 6-I: Keysetting Operation

Ser.	Operation	Machine Function	Remarks
1.	Operate mains switch and ON button.	1. Mains switch neon glows. 2. ON button lamp glows.	Fan motor operated.
2.	Type "KEYINSERT" on keyboard.	AROFLEX prints KEYINSERT followed automatically by INSERT on a new line.	PROCEDURE and DECIPHER lamps glow.
3.	Select key compartment letter on the keyboard.	Print out of key compartment letter as typed.	The user is selecting store location, A to Y for daily keys and Z for the system key. Mark up store location with key short title on tote plate provided.
4.	Enter key by keyboard or tape reader.	Print out of inserted key short title and check group.	Entered keys are stored in assigned storage compartments. Tape reader will stop after key insertion if reader is used.
5.	Enter carriage return or line feed. Additional keys can be entered by repeating steps 3 & 4.	Print out "INSERT" on new line.	All compartments made available for key setting. If a mistake is made in key setting, the procedure alarm will sound and two check groups are printed. These are the correct check group and an incorrect check group generated by the incorrect key. To clear incorrectly entered key, type one CR or one LF.
6.	Operate the OFF button.	ON button lamp off.	Fan motor off. AROFLEX in standby mode. This is a mandatory requirement after key setting procedure before further operations may take place.

Notes:
1. The absence of an indicator key in compartment Z results in all cryptograms starting and finishing with the group ZZZZZ. This signals the absence of an enciphered indicator.
2. The tote plate on the front of AROFLEX may be used to write the check groups or short titles. See par. 615.
3. Emergency destruction of keys may be accomplished by pressing the RED ZEROISING BUTTON **24**.

SECTION 4 - Enciphering

6.1.4 General

Messages can be enciphered in the DIRECT or INDIRECT mode. In practice it may be considered appropriate to use the DIRECT mode for long messages and divide such a task into message header preparation and text preparation. For short messages the INDIRECT mode lends itself to the preparation of the message header and text in one operation, entered directly by the keyboard.

6.1.5 Enciphering DIRECT mode operating procedures

See Table 6-II: Enciphering - Direct Operation.

6.1.6 Enciphering INDIRECT mode operating procedures

See Table 6-III: Enciphering - Indirect Operation.

Table 6-II: Enciphering - Direct Operation

Ser.	Operation	Machine Function	Remarks
1.	Operate the ON button.	Button lamp glows.	Fan motor operated.
2.	Operate PROCEDURE button.	1. Button lamp glows. 2. Print out of System Indicator short title with Check Group. 3. Print out SELECT.	
3.	Type in selected Store location A - Y.	1. Print out of selected store location. 2. Print out of selected Daily Key short title with Check Group. 3. Print out PAGE 1.	If the alarm sounds and CORRECTION lamp flashes, this condition indicates absence of key in selected store. Release PROCEDURE button and take corrective action.
4.	Type in Routing Indicator of the station of origin and the station serial number.	Print out of information as typed.	1. This is the insertion of paging information for the cryptogram. 2. If the paging information is less than 17 characters, one carriage return is necessary to initiate separation. 3. If paging information is equal to 17 characters, separation is automatic.
5.	Type in CR as required (i.e. if paging information is less than 17 characters).	Generation of 15xLF, 2xCR and 17 LS.	This is the separation between the crypto procedure and the message proper.
6.	Type in LS.	Nil.	To change machine to lower case prior to FML 1.
7.	Operate Tape Punch on button.	Button lamp glows.	
8.	Type in FML's 1 to 4 incl., inserting in FML 3 after Julian date but before EOLF one LS. Also in FML 4 omit EOLF.	Print out of information as typed.	1. Ensure that INDIRECT button is released. That is, button is in the up position and the button lamp off. 2. Format Lines 1 - 4 incl. can be entered via the tape reader. 3. To ensure conformity with ACP 127 NATO Supp 3 Figure shifts and Letter shifts must inserted separately in FML 1 - 4 incl., in accordance with ACP 127 Supp 3, Annex B.
9.	Operate PREAMBLE button.	1. Button lamp glows. 2. EOLF generated. 3. PROCEDURE button lamp off.	The operation of this button starts the paging procedure count for the cryptogram.

Table 6-II: Enciphering - Direct Operation (continued)

Ser.	Operation	Machine Function	Remarks
10.	Type in format lines 5, 10 and 11, omitting FML 11 EOLF.	Print out of information as typed.	FML 10 will always be "GR NC".
11.	Operate ENCIPHER button.	1. PREAMBLE button lamp off. 2. ENCIPHER button glows. 3. Print out of enciphered System Indicator, the random message key repeated five times, followed by five other cipher groups.	These machine-generated eleven cipher groups are the first part of Format Line 12.
12.	Enter plain text of message via the keyboard or tape reader.	Print out of cipher groups.	1. If paging of the received deciphered plain text is required, then the original plain text must also be paged. 2. When the enciphering process is completed, printing will cease.
13.	Type in plain text in Format Line 13 and end of transmission sequence.	Print out of further cipher groups.	FML 13 and EOTS of plain text message may be entered via the tape reader. Proceed to step 15 if station validation is required on cryptogram.
14.	Release PROCEDURE button.	1. ENCIPHER lamp off. 2. Automatic completion of cryptogram of FML 12 and 13. 3. Automatic insertion cryptogram FML 14 as group count. 4. Omission of FML 15. 5. Automatic insertion of FML 16.	Final output of machine is now a page copy of the complete message in cipher text together with a tape copy.
15.	Operate PREAMBLE button.	1. PROCEDURE and PREAMBLE buttons glow. 2. ENCIPHER button goes off. 3. Automatic generation of cryptogram FML 13 and 14.	
16.	Insert cryptogram validation symbol, station serial number and one LS.	Print out information as typed.	
17.	Release PROCEDURE button.	Automatic insertion of FML 16.	

Table 6-III: Enciphering - Indirect Operation

Ser.	Operation	Machine Function	Remarks
1.	Operate the ON button	Button lamp glows.	Fan motor operated.
2.	Operate PROCEDURE and then INDIRECT button.	1. Button lamps glow. 2. Print out of System Indicator short title with check group. 3. Print out SELECT.	MEMORY warning lamp glows, indicates memory active.
3.	Type in selected store location A - Y.	1. Print out of selected store location. 2. Print out of selected daily key short title with check group. 3. Print out PAGE 1.	If the alarm sounds and CORRECTION lamp flashes, this condition indicates absence of key in selected store. Release PROCEDURE button and take corrective action.
4.	Type in routing indicator of the station of origin and the station serial number.	Print out of information as typed.	1. This is the insertion of paging information for the cryptogram. 2. If the paging information is less than 17 characters, one carriage return is necessary to initiate separation. 3. If paging information is equal to 17 characters, separation is automatic.
5.	Type in CR as required.	Generation of 15xLF, 2xCR and 17xLS.	This is the separation between the crypto procedure and the message proper.
6.	Type in LS.	Nil.	To change machine to lower case prior to FML 1.
7.	Type in FML 1 to 4 incl., inserting in FML 3 after Julian date but before EOLF one LS. Also in FML 4 omit EOLF.	Print out of information as typed.	
8.	Operate PREAMBLE button.	1. Button lamp glows. 2. EOLF generated. 3. PROCEDURE button off.	The operation of this button starts the paging procedure count for the cryptogram.
9.	Type in FML 5, 10 and 11, omitting FML 11 EOLF.	Print out of information as typed.	FML 10 will always be "GR NC".
10.	Operate ENCIPHER button.	1. PREAMBLE button lamp off. 2. ENCIPHER button glows. 3. EOLF generated.	Oblique strokes indicate indirect mode and marks the point where enciphering begins.
11.	Enter plain text of message via the keyboard or tape reader.	Print out of plain text.	During the indirect mode corrections can be made as described in Chap. 6 Sect. 6 below. The corrected errors are eliminated from the memory.

