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 pocket cipher machine "ME 540"

TABLE OF CONTENTS

Mils,

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 pocket cipher machine "ME 540"

1. Object:

The cipher unit "ME 540" serves for encryption and decryption of shorter messages. It can be operated as well off-line as on-line and is equipped - depending the option - with a printer and an acoustical coupler.

Via a special interface a teleprinter can be connected to the machine. So each teleprinter can be modified economically to a comfortable cipher station.

Naturally also peripheral machines with other interfaces can be adapted.

The transmission speed can be up to 9600 bit/sec. depending the peripheral unit respectively the transmission channel.

Rechargeable Ni-Cd-batteries offer up to 100 hours of non-interruped operation, depending the operation mode.

Via a plug the "ME 540" can be supplied with DC-power also externally. Like this, the internal batteries are recharged.

2. Function specifications:

2.1 Text input via:

- the keyboard of the machine "ME 540", alternatively via the keyboard of a connected peripheral machine, i.e. a teleprinter
- the photoreader of an eventually connected peripheral machine, i.e. a teleprinter
- the acoustic coupler (modem, as plug-in module)

2.2 Text output via:

- the liquid crystal display of the "ME 540", alternatively via the page printer of the connected teleprinter
- the perforator of the connected teleprinter
- the acoustic coupler (modem, as plug-in module)
- the mini-printer (as plug-in module)

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

Dorfstrasse 20
A-6060 Mils i. T.
Phone (52 23) 77 10-0
Telex 533009 mils a
DVR 0421701

2.3 Output format:

2.3.1 If no peripheral unit (e.g. teleprinter) is connected to the "ME 540", the output of the ciphered message is displayed or printed automatically in groups of 5 characters with 5 groups per line and can consist of:

- 10 numbers (Modulo 10)
- 16 free choicable letters (Modulo 16)
- 26 letters (Modulo 26)

Typical print-out - via the miniprinter - of an enciphered message in modulo 16:

```
CIPHERTEXT:

FROM MILS TO LONDON

//// 333 111 ABXJJNT ABXJJNT ABXJJNT
AEKEC HCKFT KSBRJ KJYEA PBARY RAHTY KR

001    NPNPB PWAFS HENXE XAXBB YNBNR
002    KHBHR TWHHE YBBJT WXFAJ PNBCX
003    TBWFP RYABT CKRXY WPBYC FAFFS
004    KJWXB CAKKP RBXWY THWBK HBKFB
005    FWJKR NHRXK AFHBJ BSJSN WBBKS
006    PCKKR NTBSE PFCNR JJXNS NYJTJ
007    SEAPS CRWFT XCKBB ANTAA HJXSS
008    RYPFS ARKBT CCWNY TAPTT HFACS
009    AKPHE PCXKA TRCXT BSEXS AWCBC
010    XNRXP YAHJN EAPCK EWFCF WJBXT
011    XKPBF HRBAK SKCRK KNJCN XCHXC
012    RAPPK BXNRS EPFWS SHRBS PYXBP
013    YSFBW XWTPE FKNTY HTCRX RYKST
014    NBKCE ATNPH PYENX FXNTN CBNSW
015    PRYAJ WHETF FFBTA FRXRX SFRTY
016    FCHHE XTYBC ACXWH NFCSS APJBC
017    EWTAY CSSXY BJYBB SPJNR STTNP
018    TWBNC FTECN HTBYC SKESH CJWNC
019    FJBBA WYKHX APPAR RJRXC AHAFS
020    NCXRF TRRTX YYTWE FTSAF TTACP
021    FPBBF RNSTT CRSBS XCRFY WRFTC
022    PAPPY +++++

106 106 106
NNNN

----------
```

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

Dorfstrasse 20
A-6060 Mils i. T.
Phone (52 23) 77 10-0
Telex 533009 mils a
DVR 0421701

To check the already inputted text it is necessary that this text can be re-displayed at any time. In order to control this very easy there are 3 special functions:

- display the 1st text-line
- display the next text-line
- display the previous text-line

(further details see point 2.5.9, 2.5.10 and 2.5.11)

2.3.2 If a peripheral machine is connected to the "ME 540" the text-input and text-output is executed via the respective functional unit of this machine (keyboard, printer, i.e. teleprinter).

In such an operation mode the ciphered message can have any requested format and can consist 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 (e.g. 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 consist 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 (e.g. automatic start of the tape reader, where a prepared tape is inserted or automatic switching on or off of the perforator which represents a high operation comfort at mixed operation, i.e. sometimes clear, sometimes ciphered).

