MILS ELEKTRONIK
G.m.b.H. & Co. KG

Dorfstrasse 20
A-6060 Mils / Austria
Phone (52 23) 77 10-0, 24 77-0
Fax (52 23) 24 77 18
Telex 533009 mils a
DVR 0421701

Technical specifications for the cipher machine "ME 640"

TABLE OF CONTENTS

Mils,

I/2

MILS ELEKTRONIK
G.m.b.H. & Co. KG

Dorfstrasse 20
A-6060 Mils / Austria
Phone (52 23) 77 10-0, 24 77-0
Fax (52 23) 24 77 18
Telex 533009 mils a
DVR 0421701

Technical specifications for the cipher machine "ME 640"

1. Object:

The "ME 640" is an off-line unit to encipher/decipher messages transmitted by telex or letters. It can be adapted to each standard terminal (interface RS 232) or any teleprinter (interface current loop).

Depending the station where the mixer "ME 640" is used, it can be equipped with different peripheral equipment (terminals), which allow a more or less comfortable operation and more or less throughput. That means, stations with high or medium message traffic work with faster printers, readers or perforators than stations with low message traffic - but the cipher machine is always the same!

1.1 Photoreader (standard) in order to read the random key tape (red punched tape in our catalogue ME 640).

1.2 Option: Special photoreader with five LED´s, to display the respective character which is read actually

1.3 Option: Single step operation
Two additional push buttons allow to position the key tape to the actual insertion marking by pressing only the "single step forward" button or the "single step backward" button.

This option is recommended only in connection with option 1.2.

Comment:

Both of the options (1.2 and 1.3) together support the operator to put in the key tape at the correct character.

After closing the flap of the photoreader the actual character which will be read as next, is displayed by five LED´s.

In case the operator is shifting the key tape during putting in, the wrong character is displayed.

With the two buttons "single step forward" and "single step backward" the operator can move the key tape either in one or the other direction until the character, with which the encipher/decipher process must be started, is on the correct position.

2. Function Specifications:

2.1 Text input via:

- keyboard of the connected terminal/teleprinter
- photoreader of the connected terminal/teleprinter

2.2 Text output via:

- page printer of the connected terminal/teleprinter
- perforator of the connected terminal/teleprinter

2.3 Output format:

The ciphered text can have any requested format (like groups of 5 characters) and can consist either of

- 10 figures or	(modulo 10)
- 16 free choiceable letters or	(modulo 16)
- 26 letters or	(modulo 26)
- 31 telex-characters or	(modulo 31)
- 32 telex-characters or	(modulo 32)
- other combinations on request at no extra cost	

Comment:

In international telex networks there are special sequences of characters which represent commands for the telex exchanges (i.e. the sequences "MMMM" or "....") interrupt the line). This does not matter as long as only plaintext is transmitted because there are no sequences like mentioned above. However, an encrypted message can exist out of any combination or sequence - also out of such one mentioned above.

There are also customer specific telex networks, where a certain sequence of characters can remote control some functions of the on-line teleprinter at the receiving station (i.e. automatic start of the tape reader, where a prepared punched tape is put in).

In order to prevent from such results the enciphered message can consist of a combination of any 16 letters. That means that all these letters which have a "remote control function" where suppressed and will appear in the enciphered message not at all.

2.4 Facilities of tests:

2.4.1 Automatic self diagnostic:

Whenever the operator wants, he can start an automatic self diagnostic routine which checks all internal functions of the equipment. In case a hardware module has malfunctioned an error report is printed via the connected teleprinter notifying the operator which module has to be replaced.

2.4.2 Component-level:

On request we can offer a microprocessor controlled, compact test unit which allows automatic detection of some 96% of component faults from a PC-board.

2.5 Particularities:

2.5.1 Automatic re-synchronization in case of transmission errors:

Comment:

In sending messages, one generally has to take into account transmission errors which may garble the message being received, the garble rate being a function of the quality of the transmission channel.

Transmission errors which either add or delete letters from the message received have disastrous consequences on the readability of the decrypted plaintext, when countermeasures are lacking. Both types of errors have the same effect: they disturb the relationship of the ciphertext to the key sequence of the receiving side. This means that the message can no longer be continuously decrypted. Many errors like this hinder manual attempts at decryption since it is already so difficult that this can only be done successfully with considerable expenditure of time.

To remedy this you need complicated programm routines which automatically suppress such errors and under almost all circumstances guarantee the integrity of the ciphertext being received.

Under this option these kinds of transmission errors are corrected automatically in order to make sure the synchronisation between key and encrypted message during the encipher process.

Restriction:
The automatic error correction works only if enciphering process is executed in modulo 10, 16 or 26.

A copy explaining the efficiency of this automatic error correction is attached to this offer.

2.5.2 Figure shift/letter shift function during the deciphering process:

As described under 2.5.1 the automatic re-synchronization prevents indeed the propagation of a transmission error into the following text. Due to mathematical rules, however, the individual fault itself can be corrected only in a very limited way.