Table 6-III: Enciphering - Indirect Operation (continued)

Ser.	Operation	Machine Function	Remarks
12.	Type in plain text FML 13 and EOTS.	Print out of input.	If station validation function (FML 15) is required, proceed to Step 18.
13.	Release PROCEDURE button.	1. ENCIPHER lamp off. 2. EOLF generated. 3. 10 oblique strokes generated. 4. EOLF generated.	Oblique strokes mark the end of enciphering. INDIRECT and MEMORY warning lamps remain lit.
14.	Operate tape punch button.	Button lamp glows.	
15.	Operate OUTPUT button.	Print out of 15xLF, EOLF, 17xLS followed by the completed cryptogram.	1. The cryptogram is complete with header and EOTS. 2. Cryptogram will be paged. 3. Cryptogram will omit FML 15.
16.	Repeat operation of OUTPUT button.	Print out of 15xLF, EOLF, 17xLS followed by the completed cryptogram.	Repeated operation of OUTPUT button will generate a further copy of the completed cryptogram.
17.	Release INDIRECT button.	MEMORY warning and INDIRECT buttons off.	Memory now cleared. N.B.: The memory is not cleared until the INDIRECT button is released.
18.	Operate PREAMBLE button.	1. PROCEDURE and PREAMBLE buttons glow. 2. ENCIPHER button lamp off.	10 oblique strokes are printed indicating end of enciphering.
19.	Insert validation symbol and station serial number.	Print out of information as typed.	
20.	Release PROCEDURE button.	PROCEDURE and PREAMBLE lamps off.	
21.	Operate tape punch on button.	Button lamp glows.	
22.	Operate OUTPUT button.	Print out of 15xLF, EOLF, 17xLS followed by completed cryptogram.	The cryptogram is complete with header and EOTS including FML 15.
23.	Release INDIRECT button.	MEMORY warning and INDIRECT button lamps off.	Memory now cleared. N.B.: The memory is not cleared until the INDIRECT button is released.

SECTION 5 - Deciphering

617. General

Deciphering can be performed in both the DIRECT and INDIRECT mode. An advantage of the INDIRECT mode is that multiple copies can be produced of the deciphered plain text. Also corrupted cipher text can be serviced to advantage in the INDIRECT mode by correction procedures.

618. Deciphering DIRECT mode operating procedures

See Table 6-IV: Deciphering - Direct operation.

619. Deciphering INDIRECT mode operating procedures

See Table 6-V : Deciphering - Indirect operation.

Table 6-IV: Deciphering - Direct Operation

Ser.	Operation	Machine Function	Remarks
1.	Operate the ON button.	Button lamp glows.	Fan motor operated.
2.	Operate DECIPHER button.	1. DECIPHER lamp button glows. 2. EOLF and LS generated.	
3.	Enter complete cryptogram on keyboard or tape reader.		Tape punch may be operated, as required.
4.	Operate tape run button as appropriate.	Header and plain text are reproduced.	1. The plain text will include the daily key short title and check group of enciphering key. 2. If the relevant key is not stored, the tape stops after the 11th group and the serial number of the actually used key setting is automatically deciphered and printed, provided the correct indicator key is stored in compartment Z. The slow blinking of the CORRECTION lamp and sounding of alarm indicate the "NO KEY" condition. 3. Incorrect format of a cryptogram, found after the beginning of the cryptogram has been recognized as such cause the lighting of the CORRECTION lamp. The tape itself continues stepping. 4. At the end of each received message, the operator shall note the appearance of the end of message function represented by NNNN and the check group that follows. The operator will record the check group at the beginning of the message header. If the check group OOOOO TTTTT appears, the operator will report it immediately to the comsec officer. For further action, see par. 307.
5.	Release DECIPHER button.	DECIPHER button lamp off.	

Table 6-V: Deciphering - Indirect Operation

Ser.	Operation	Machine Function	Remarks
1.	Operate the ON button.	Button lamp glows.	Fan motor operated.
2.	Operate the DECIPHER and INDIRECT button.	Button lamps glow. 2x EOLF and LS are generated.	MEMORY warning lamp glows.
3.	Enter cryptogram by keyboard or tape reader.	If input is by tape reader, header and first eleven groups of cryptogram are printed and tape reader stops.	Tape punch may be operated as required. If the relevant key is not stored the alarm sounds and the correction lamp blinks, corrective action must be taken.
4.	Operate tape run button as appropriate or continue entry by keyboard.	Reproduction of remainder of cryptogram as transmitted/received.	If cryptogram is entered by keyboard, there is no apparent stop after the 11th cryptogroup if the correct key is present. If correct key is not present, see above. INDIRECT procedure may be required if the cryptogram requires corrections as detailed in Section 6 below.
5.	Operate OUTPUT button.	Complete message in plain text is reproduced.	1. Plain text will include the daily key short title and check group of the enciphering key. 2. At the end of each received message, the operator shall note the appearance of the end of message function represented by NNNN and the check group that follows. The operator will record the check group at the beginning of the message header. If the check group OOOOO TTTTT appears, the operator will report it immediately to the comsec officer. For further action, see par. 307.
6.	Repeat operation of OUTPUT button.	Complete message in plain text is reproduced.	Repeated plain text copies will be produced for every operation of the OUTPUT button.
7.	Release DECIPHER and INDIRECT buttons.	MEMORY warning, INDIRECT and DECIPHER lamps off.	Memory is cleared. N.B.: Memory will hold plain text until INDIRECT button is released.

SECTION 6 - Corrections

620. General

This section of the manual describes the correction of faults which appear in the different operating modes of Aroflex such as, input mistakes, incorrect format, character corruptions etc.

ANNEX A of this manual contains examples to demonstrate the correct message correction procedures.

ANNEX B explains the conversion of the 32 characters of the CCITT code to the 26 characters of the English alphabet and the use of "double characters" in the cryptograms.

621. Corrections in the crypto procedure

Wrong input paging information.

If mistakes have been made in the first 16 characters of the paging information, actuate the CORRECTION button **13** for character-by-character correction of the input.

It is also possible to start a new crypto procedure by releasing and pushing the PROCEDURE button **7** again.

622. Corrections in the INDIRECT ENCIPHERING mode

Wrong clear text input.

AROFLEX is capable of correcting the clear text input in the INDIRECT ENCIPHERING mode, as soon as the memory is active and the store location is selected. If a mistake has been made during the typing in of the text by means of the keyboard, actuating the CORRECTION button **13** will wipe out the last character typed in. As a check, the wiped-out character is printed again. If for instance a mistake is detected after several characters have been typed in, the wrong character will be wiped out by pushing the CORRECTION button **13** repeatedly till the wrong character is printed. Subsequently, the typing-in of the text can continue. Example:

QWICK	KCIW	UICK	results in: QUICK
Keyboard	Correction	Keyboard	

being enciphered and stored. In this way, it is possible to have faultless clear text input via the keyboard. One must not push the CORRECTION button **13** whilst it is still lit: when the lamp inside the button extinguishes after a few seconds, the button can be actuated again.