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

Dorfstrasse 20
A-6060 Mils i. T.
Phone (52 23) 77 10-0
Telex 533009 mils a
DVR 0421701

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" are suppressed and therefore, unintentional effects to the communication channel are eliminated.

2.4 Facilities of test:

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 of mal-function an error report is displayed, notifying the operator which module has to be replaced.

2.5 Particularities:

2.5.1 automatic 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 without aid of the operator. 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 synchronism of the ciphertext being received.

Under this option these kinds of transmission errors are corrected automatically in order to make sure the

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

Dorfstrasse 20
A-6060 Mils i. T.
Phone (52 23) 77 10-0
Telex 533009 mils a
DVR 0421701

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 memory function to re-use a once prepared message for several encipher processes to different addressees. Therefore, there are different memory-sections (cleartext memory, sending memory and receiving memory) with a total capacity of 8000 characters (further details see point 3.5).

2.5.3 header function (further details see point 3.6)

2.5.4 text editing to correct typing errors during text inputting

Naturally, text parts can be corrected also subsequently: characters can be inserted, changed or deleted.

2.5.5 dialog-controlled operator guidance

A well designed operator dialogue in any desired language (without additional costs) enables from the beginning a faultless operation of the "ME 540", even for untrained persons.

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. He then chooses the desired function via the keyboard.

MILS ELEKTRONIK
G.m.b.H. & Co. KG
Dorfstrasse 20
A-6060 Mils i. T.
Phone (52 23) 77 10-0
Telex 533009 mils a
DVR 0421701

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

Clear 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.

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 operation 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.

2.5.6 maintenance free

2.5.7 automatic calender

The date is put ahead automatically to the begin of the plain header.

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

Dorfstrasse 20
A-6060 Mils i. T.
Phone (52 23) 77 10-0
Telex 533009 mils a
DVR 0421701

With this feature the receiver knows always when the messages were prepared and can, independant of the time he received this message, evaluate how current the received message is.

2.5.8 programmable alarm clock

At a freely programmable time several different "alarms" can be inputted, which give an optical and acoustical reminding signal when reaching the time limit.

Comment:

This function has several possibilities of application and is especially interesting because of the following:

If a prepared message can be received by the receiving station only during a small period (time window), this period can be preprogrammed during preparing the message.

If this time is reached, an acoustical alarm reminds the operator and at the display the thereto memorized comment appears. Like this, it is impossible to forget such terms.

2.5.9 automatic line index

Each line of the enciphered message is numbered automatically with a continuous 3-digit line number.

At inputting of the enciphered message during the decipher process the operator has to start each line with the corresponding line number. Like this, the operator is supported optimally for a faultless input of the ciphered message.

In case of an erronous input an acoustical alarm points this out immediately and an error report at the display specifies the mistake he made.

Comment:

In case of vocal transmission of the encrypted messages (spelling via radio or telephone) it is sometimes very

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

Dorfstrasse 20
A-6060 Mils i. T.
Phone (52 23) 77 10-0
Telex 533009 mils a
DVR 0421701

difficult, that both parties stay in synchronism during the transmission of such an incoherent message.

The solution offered by MILS ELEKTRONIK eliminates such problems almost completely and allows additionally a directed and simple selecting of an individual line without repeating several groups of 5.

In case of extreme transmission conditions and the resulting bad intelligibility this line index can be used very helpfully in order to ask for retransmission of a cipher group which was not received correctly. Example: Retransmit group 2 of line 25.

2.5.10 automatic line search during cipher mode

After inputting this command and the concerning line number the requested line appears on the display.

Comment:

Sometimes, the receiving station may want to have a retransmission of certain characters, groups or lines for control. This feature allows to find the concerning text part, where he can execute in case of need the necessary corrections (see also point 2.5.4). A lengthy manual process is therefore unnecessary.

2.5.11 automatic file system

The "ME 540" can manage automatically up to 16 (on request up to 32) different files.

For a simple handling, the operator can give to each message different filenames, with which he can recall afterwards the stored message.

Comment:

In case the transmitting station can not reach the concerning receiving station to which the already prepared message should be transmitted (e.g. the transmission channel is not available), with conventional equipment there are only two unsatisfactory ways:

MILS ELEKTRONIK
G.m.b.H. & Co. KG
Dorfstrasse 20
A-6060 Mils i. T.
Phone (52 23) 77 10-0
Telex 533009 mils a
DVR 0421701

- to wait until the stored message can be transmitted and to block meanwhile the complete cipher unit

- to erase the stored message in order to use the equipment in the meantime for other ciphering processes

Not so with our "ME 540" unit. In case a message can not be transmitted the operator creates any name for it and stores it until it can be transmitted. Now, he can work in the usual way and in between he tries to build up the requested connection. As soon as this connection is established, he calls-up the requested message with the corresponding filename and transmits it.

