AROFLEX (UA 8116) and BID 1100

AROFLEX 8116: The crypto module is the black box which is bolted to the bottom of the unit under the keyboard. UA8116 is actually the model name of the keygen card, Most users referred to the machine simply as Aroflex.

The AROFLEX type UA 8116 highly automated equipment for the rapid, reliable, and efficient OFF-LINE encryption of written or punched tape messages. Additionally, AROFLEX can be used as a stand-alone message tape preparation facility. Line-connected operation is made possible by the addition of suitable line-terminating circuitry and appropriate COMSEC measures.

This 5-level, 50 to 100 baud teleprinter employs a Siemens daisy wheel printer. The commercial version of the teleprinter was called the T-1000 while the crypto version was known as the 1000 CA. (CA means Cryptological Application). For Siemens, this computer controlled printer was the high point of the Telex era.

AROFLEX also contains a light-weight optical tape reader and a compact tape punch. The flat and shallow Norwegian produced crypto module is bolted to the bottom of the teleprinter while the operating controls for both teleprinter and crypto module are grouped in a single row along the top of the keyboard. Normally it was set up to operate at 50, 75 or 100 baud on-line, but in the off line mode it operated at 100 baud.

Instead of the tape punch, a magnetic tape cassette recorder can be connected. The magnetic tape has a storage capacity of some 60,000 characters; the recorder can be used for the medium-speed transmission/reception of cryptograms with the aid of special modems. Stand-alone tape readers and tape punches, operating at speeds of up to 600 baud, can be connected to AROFLEX, thus increasing the throughput speed from 100 to 600 baud. AROFLEX has a standard crypto memory of 6 pages (120 lines of crypto groups) and the format of the cryptograms produced is completely in accordance with the ACP-127 procedure.

A. KEY SETTING

AROFLEX has 26 stores for keying variables: 23 for ordinary traffic, 2 for SPECAT (Special Category) traffic and 1 for enciphering/deciphering the system indicators (serial numbers of the keys).

Insertion of a new key is simple and takes only a few moments:
• insert and turn the physical INSERT key in the appropriate lock on the crypto module.
• type the address of the required key store.
• type the serial number, the keying variables and the check word from the key list.
• remove the INSERT key

The keying variables can also be inserted by means of punched tape fed through the tape reader. A connector for an electronic gun is fitted for keying purposes. The two SPECAT key stores can only be used (for key-setting, encryption, or decryption) if the physical SPECAT key is inserted and turned in the second lock on the crypto module. The use of "all zero" or "empty" key stores is automatically inhibited. In an emergency situation, all stored keying variables and the contents of the crypto memory are destroyed instantly on firmly pushing the red button on the crypto module.

B. LINE CONNECTED OPERATION

AROFLEX readily lends itself to line-connected operation for transmission and reception of both clear and crypto text. The addition of suitable line circuitry and communications security devices turns a pure off-line equipment into a self-contained line-connected crypto terminal.

Whenever AROFLEX is connected to the line, a clear warning lamp lights up to signal to the operator that he is not operating in the off-line mode. Classified text is first off-line encrypted in the INDIRECT mode. When the encryption process has been completed, the OFF LINE mode is terminated by pushing of the OUT button; next the LINE CONNECT button is pressed. As a result of the pushing of the OUTPUT button, the complete cryptogram is then transmitted at the appropriate line speed.

C. DECIPHERING

AROFLEX is capable of virtually "on-line decryption when it is set to the DIRECT DECIPHER mode; incoming cryptograms are automatically decrypted and printed or punched. If the correct key is not stored, or if a SPECAT key was used, or if a clear text message is received, the actual incoming text is printed and punched for later processing. As soon as a message comes in, the warning lamp lights up and any off-line process is "frozen" immediately, to be resumed when the message has been received completely and the line is released again. The answer-back device is always free to react to the "Who are you?" signal.

D. TYPES OF LINES

Line circuitry for point-to-point circuits, telex networks, store-and-forward systems, and Telex Over Radio (ARQ) is available, covering a wide range of signalling voltages, currents, polarities, and characteristics. AROFLEX is provided with the normal teleprinter controls for either point-to-point or switched circuits; these controls are: "CALL", "CLEAR", "HERE IS", "PUNCH STAND BY", and "OFF LINE". All teleprinter controls are grouped together in the left-hand row of push buttons directly above the keyboard.

E. SUMMARY OF FEATURES

OFF-LINE MODE

• Direct encryption/decryption with immediate output.
• Indirect encryption/decryption with monitoring of the input, and intermediate storage, of the cryptogram and subsequent production of the output in a second cycle of operations.
• Completely automatic decryption.
• Plain text modes without and with counting of line feeds and automated procedures in accordance with ACP-127.
• Plain text copy.