623. Corrections in the INDIRECT DECIPHERING mode

a. *Mistakes typing-in crypto text*
If a mistake has been made during the typing-in of the crypto text, the last character can be wiped out by pushing the CORRECTION button **13** as described in paragraph 621 above. If for instance ABFDE was put in where ABCDE should have been put in, the CORRECTION button **13** is pushed three times after which the correction can be made and the input of text can be continued.
The printed result is:

ABFDEEDFCDE, resulting in ABCDE in the memory.

b. Key not stored
No signal in the INDIRECT DECIPHER mode after the putting in of the 11th group indicates that the key for deciphering the message is indeed present in the key store: the absence of the correct key is signalled by the printout of the deciphered indicator.

c. Intermediate Output
It is possible to produce an intermediate output any time during the INDIRECT deciphering process. One can check, after carrying out the correction, whether or not it was effective. After an intermediate output, the deciphering process can be continued at the place where it was interrupted.

d. Backstepping characters
Using the CORRECTION button **13** for backstepping character-by-character opens the possibility of producing faultless clear text tapes without "lettering out" of tapes in the plain text mode; in the INDIRECT DECIPHER mode the text can be put in clear form and corrected; AROFLEX regards this clear text as a preamble of a cryptogram.
After the clear text has been put in and terminated by CR, CR, LF actuating the OUTPUT button **10** will produce an output on paper or punch.

e. Wrong groups
If a taped cryptogram is deciphered in the INDIRECT DECIPHER mode, the tape stops after the 11th group. If no signal is given the correct key is present in the key store and the tape can be started again. Incorrect format will also cause the stopping of the tape reader, the sounding of the procedure signal and the lighting of the CORRECTION lamp **13**. The rejected character, read out of the tape reader, is not stored. The correction of the format can be done by hand from the keyboard and subsequently starting the tape reader again.

f. Corruption of a single character
Will as a rule result in the corruption of one or two characters.
Cryptosync will as a rule not be lost as long as the format remains intact.
The effects of the corruption can very often be nullified by making a tape of the deciphered cryptogram and altering the character where the corruption begins, such as for instance incorporating an extra line feed when a "wrong" carriage return occurs or adding a figure or letter shift when a corruption results in a wrong shift.

g. Corruption of the space between groups
In principle, the corruption of one or more spaces between the groups does not matter; once cryptosync has been achieved, the space between the groups are taken for granted by the machine. As long as the total number of characters per line is 59 (10 groups with 9 spaces), followed by CR, CR, LF, cryptosync will be maintained. When deciphering in the Direct mode the Correction lamp will be lit but the cryptogram can be deciphered. Correction in the Indirect Deciphering mode however, will result in stopping the tape because of finding the wrong format: in the Indirect Deciphering mode the machine must find a space after 5 characters.

h. Other mistakes
The "end of crypto" flag consists of NNNN in plain text. When the receiving machine deciphers characters as NNNN, the remainder of the cryptogram is disregarded completely, regardless of the length. To restart the Decipher mode, the machine should be given a consecutive series of 12 letters.

When in original text it is mandatory to transmit NNNN not as End of Message but as part of the text, this NNNN should either be interlaced with spaces or, if that is not allowed, be interspaced with Figs-Letter shifts several times.

624. Corrections in the DIRECT DECIPHERING mode

Format faults in the DIRECT DECIPHERING do not cause blocking of the tape reader but are signalled only by the lighting of the CORRECTION lamp **13**.
The incorporated synchronisation program takes care that cryptosynchrony is not lost forever; depending upon the nature and the frequency of the faults in the crypto text, single characters, whole groups, whole lines or even whole pages can be garbled after which cryptosynchrony is again achieved and correct deciphering is again possible. Cryptosynchrony is regained by means of the format: either after a group, line(s) of 10 groups upon the reading of CR, CR, LF or after the beginning of a new page.

A combination of deciphering the INDIRECT and DIRECT modes make faultless deciphering possible; the worst mistakes can be set right in the INDIRECT mode.

CHAPTER 7

OPERATOR MAINTENANCE

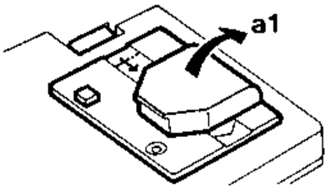
701. Cleaning the Tape reader

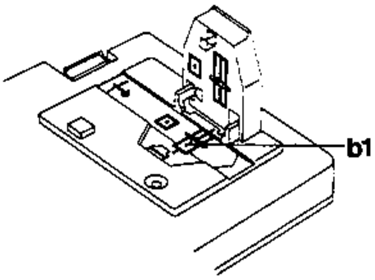
AROFLEX does not need periodic maintenance apart from the daily cleaning of the optical reader:

a. Open the tape retainer (a1)

b. Clean reading point (b1) using a nonfraying soft cloth

c. Close tape retainer





702. Routine Check Security Check

A routine check on the proper operation of AROFLEX is to be carried out at every Crypto change period.

a. Referring to paragraphs 609 and 610 perform the following:

(1) Set a daily key in compartment A, consisting of 12345 and 24 times A.
Press EOLF or CR and the checkgroup printed must be OITDO.

(2) Press EOLF again.

(3) Set a system key in compartment Z, consisting of 99999 and 24 times Z.
Press EOLF or CR and the checkgroup printed must be CFUTH.

(4) Reset the AROFLEX by turning it "OFF" and "ON".

b. Decipher in the DIRECT mode:

```
GKYJU  NFKHF  NFKHF  NFKHF  NFKHF  NFKHF  DQSPZ  HMXBP  BHSUW  BOUWB
TACYW  HAVUA  AKQLN  KOZGH  GZTEW  EPWFR  MFFRJ  YRPVX  GKYJU
```

Result must be: MACHINE O.K.
NNNN

12345 OITDO

(This operation tests the AROFLEX containing a valid key).

c. Decipher in the DIRECT mode:

```
OFKMZ  AXRRK  AXRRK  AXRRK  AXRRK  AXRRK  RBDPF  JWGNI  ORUZK  SSVRS
PEJZD  WUZLD  YVRIN  OFKMZ
BT
```

Result must be: 66666
The correction button blinks and the procedure signal sounds.

(This tests the AROFLEX in absence of a valid key).

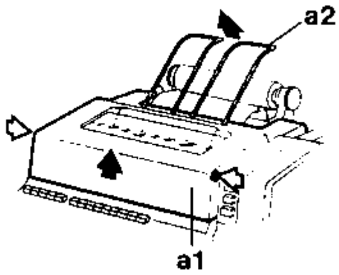
d. Push the red ZEROIZE button, thereby destroying all stored keys and try to encipher or decipher a message according to subpar. b above. It should not be possible to do so. The correction button blinks and the procedure signal sounds.
Cancel by releasing DECIPHER button.

e. If the results of the routine check are all positive, AROFLEX is in good working order. Should these results be negative, repeat the routine security check and, if still proves to be negative, report problem to qualified maintenance personnel.

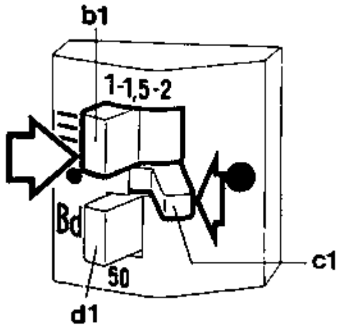
703. Adjusting the line spacing and print force

Before opening cover lid withdraw AC power connector.

a. Open the cover lid (a1).
Swing the paper deflection
frame (a2) to the front.



b. Line spacing (b1):
1 : single line spacing
1,5 : $1^{1}/_{2}$ line spacing
2 : double line spacing.



c. Print force • ● (c1).
Left position of lever : single copy (no carbon copy).
Right position of lever: up to four copies (up to three carbon copies).

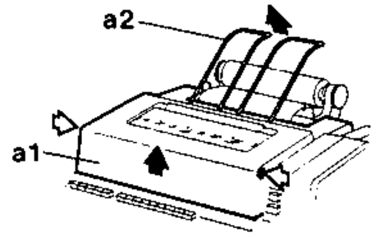
d. Baud Switch (d1) position irrelevant in off-line mode.

REPLACEMENT OF EXPENDABLE ITEMS

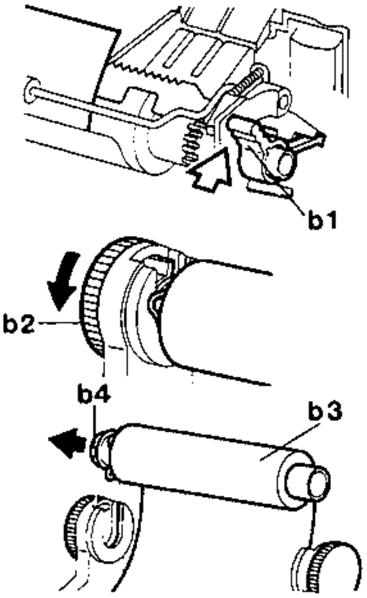
704. Replacing the paper roll

If a colored stripe appears on the edge of the paper, the paper roll must be replaced before the next message is sent or received.