If such a transmission error entails at the receiving station a figure shift character, the following text will be printed on figure side until the next letter shift character appears.

For the praxis this means, the illegibility of a corresponding length of text, even only one character has been garbled into figure shift or letter shift.

With the figure shift/letter shift function the operator can insert subsequently several characters, in order to increase the legibility of the deciphered plaintext.

In order not to falsify the original message, the machine "ME 640" accepts only four characters to be inserted afterwards: letter shift, figure shift, carriage return and line feed. As these characters do not interfere into the decipher process they are used only to control the output format of the deciphered plaintext. Due to this fact, they can be used within the text at any position and as often as required.

2.5.3 Memory function:

This function allows the multiple use of an once inputted plaintext.

Comment:

Depending to the content of a message, mostly a different number of copies from this message is required.

This function allows, by inputting of a certain number, a corresponding output of copies - directly from the memory.

The advantage of this function can be found especially in the following three points:

- the last copy is readable just as good as the first one
- it can be worked constantly with one-fold paper (saving of expense)
- no carbon paper is necessary, which has to be destroyed because of security reasons as well as copies which eventually will not be used.

Of course, an once prepared plaintext can also be enciphered for different addressees with individual keys (further details see point 3.5).

2.5.4 Header function (further details see point 3.6)

2.5.5 Text editing to correct typing errors during text inputting

2.5.6 Dialogue-controlled operator guidance:

A well designed operator dialogue in your mother-language in order to operate the "ME 640" via the keyboard of the connected terminal guarantees a fault-less operation also for untrained operators

Comment:

Ciphering equipment needs always a keyboard and a connected printer for text input and output. This offers the opportunity not only to process messages by the input/output units but also to conduct a dialogue between man and machine. This means that the equipment offers the operator a corresponding "menu" in his national language via printer. He then chooses the desired function via the keyboard.

Example for a "menu":

c: cipher mode
d: decipher mode
t: test mode

For a better comprehension, please read this print-out like this:

Press the key "c", if you want to cipher
Press the key "d", if you want to decipher
Press the key "t", if you want to test

Please take detailed informations thereto from the general page (4. inner side) of the catalogue "ME 640" - title: "Example of a dialogue".

Instructions guide so the operator in logical steps throughout his entire work. The well-contrived program not only warns the operator of missing or incorrect inputs but also tells him what to do next in each case in comprehensive instructions.

Since this dialogue has modular software it can be easily adapted to special customer requirements. It is designed to be quickly and inexpensively modified to be suitable for the most diverse applications.

This kind of dialogue-controlled operation has the following two advantages compaired with a conventional operation panel with a lot of switches and indicating lamps:

- An operation manual and the studying of that are completely unnecessary and even operators, who are using the cipher machine only sporadically, will not have any problems with the handling.

- After half an hour of training, we can guarantee a faultless operating of the machine.

Naturally, our cipher machines write and cipher in any language (even in arabic or cyrillic characters) and are compatible with the telegraph norm CCITT 2.

2.5.7 Buffer operation of the memory in case of mains breakdown (option): ul. 20.10.87

Built-in, rechargable batteries and special integrated circuits supply the plaintext memory and the ciphertext memory at mains breakdown for at least 48 hours with the necessary voltage in order to keep the actual content of the memory (inserted message).

By inputting the combination "eee", however, the content of the memory will be erased.

In case, the mains fail just during a text is inputted, also the concerning memory address at which the breakdown has happened is stored automatically. After mains are coming back, the last inputted text line will be printed out automatically. Like this, the operator can continue to work exactly at this point where he has been interrupted before.

2.5.8 Maintenance free

2.5.9 Operational speed:

Depending the connected peripherals the "ME 640" can work up to 9600 Bd

2.5:10 Authorisation of the operator:

After switching on the machine or alternatively before selecting any new operation function, the operator has to proof the machine his authorisation of use.

This is made by inserting the right authorisation-code, which can be choosen by the user from 65.536 different possibilities.

2.5.11 Tape identification header

Depending of the correspondence code of the random key tape used for the encryption process each message gets a perforated identification header which is legible visible.

How this is executed can be seen in the example which is attached as appendix A.

- Tape 1 shows the text: MILS ELEKTRONIK
- Tape 2 shows the alphabet from A to N
- Tape 3 shows the alphabet from O to Z
- Tape 4 shows numbers from 0 to 9
- Tape 5 shows a ciphered message with a perforated identification header (with text: TO VIENNA)

Normally the cipher department delivers the encrypted message to be transmitted from the on-line operator.

To put the on-line operator in the position to separate the individual, encrypted tapes depending their destination to where they have to be transmitted all of the tapes can have such a preamble.

The application of this feature is mainly to simplify the "in-house-organisation" between cipher department and the communication headquarter:

- so the tape identification header could show the name of the city where the Embassy is situated to which the message should be transmitted

- or it could show directly the telex number which has to be dialed from the on-line operator to reach the receiver.