LINE CONNECTED MODE

• Automatic on-line decryption.
• Unrestricted transmission of cryptograms.
• Ample communications security devices against operator's mistakes.
• Line circuitry for point-to-point circuits, for circuit-switched networks and store-and-forward systems for Telex over Radio (ARQ).
• Stand-by position with automatic start of tape punch.

INPUT/OUTPUT

• Keyboard with automatic figures/letters shift, automatic carriage return plus line feed.
• Built-in lightweight optical tape reader.
• Daisywheel printer which can be switched off.
• Clip-on tape punch.
• Option of connecting external stand-alone tape readers and punches of more than 600 baud via adaptors.

FORMAT

• Crypto output in 5-letter groups in the English alphabet and the CCITT # 2 code; one space between groups; 10 groups to one line; 20 lines to one page; 6 pages to one transmission section.
• Automated beginning, paging information, and termination of messages with automatic group count, according to ACP-127.
• Automatic correction of format or during decryption.
• Manual rectification of format or input possible during decryption in the INDIRECT mode, in order to ensure flawless decryption.

KEY SETTING

• Five figure indicator plus 24 characters plus five letter check word which can be inserted by means of the keyboard or tape reader.
• 23 "general" and 2 "special category" key stores.
• Automatic generation of check word for each key.
• Use of "all zero" or "empty" key stores impossible.
• Zeroizing of all key stores and crypto memory in case of emergency by pushing a special button.
• No loss of stored keys or contents of crypto memory during power mains interruptions of less than 1 hour.
• Automatically generated and processed message key automatic selection of key-setting for decryption.
• Key stores accessible for insertion of new keys only when a physical key is turned in a lock.

BASIC DATA

• Height: 230 mm; 330 mm with full roll of paper.
• Width: 420 mm; 530 mm with clip-on tape punch.
• Depth: 550 mm; 600 mm with full roll of paper.
• Weight: 20 kg; 25 kg with tape punch; 35 kg in transport case.
• Power supply: 110/220 VAC, 50/60 or 400 Hz.
• Power consumption: 150 VA (volt-amps) in full operation, 40 VA in stand-by mode.
• Operating temperature range: - 10°C to + 55°C.
• MTBF: calculated to be well in excess of 5000 hours. No periodic maintenance or electronic calibration required.
• Noise with operating tape punch: less than 55 dB (A)

CRYPTOLOGICAL DATA

• 1036 different key families.
• 107 variations of any key family.
• Guaranteed minimum length of any key series: 240 years at 100 baud.
• Automatic generator for random message keys.
• L.S.I, hardware key generator, software controlled adequate fail-safe and TEMPEST measures.

OPTIONAL ITEMS

• Magnetic cassette tape recorder instead of tape punch.
• Wooden or metal transport cases.
• Line terminating circuitry for line-connected mode.
• Electronic gun for rapid key-setting.
• Adaptors to connect stand-alone tape equipment to AROFLEX.

MAIN CRYPTO CONTROLS

• Physical key for INSERTING key settings.
• PROCEDURE and PREAMBLE buttons for clear text start and end of message.
• ENCIPHER
• DECIPHER
• PLAIN TEXT

SECONDARY CRYPTO CONTROLS

• Selection of DIRECT or INDIRECT mode.
• Production of OUTPUT.
• CORRECTION of input during INDIRECT DECRYPTION and ENCRYPTION.
• Physical SPECAT key for SPECAT traffic.
• ZEROIZING all key stores and crypto memory.

USEAGE

The Aroflex device was used by the Canadian Diplomatic Communication Service[1.] (CDCS) in the few missions where it was deployed for rapid and reliable encryption and decryption of messages. The correct daily key was automatically selected at the beginning of decryption. After decryption, the plain text could either be printed or sent to a tape punch. One of the device's endearing features was the fact that an operator could use the device without removing it from the shipping case.

Aroflex was first manufactured by Philips Usfa B.V in the mid-1970's. The designed was based on the Intel 8080a CPU.

Footnotes:
[1.] This term went out of use when the Department of Foreign Affairs and International Trade (DFAIT) adopted an encrypted e-mail system which was called SIGNET. That acronym means *S*ecure *I*ntegrated *G*lobal *Net*work.
Signet-C: Classified network permitting information storage/transmission up to the SECRET level.
Signet-D: Designated or unclassified network permitting information storage/transmission up to Protected C level.
Currently (2005), Signet 3 is being deployed on Signet-D infrastructure around the world using Windows 2003 platform servers and XP Pro on workstations. In native mode and 100% deployment, the storage of information and transmission will meet Protected A level .