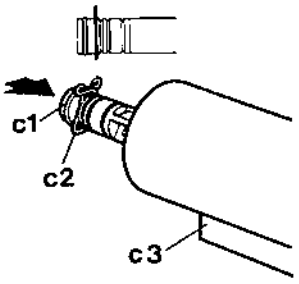
Before opening cover lid withdraw AC power connector.



a. **Open the cover lid (a1).**
Swing the paper deflection frame (a2) to the front.

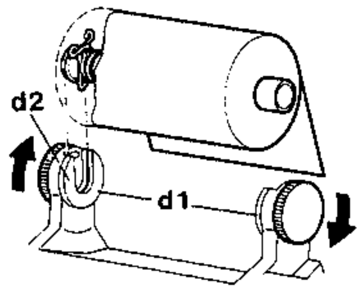


b. **Move paper pressure lever (b1) backwards.**
For mobile use only:
Unlatch paper roll axle (b2) on both sides.
Remove the old paper roll (b3) and pull the rest of paper backwards and out.
Pull paper roll axle (b4) out of the old roll (b3).



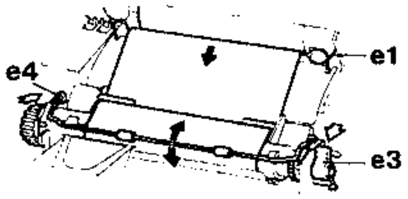
c. **Push the paper roll axle (c1) into the new paper roll until it makes contact with the wire clip (c2).**

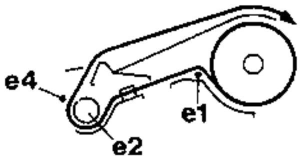
The paper must unwind shown in the picture (c3). The wire clip always rests in the outermost groove.

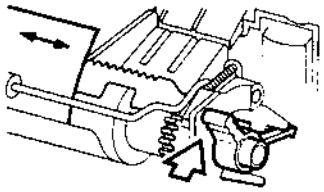


d. **Load the new paper roll into the holder (d1).**
(Latch up the paper roll when the teleprinter is in mobile use)

Ring-shaped collar must always rest in the groove of the left-hand roll holder (d2).

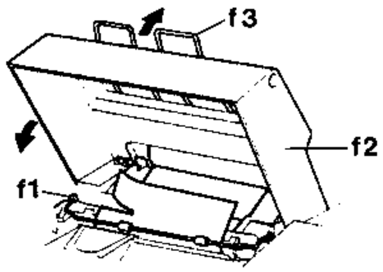






e. **Feed the paper over the pull relief rod (e1) and insert it under the platen (e2).**
Swing the paper pressure lever (e3) to the front.
Swing the paper pressure rod (e4) upwards.
Wind the paper around the platen and feed it under the paper pressure rod (e4).
Swing the paper pressure rod downwards.

(To align the paper: swing the paper pressure lever (e3) backwards)

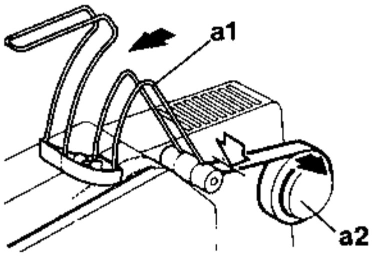


f. **Tear off paper along the tear-off edge (f1).**
Close cover lid (f2).
Move paper deflection frame (f3) backwards.

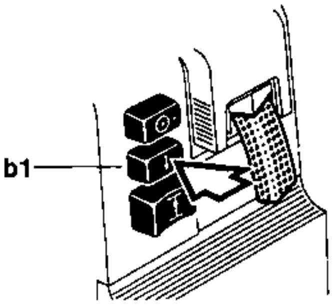
ORIGINAL

705. Replacing the paper tape roll

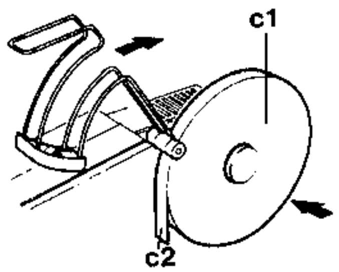
When the colored warning stripe becomes visible while the tape is being unwound the paper tape roll must be changed before the next message is sent or received.



a. **Swing guide rod (a1) upwards.**
Tear off paper tape.
Remove the old tape roll from core (a2).

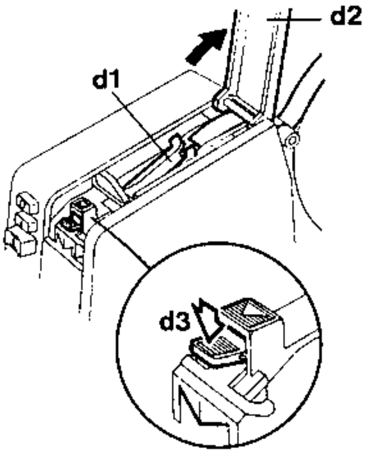


b. **Press the tape feed button (b1) until the rest of paper tape has run out of the tape punch.**



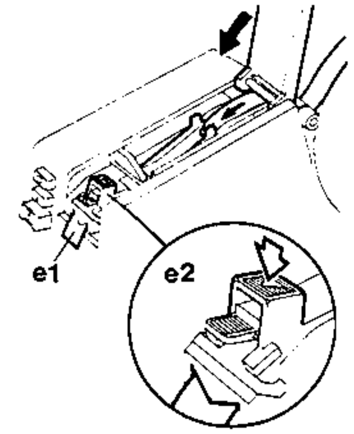
c. **Place the new paper tape (c1) roll over core.**
Swing guide rod back into posilion.

The tape must unwind as shown in the picture (c2).



d. **Advance paper tape in the tape punch until it has reached the beginning of the tape guide (d1).**
Open the cover (d2).
Press on tape gate (d3).

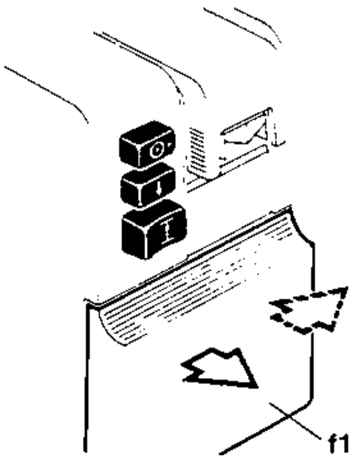
The tape gate swings upwards.



e. **Push the tape further until it emerges from the punch at the front (e1). Press on the tape gate (e2).**

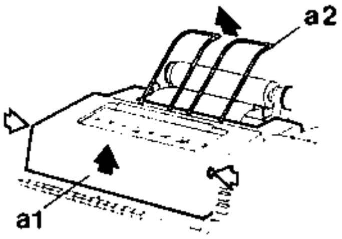
Close the cover. Tear off punched tape upwards.

The tape gate latches. The tape is automatically fed forward by 32 spaces and punched (5-hole combinations).



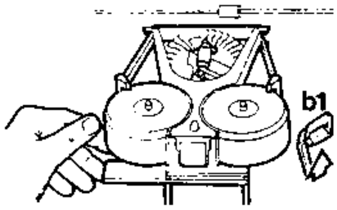
f. **Pull chad waste box (f1) out to the front or sideways and empty.** (Do this every time the tape roll is changed)

706. Replacing the ink ribbon

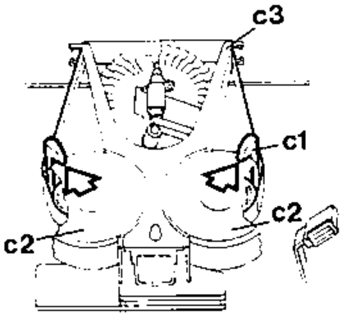


Before opening cover lid withdraw AC power connector.