To allow the maximal flexibility the customer can program this preamle by himself just by writing the required text once via the keyboard. It is then memorized until it is erased or amended. Depending the number of destinations required the maximal length of the preamble is calculated automatically (i.e. for 75 destinations each preamble can have up to 20 characters).

2.5.12 Function "best selection"

As known, especially garbled, encrypted messages require from the operator sometimes very time-consuming processes in order to decipher the message again.

If a message consists of a longer text and the transmission errors are distributed over the entire message it is sometimes very difficult to get back the plain text.

Only a retransmission of the same message will principally not solve this problem, because there will be other garbles, although on other positions within the message.

However, here our feature "best selection" starts: both of the received, but varying garbled messages will be entered into our cipher machine "ME 640". It calculates out of both of the two garbled messages a good third one which will be finally deciphered.

This best selection is executed full automatically and delays the decipher process only for the time needed to enter the second punch tape - and this requires just 1 minute per 800 characters.

2.5.13 Priority of messages to be transmitted

In order to give telex messages a certain priority, to each message one of the three priority levels

1: normal
2: urgent
3: flash

can be added. As soon as the priority level is higher than "1" the concerning level "URGENT" or "FLASH" is perforated automatically into the punched tape in a legible visible way (like explained under position 2.5.11) and in addition to this the remark "URGENT" or "FLASH" will be printed as well on the top of the plain text as on the top of the enciphered message.

3. Cryptographic Specifications:

3.1 Cipher-Modes:

Cleartext (plaintext) can be enciphered either by an

3.1.1 external ONE TIME TAPE, generated for example with our random tape generator type "A6723" or type "ME 600" or with a

3.1.2 built-in, non linear, microprocessor-controlled, electronic key generator, which has the following datas about its cryptovariables:

-- Three levels of cryptovariables:

= LONG TERM KEY, consisting of

- a permutter key with the incredible large number of 8.6 x 10^{506} presettings

- an algorithm key with an additional number of 1.2 x 10^{24} presettings for telex applications and 3.4 x 10^{38} for ASCII applications

= SECRET KEY
with 7.9 x 10^{28} presettings

= MESSAGE KEY
with 1.1 x 10^{15} presettings for telex applications
and 1.2 x 10^{24} presettings for ASCII applications.

This message key is generated automatically and randomized to prevent reuse of key; one part of it is enciphered to conceal if from any eavesdropper.

Thus the key generator has a total possible presetting number of

8.9 x 10^{574} for telex and
2.7 x 10^{598} for ASCII.

-- Minimum cycle length of 1.7 x 10^{38}

-- Maximum cycle length of 4.1 x 10^{62}

-- Cascade of unbiased nonlinear combiners to produce outputs in order to control stepping of linear registers

-- Byte-oriented operations including the highly generalized and unstructured "table look-up" process

The "ME 640" cipher unit includes both possibilities in its standard version. The "ME 640" unit is crypto-compatible to equipment of all other manufacturers.

3.2 Automatic control of the inputted secret key in order to check the correct input:

A special program controls the input of the "secret key" and confirms the correct key setting.

Incorrect key settings are rejected and there is a corresponding comment printed via the teleprinter.

3.3 Automatic initialisation of the internal key generator at the receiver station, without any key input from the operator

3.4 Radiation:

The "ME 640" unit is equiped with measures to minimize any radiation.

3.5 Memory function:

Since in the "ME 640" unit the cleartext is stored in a memory it can be used several times to be enciphered. In doing so of course different codes, depending the destination can be used.

This function is especially usefull in large networks, which consist of several levels in order to transmit circular messages.

By pressing a certain key the memory can be erased.

3.6 Header function:

Introductory notes in plain language containing information to the addressee, such as sender, insertion marking, date, etc. can be preceeded to each ciphered message. After the "header-end-dedection" the encipher/decipher process is started automatically.

4. Electrical Specifications:

4.1 AC: 220 volt; +10%, -15%
110 volt; +10%, -15%
DC: on request

4.2 Option: Low Voltage Indicator
If supply voltage (DC or AC) reaches a certain critical limit, it is automatically indicated to the operator by an acustical and optical alarm. If the supply voltage gets under this critical value, however, all functions of the machine are blocked automatically. This ensures, that the equipment works correctly or not at all, in order to prevent from incorrect and undedected operations.

5. Mechanical Specifications:

Width	460 mm
Height	220 mm
Depth	320 mm
Weight	10,5 kg

6. Ambient Specifications:

6.1 Temperature

0° to 50° C
0° to 70° C storage

6.2 Humidity

10 % to 90 %
5 % to 95 % storage

6.3 Reliability

Meantime between falses: 10.000 hours

There is also a military version of the above specified equipment, called "ME 660". It is only 3 cm high and can be shifted directly under the already used teleprinter. The military version "ME 660" is displayed in the catalogue "MILS ELEKTRONIK" on the last inner page.

T. Hartmann
General Manager

Enclosures

- Catalogue ME 640
- Catalogue MILS ELEKTRONIK
- Automatic error correction
- Appendix "A"