2.5.12 calculating function

Beside all other functions the "ME 540" unit allows also to use a calculator program with the 4 basic functions. On customer's request we can implement complete mathematical functions.

2.5.13 authorisation of the operator

After switching on the machine or alternatively before selecting any new operation function, the operator has to prove to 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.

3. Cryptographic specifications:

3.1 The encipher/decipher process is executed by an 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 incredibly large number of 8.6×10^{506}
      presettings

MILS ELEKTRONIK
G.m.b.H. & Co. KG
Dorfstrasse 20
A-6060 Mils i. T.
Phone (52 23) 77 10-0
Telex 533009 mils a
DVR 0421701

- an algorithm key
  with an additional number of 1.2×10^{24}

- SECRET KEY
  with additional 7.9×10^{28} presettings

- MESSAGE KEY
  with additional 1.1×10^{15} presettings
  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

8.9×10^{574}

- Minimum cycle length of 1.7×10^{38}
- Maximum cycle length of 4.1×10^{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

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 input of any key variables by the operator

3.4 The "ME 540" unit is equiped with measures to minimize any radiation.

3.5 Memory function

Since in the "ME 540" unit the cleartext is stored in

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

Dorfstrasse 20
A-6060 Mils i. T.
Phone (52 23) 77 10-0
Telex 533009 mils a
DVR 0421701

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 an "emergency key" the stored cleartext can be erased.

3.6 Header function

Introductory notes in plain language containing information to the addressee, such as sender and/or receiver of the message, 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 The "ME 540" unit works with a rechargeable battery pack, which is pluggable and can be replaced easely.

4.2 An external adapter supplies the equipment as well as recharges the battery pack.

4.3 Supply voltage is 9 VDC.

4.4 One set of batteries allows up to 100 hours of operation, depending the operation mode.

4.5 If supply voltage breaks down under a certain limit, an indication at the display informs the operator about this fact.

5. Mechanical specifications

Width	227 mm
Height	30 mm
Depth	95 mm
Weight	620 g

6. Ambient specifications:

6.1 Temperature

10° to 50° C; operation range
10° to 60° C; storage

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

Dorfstrasse 20
A-6060 Mils i. T.
Phone (52 23) 77 10-0
Telex 533009 mils a
DVR 0421701

6.2 Relative humidity, not condensing

10% to 90%; operation range
5% to 95%; storage

T. Hartmann
General Manager

Enclosures

- Copy to explain the efficiency of our automatic error correction
- Photo of the cipher machine "ME 540" in actual size

MILS ELEKTRONIK
G.m.b.H. & Co. KG
Dorfstrasse 20
A-6060 Mils i. T.
Phone (52 23) 77 10-0
Telex 533009 mils a
DVR 0421701

Efficiency of our automatic error correction

Original plaintext, like it was prepared
by the transmitter station:

the desire to protect communications against foreign,
unauthorized interception may well be as old as ability
itself to communicate. therefore, it is hardly surprising
that even in antiquity there were methods to keep
important, written messages from being generally intelligible.

++++

ciphertext, like it was transmitted:

//// 1 1111 3962 001 003 0077 213
rjttk tshxw kwkxr ynrjr cckpp yrrxc ktnae wraap chekw xwxsn
ckpww xbten ejkcx eypft xwswr sfnks ebsxc fxnbn bsajj jfsre
xeexr fkxyj ynsej ttebr abeaw yajkb csbef wscbe nsyty tyasa
kwfkt yahpj ebfyw eafpr xtctw anxfc xwwpf rkjfb penwh btcwj
acacb caws anjpj rxchj rrjtk wseby wneea twykw ecsey paxta
axcnt shefn xasph bthpp sywrh ewnsh cpwae ywssy wpcyj xybfp
ebjkr wxjss jwwbh chbnx bhakp ysxbn xhwxh bahkb hxcch nxxcc
ssehy xjjen rcxtf wxrpa ysrfe bwhba kcysf zzzz