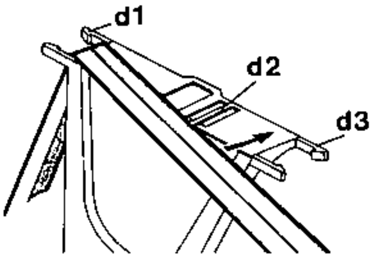
a. **Open cover lid (a1).**
Swing paper deflection frame (a2) to the front.



b. **Press the lever (b1) backwards and swing the printing mechanism up until it latches.**

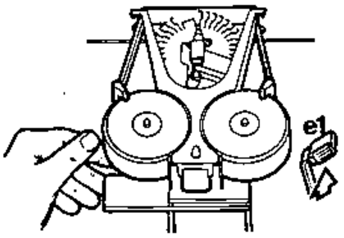


c. **Press lever (c1) in the direction of the arrow and pull ribbon spools (c2) off the guidepins. Remove ink ribbon from lateral guide (c3) and pull upwards and out of guide plate slot.**



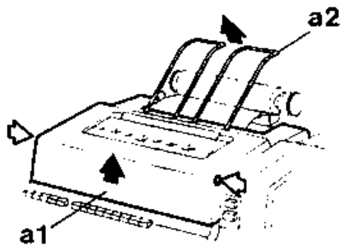
d. **Hook free ribbon end of new ribbon spool to an empty spool just as you do when replacing a typewriter ribbon. Place one ribbon spool in position.**
Ensure red side of ribbon points upwards. Insert ink ribbon in the first lateral guide (d1) on the ribbon guide fork, in the guide plate slot (d2) and the second lateral guide (d3). Install second ribbon spool.

e. **Press lever (e1) backwards.** Printing mechanism swings downwards and latches up.



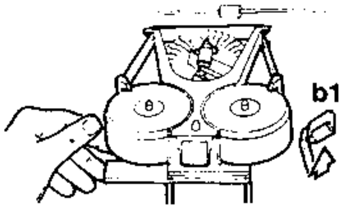
f. **Tear paper off along the tear-off edge.**
Close the cover lid.
Move paper deflection frame backwards.

707. Replacing the print wheel

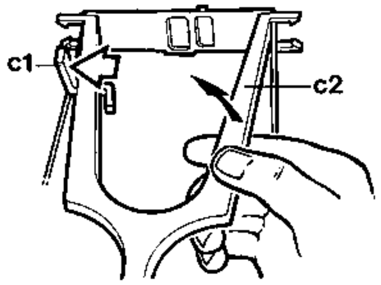


Before opening cover lid withdraw AC power connector.

a. **Open the cover lid (a1).**
Swing paper deflection frame (a2) to the front.

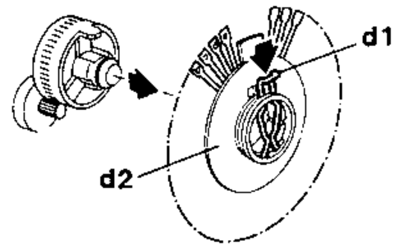


b. **Press lever (b1) backwards and swing the printing mechanism upwards until the latches.**

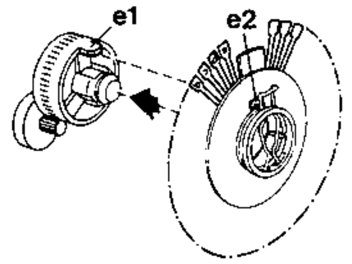


c. **Disengage latch (c1) and swing ribbon guide fork (c2) upwards.**

d. **Press down wire clip (d1) radially and pull off print wheel (d2) in the direction of the arrow.**

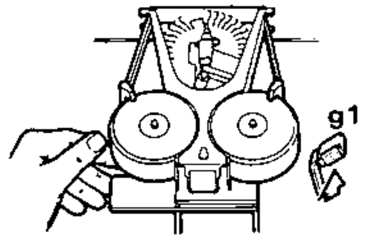


e. **Push the new print wheel in until it locks in position.**
(The driver (e1) must engage in the appropriate opening (e2) of the print wheel)



f. **Swing ribbon guide fork downwards. Ribbon guide fork is locked in position.**

g. **Push lever (g1) backwards.** The printing mechanism swings downwards and locks in position.



h. **Tear paper off along the tear-off edge.**
Close cover lid.
Move paper deflection frame backwards.

708. List of ancillary items

AROFLEX CEROFF equipment UA 8116/06 NSN 5815-17-052-0861.

Note: The paper roll axle, the expendable items and the set of spare parts, delivered with the equipment, are packed in the transit case:

a. Expendable items

(1) paper roll : DIN Std 6720, Sh1; width: 210 mm.

(2) paper tape roll : DIN Std 6720, Sh2; width: 17.4 mm.

b. Transit case for AROFLEX UA 8478/00 NSN ....

c. Set of spare parts UA 8514/00 NSN ....

The set of spare parts is a plastic box containing the following parts:

Part	Quantity	Type No.	NSN
plastic box	1	C22407-Z9-C33	
copy lamp	3	C22230-Z1000-C21	
button lamp	3	C22230-Z1000-C1	
fuse (2.5A medium-lag)	3	D41571-M2500-E2	
print wheel	1	S22711-J1-J213	

Push buttons:

1. Spare
2. ON
3. OFF
4. Spare
5. Spare
6. Memory warning
7. PROCEDURE mode
8. PREAMBLE mode
9. ENCIPHER mode
10. OUTPUT
11. DIRECT/INDIRECT mode
12. PLAIN text mode
13. CORRECTION
14. DECIPHER mode

Other controls:

15. Tape punch ON/OFF
16. Tape run out "Letters"
17. Tape backspacer
18. Tape retaining catch
19. Mains ON/OFF switch
20. Fuse
21. Taut tape contact
22. Tape reader ON/OFF/SINGLE
23. Tape reader cover
24. Zeroize and batteries off
25. Battery drain indicator
26. Power on indicator
27. "Here is" button (inactive)
28. Tote plate

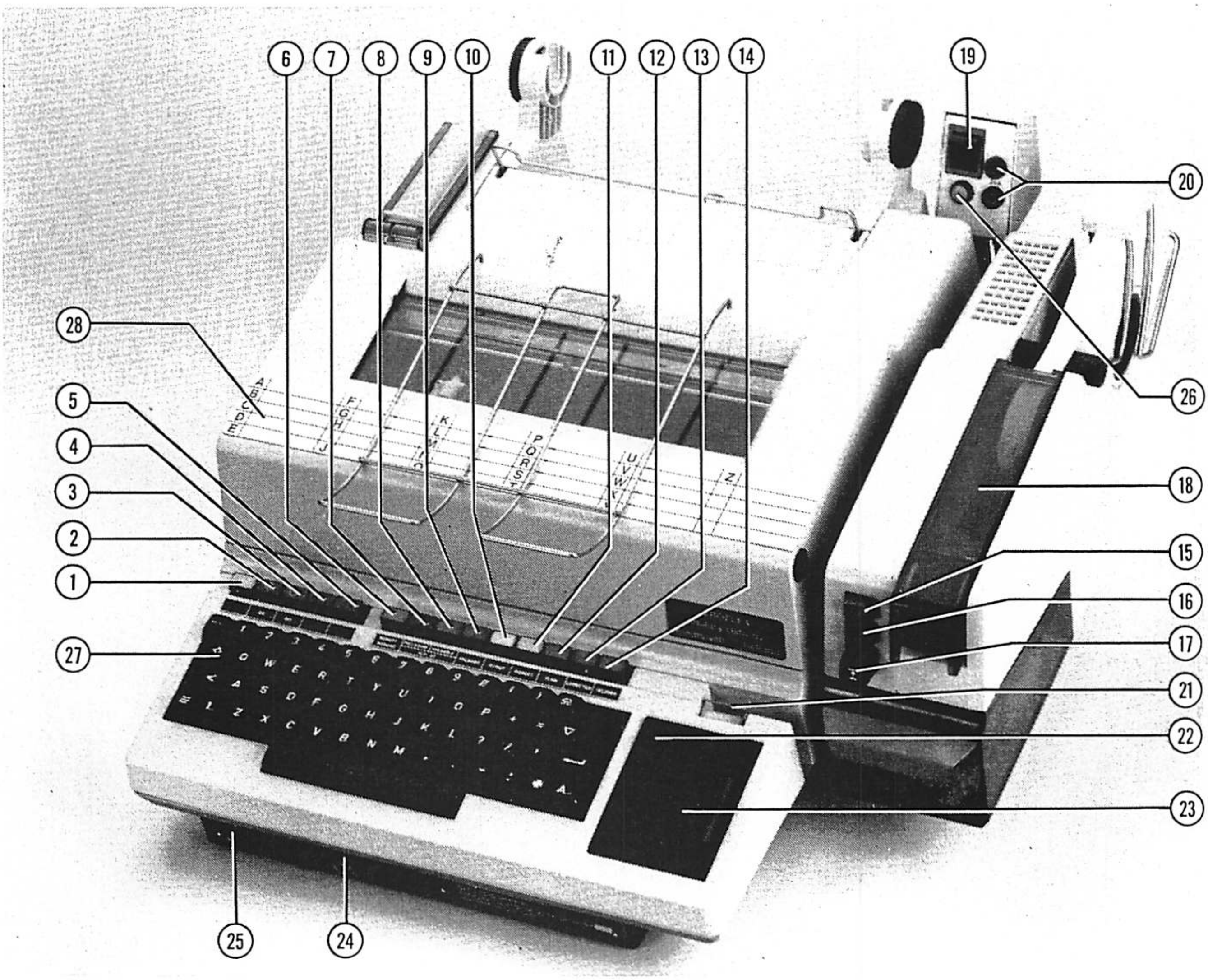


Figure II: Operating controls

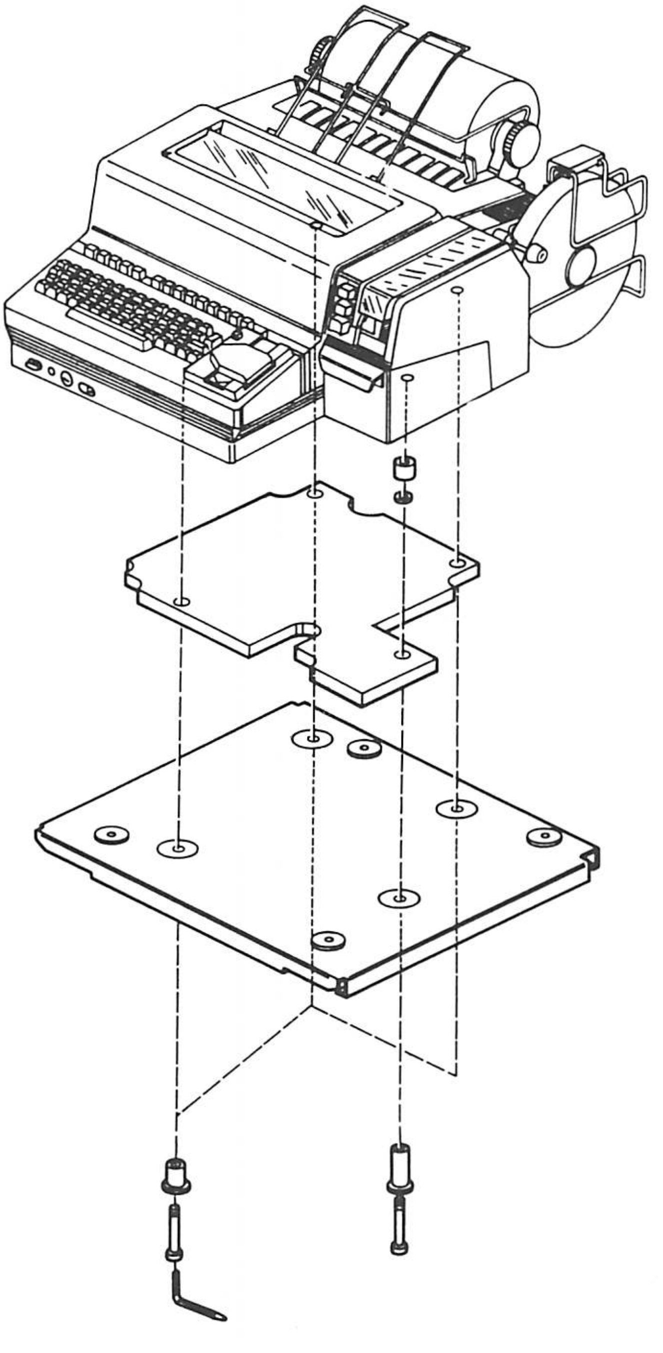


Figure III: Mounting details for mobile use

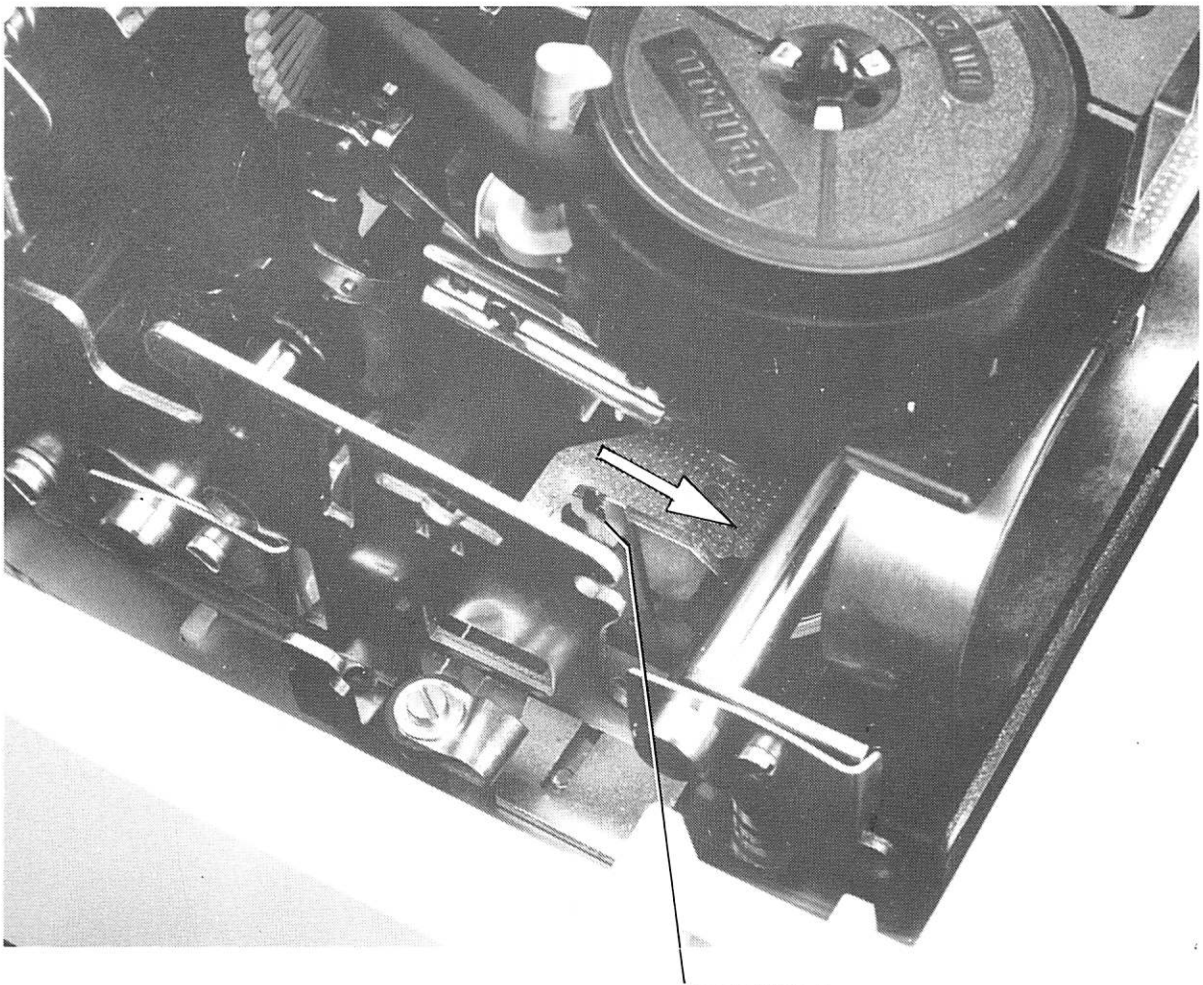


Figure IV: Unlock the printer carriage.