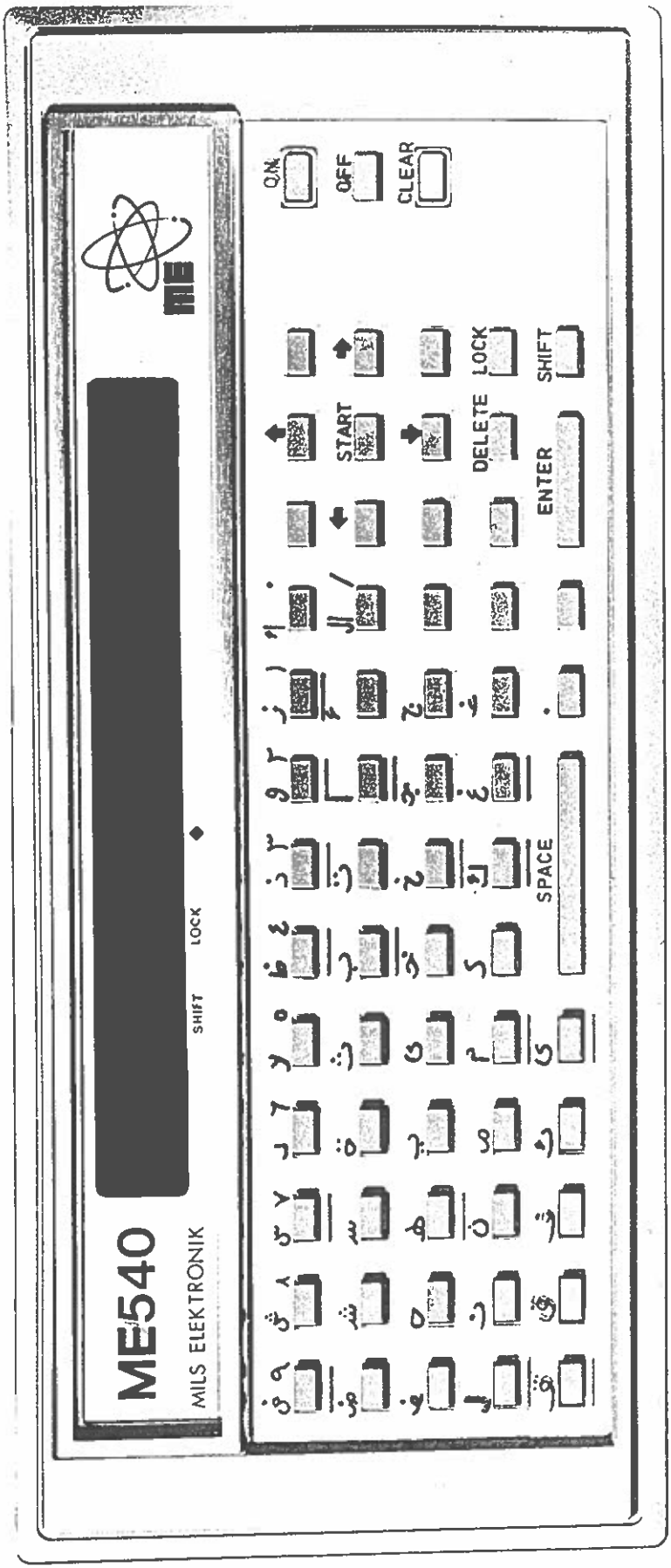
ciphertext, like it was received (garbled):

//// 1 1111 3962 001 003 0077 213
rjttk tshxw kwkxr ynrjr cckp yrrxc ktnae wraap chokw xwxsn
ckpww xbtmn ejkcx eypftxwswr sfnks ebsxc fxnbn bsajj jfsre
x exr fkxyjaynsej ttebr abeaw yajkb csbef wscbensyty tyasa
kwfkt yahpj ebfyw eafprw xtctw anxfc xwwpf rkjfb penwh btcwj
acacb caws anjpj rxchj rrjtk wseby wneeaa twykw ecsey paxta
axcnt sh fn xasph bthppsywh ewnsh cpwae ywssy wpcyj xybfp
ebjkr wxjs jwwbh chbnx bhakp ysxbn xhwxh bahkb hxcchg nxxcc
ssehy xjjen rcxtf wxrpa ysrf bwhba kcysf zzzz

decrypted plaintext, like it was reconstructed out of the
above garbled message by the receiver station:

the desire to protect communications against foreion,
unauthorized interception may well be as old as azility
itself to communicate. therefore, it is hardly surprising
that even in antiquity there were menyods to keep
important, written messages from being generally intelligible.
=
++++++

Actual size of Pocket Cipher
Machine "ME 540"



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

Dorfstrasse 20
A-6060 Mils i. T.
Phone (52 23) 77 10-0
Telex 533009 mils a
DVR 0421701