ANNEX A

EXAMPLES FOR MESSAGE CORRECTIONS

ON CEROFF AROFLEX

AROFLEX has two modes of Decipher Operation. These are Direct Decipher Mode and Indirect Decipher Mode. The latter mode of operation is used with Operator Intervention when input from the Keyboard is desired to regain Crypto Synchrony or when monitoring of the input is required.

The following Error Tests were carried out to demonstrate the correct message correction procedures. These corruptions occur after group 12 and before End Of Message Functions only.

1. Error Test No. 1: Group Length Correction (6 letter group)

The last character in the 19th group had a character added immediately before the plain text space.

CIPHER TEXT (example 1)

```
VEDYD LAOGQ LAOGQ LAOGQ LAOGQ LAOGQ XVYHL DRLBW KKVIK PEIPC
MVCYA LLWJJ IGCQA TMHZI DRZHC GULZA WIESC MQBZB FVDZJX RXVRU
OSXFD KWQPW PBPGS RUXOT NMLWB JDZQH JHVOZ CNHMJ FISNU ZJSID
KOSOD SDBSV UVJEJ VEPHZ JHYCR RDBFQ HQJVY VUADA AAYMD RG
```

PLAIN TEXT (example 2)

Decryption method: Direct Deciphering.

```
THE QUICK BROWN FOX JUMPS OVER THE X X
                                       DOG 1234567890
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG 1234567890
```

The correction procedure for the Operator is to Decipher the message again in the Indirect Decipher Mode.

a. Insert tape in reader, press the INDIRECT, DECIPHER and tape run buttons in that order.

b. The tape reader stops the tape automatically after the 11th group is read by the reader.

c. The tape run button is again depressed, the incorrect format of groups 19 and 20 will automatically stop the tape reader.

d. The CORRECTION lamp comes on and the Procedure Signal is heard, the rejected character read by the tape reader is thrown away.

e. The Operator has only to press tape run (error character has been thrown out automatically).

f. Correction lamp extinguishes.

g. The five letter group format of the Cryptogram (example 3) is stored.

h. The Output button is now pressed to obtain a Plain language copy (example 4).

CIPHER TEXT (example 3)

```
VEDYD LAOGQ LAOGQ LAOGQ LAOGQ LAOGQ XVYHL DRLBW KKVIK PEIPC
MVCYA LLWJJ IGCQA TMHZI DRZHC GULZA WIESC MQBZB FVDZJ RXVRU
OSXFD KWQPW PBPGS RUXOT NMLWB JDZQH JHVOZ CNHMJ FISNU ZJSID
KOSOD SDBSV UVJEJ VEPHZ JHYCR RDBFQ HQJVY VUADA AAYMD RG
```

PLAIN TEXT (example 4)

Decryption Method: Indirect Deciphering.

```
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG 1234567890
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG 1234567890
```

2. Error Test No. 2: Space changed to an alphabet character

a. The plain text space between group 19 and 20 is changed to an alphabet character.

CIPHER TEXT (example 5)

```
VEDYD LAOGQ LAOGQ LAOGQ LAOGQ LAOGQ XVYHL DRLBW KKVIK PEIPC
MVCYA LLWJJ IGCQA TMHZI DRZHC GULZA WIESC MQBZB FVDZJARXVRU
OSXFD KWQPW PBPGS RUXOT NMLWB JDZQH JHVOZ CNHMJ FISNU ZJSID
KOSOD SDBSV UVJEJ VEPHZ JHYCR RDBFQ HQJVY VUADA AAYMD RG
```

PLAIN TEXT (example 6)

Decryption Method: Direct Deciphering.

```
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG 1234567890
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG 1234567890
```

Correction is not required, after a five letter group the AROFLEX looks for a space function. If the space is changed to an alphabet character, this has no effect on the deciphering procedure. The Plain text copy is error free (example 6).

b. The spaces between all groups after group 12 are changed to the alphabet character A: this has no effect and crypto synchrony has been maintained.
The space function separating the groups is in error: no influence on the plain text copy.

CIPHER TEXT (example 7)

```
VEDYD LAOGQ LAOGQ LAOGQ LAOGQ LAOGQ XVYHL DRLBW KKVIK PEIPC
MVCYA LLWJJAIGCQAATMHZIADRZHCAGULZAAWIESCAMQBZBAFVDZJARXVRU
OSXFDAKWQPWAPBPGSARUXOTANMLWBAJDZQHAJHVOZACNHMJAFISNUAZJSID
KOSODASDBSVAUVJEJAVEPHZAJHYCRARDBFQAHQJVYAVUADAAAAYMDARG
```

PLAIN TEXT (example 8)

Decryption Method: Direct Deciphering

```
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG 1234567890
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG 1234567890
```

3. Error Test No. 3: Group Length Correction (4 letter group)

The last character of group 19 is omitted.

CIPHER TEXT (example 9)

```
VEDYD LAOGQ LAOGQ LAOGQ LAOGQ LAOGQ XVYHL DRLBW KKVIK PEIPC
MVCYA LLWJJ IGCQA TMHZI DRZHC GULZA WIESC MQBZB FVDZ_RXVRU
OSXFD KWQPW PBPGS RUXOT NMLWB JDZQH JHVOZ CNHMJ FISNU̅ ZJSID
KOSOD SDBSV UVJEJ VEPHZ JHYCR RDBFQ HQJVY VUADA AAYMD RG
```

PLAIN TEXT (example 10)

Decryption Method: Direct Deciphering

```
THE QUICK BROWN FOX JUMPS OVER THE□:✤2,✤9⊟1234567890
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG 1234567890
```

The correction procedure for the Operator is to decipher again in the Indirect Decipher Mode.

a. Insert tape in reader, press the INDIRECT, DECIPHER and tape run buttons in that order.

b. The tape reader stops the tape automatically after the 11th group is read by the reader.

c. The tape run button is again pressed and the incorrect format of group 19 stops the tape reader.

d. The correction lamp comes on and the Procedure Signal sounds. The rejected character here is thrown out (in this case it is the space function).

e. The Operator makes the correction by putting in a * character and a space function (by means of the Keyboard) and pushes the tape run button.

f. The correction lamp extinguishes.

g. The cryptogram is now back to five letter groups (example 11).

h. The Output button is depressed to obtain a plain language copy (example 12).

* The Operator may choose any letter character to insert at this point as it will produce only one letter error in the Plain text. The redundancy of the English language is such that this should not cause too many problems to understand the meaning of the words.

CIPHER TEXT (example 11)

VEDYD LAOGQ LAOGQ LAOGQ LAOGQ LAOGQ XVYHL DRLBW KKVIK PEIPC
MVCYA LLWJJ IGCQA TMHZI DRZHC GULZA WIESC MQBZB FVDZ$\underline{A}$ RXVRU
OSXFD KWQPW PBPGS RUXOT NMLWB JDZQH JHVOZ CNHMJ FISN$\overline{U}$ ZJSID
KOSOD SDBSV UVJEJ VEPHZ JHYCR RDBFQ HQJVY VUADA AAYMD RG

PLAIN TEXT (example 12)

Decryption Method: Indirect Deciphering

THE QUICK BROWN FOX JUMPS OVER THEOLAZY DOG 1234567890
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG 1234567890

4. Error Test No. 4: Corruption of a double character J

The letter J is a double represented character and its plain language equivalent is ZJ. Hence when the J is encrypted there will be two characters in the crypto text representing J (ZJ).
The ZA in group 16 is the encrypted version of ZJ. (See identity chart page A-8.)

a. Stage 1. The Z which in this case was encrypted as a Z will be corrupted.

CIPHER TEXT (example 13)

VEDYD LAOGQ LAOGQ LAOGQ LAOGQ LAOGQ XVYHL DRLBW KKVIK PEIPC
MVCYA LLWJJ IGCQA TMHZI DRZHC GUL$\underline{E}$A WIESC MQBZB FVDZJ RXVRU
OSXFD KWQPW PBPGS RUXOT NMLWB JDZ$\overline{Q}$H JHVOZ CNHMJ FISNU ZJSID
KOSOD SDBSV UVJEJ VEPHZ JHYCR RDBFQ HQJVY VUADA AAYMD RG

PLAIN TEXT (example 14)

Decryption Method: Direct Deciphering

UMPSQUVER BROWNAZOXDOG 1234567890
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG 1234567890

The above example 14 has shown how the corruption of the Z before J in the crypto format resulted in a carriage return and the character "U", being generated during the decryption process. (The characters ZJ should have been generated, and the J only being printed.)

b. Stage 2. The J which is encrypted as an A will be corrupted.

CIPHER TEXT (example 15)

```
VEDYD LAOGQ LAOGQ LAOGQ LAOGQ LAOGQ XVYHL DRLBW KKVIK PEIPC
MVCYA LLWJJ IGCQA TMHZI DRZHC GULZE WIESC MQBZB FVDZJ RXVRU
OSXFD KWQPW PBPGS RUXOT NMLWB JDZQH JHVOZ CNHMJ FISNU ZJSID
KOSOD SDBSV UVJEJ VEPHZ JHYCR RDBFQ HQJVY VUADA AAYMD RG
```

PLAIN TEXT (example 16)

Decryption Method: Direct Deciphering

```
THE QUICK BROWN FOX FUMPS OVER THE LAZY DOG 1234567890
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG 1234567890
```

The plain text copy example 16 has an obvious error, but can be interpreted to read JUMPS. The plain text copy example 14 however has overprinting which makes it almost impossible to read the text. The error here happened when the Z before the J was corrupted and it turned out to be a carriage return.

c. The correct correction procedure in the Indirect Decipher Mode is as follows:

(1) Insert tape in tape reader, press Indirect Decipher and tape run buttons in that order.

(2) Tape reader stops the tape automatically after the 11th group is read by the reader.

(3) Tape run button is depressed and the cryptogram is repeated as in example 13.

(4) Engage the tape punch and then the output button, a plain text tape has been produced complete with error.

(5) The plain text tape is placed in the tape reader and stepped through character by character. When the machine function for carriage return occurs on the tape it is omitted by advancing the tape in the reader by hand, example 17 or allowing the carriage return to be read then stopping the tape and inserting a line feed by way of the keyboard and then starting the tape reader again to complete the message (example 18).

PLAIN TEXT (example 17)

```
THE QUICK BROWN FOX UUMPS OVER THE LAZY DOG 1234567890
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG 1234567890
```

PLAIN TEXT (example 18)

```
THE QUICK BROWN FOX U>
UMPS OVER THE LAZY DOG 1234567890
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG 1234567890
```

5. Conclusion

The error tests have shown errors which effect crypto procedure and a corruption of a double represented character. Corrections which involve a wrong character in the crypto text or a garbled crypto text will have to be handled by the Operator individually in a common sense way. The procedure that was used in error test no. 4 will apply if the text is garbled; if the message cannot be patched in this manner a rerun of the cipher text would be required.

6. Cipher text and tape used for error tests

```
VEDYD LAOGQ LAOGQ LAOGQ LAOGQ LAOGQ XVYHL DRLBW KKVIK PEIPC
MVCYA LLWJJ IGCQA TMHZI DRZHC GULZA WIESC MQBZB FVDZJ RXVRU
OSXFD KWQPW PBPGS RUXOT NMLWB JDZQH JHVOZ CNHMJ FISNU ZJSID
KOSOD SDBSV UVJEJ VEPHZ JHYCR RDBFQ HQJVY VUADA AAYMD RG
```

CHECK GROUPS:

A 12345 OITDO

Z 12345 CFUTH

Groups 12 through 40 were used for corruptions.

AROFLEX MESSAGE CORRECTION PROCEDURES IDENTITY CHART

```
LS  T   H   E   SP      Q   U   I   C       K       SP    B     R       O   W   N   SP  F
                                        ┌───┴───┐       ┌─┴─┐
L   L   W   J   J       I   G   C   Q   A       T   M   H   Z   I       D   R   Z   H   C

O   X   SP    J         U   M   P   S   SP      O     V     E   R       SP  T   H   E   SP
            ┌─┴─┐                                   ┌─┴─┐
G   U   L   Z   A       W   I   E   S   C       M   Q   B   Z   B       F   V   D   Z   J

L   A     Z     Y       SP  D   O     G         SP  FS  1   2   3       4   5   6   7   8
        ┌─┴─┐                       ┌─┴─┐
R   X   V   R   U       O   S   X   F   D       K   W   Q   P   W       P   B   P   G   S

9   0   CR  CR  LF      LS  T   H   E   SP      Q   U   I   C       K       SP    B     R
                                                                ┌───┴───┐       ┌─┴─┐
R   U   X   O   T       N   M   L   W   B       J   D   Z   Q   H       J   H   V   O   Z

O   W   N   SP  F       O   X   SP    J         U   M   P   S   SP      O     V     E   R
                                    ┌─┴─┐                                   ┌─┴─┐
C   N   H   M   J       F   I   S   N   U       Z   J   S   I   D       K   O   S   O   D

SP  T   H   E   SP      L   A     Z     Y       SP  D   O     G         SP  FS  1   2   3
                                ┌─┴─┐                       ┌─┴─┐
S   D   B   S   V       U   V   J   E   J       V   E   P   H   Z       J   H   Y   C   R

4   5   6   7   8       9   0   CR  CR  LF      LF  LF  LF  LF  LF      LF  LF  LS  N   N

R   D   B   F   Q       H   Q   J   V   Y       V   U   A   D   A       A   A   Y   M   D

N   N

R   G
```

TABLE A-1

ANNEX B

32 TO 26 CONVERSION OF

CCITT CODE

The CCITT code consists of 32 characters but the cryptograms are restricted to the 26 characters of the English alphabet only. This means that some measures have to be taken to present 32 characters in the 26 mode. This is achieved by the use of "double characters". These double characters consist of a "warning" character followed by the character proper. The warning character is the character Z whilst the "rare" characters G, V, Z, B, J and K are preceded by a Z.

It might seem that it would have been better to represent the machine functions (Figs, Letters, Space, Carriage Return, Line Feed, All Blanks) as "double" characters but the characters G, V, Z, B, J and K occur much more rarely than the machine functions. This implies that for enciphering/deciphering purposes the machine functions are transformed into other characters according to a fixed transformation table.

The above implies that corruption of a cryptocharacter can have unpredictable results: it might be that a cryptotext corruption is not even noticed or that the text seems to be completely unreadable. When a machine function is corrupted, the effect may be very extensive.

With a combination of plain text tapes, correcting cryptograms and operating in the indirect decipher mode with intermediate output, the original text, when consisting of words, can be reproduced. Figures of course must be completely exact, reason why it is common practice to repeat figures at the end of the cryptogram.