
LET
ON
OFF
ENC
DEC
GRETACODER 906
OPERATING MANUAL
1 2 3 4 5 6 7 8 9 Ø
Q W E R T Y U I O P
? + − = ( )
A S D F G H J K L DEL
. , : ' /
CHS Z X C V B N M CR/LF CONT
FIG KEY INP SPACE EDIT E/D LET

TABLE OF CONTENTS

1. GENERAL INFORMATION

1.1. Introduction

The GRETACODER 906 is a microprocessor controlled off-line pocket cipher unit with the cryptological strength and many of the operational features of a large cipher system. It is compatible with other GRETACODER text encryption systems and offers therefore the possibility to operate this unit as a portable external station.
An alphanumeric typewriter-like keyboard, a text memory for 719 characters, an editing capability of the complete text in memory, and a liquid cristal display (LCD) of 11 characters offer maximum comfort for the user.

1.2. Basic Operating Procedure

The cipher method used in the GRETACODER 906 follows the proven GRETAG-cryptology utilising the triple key system comprising

- Combiner Key
- Elementary Key
- Auxiliary Key

The Combiner Key is stored in a EPROM and may be unplugged easily. The Elementary Key may be stored in the unit or keyed in at the beginning as desired. The Auxiliary Key is generated automatically by a built-in random generator.

The basic procedure to operate the GRETACODER 906 is as follows:
After Elementary Key entry the source text is keyed in and stored in memory. Then, in the editing mode, the text is checked and can be corrected as required. Finally, the stored text is enciphered or deciphered and displayed in blocks of two five-letter groups or plain text respectively.

Example:

- Plain text: "PLEASE SEND IMMEDIATELY 250 NEW . . ."

- Cryptogram:

QWYTP AMOSJ	Auxiliary Key
IJBMD DKLNK	Cipher text
: :	
CEFDL AAAZO	
QWYTP AMOSJ	Auxiliary Key
QWYTP AMOSJ	Auxiliary Key

An incorrectly received cryptogram letter causes 1 – 4 wrong plain text characters. There is no error propagation, i.e. a transmission error does not affect the rest of the message.

1. GENERAL INFORMATION

1.3. Key Elements

1. The Combiner Key

is stored in a plug-in module at the bottom of the GRETACODER 906. This secret key may be changed by inserting a new module. The modules have to be programmed by the programming unit GKG 1.

2. The Elementary Key

consists of an arbitrary combination of 16 letters from A to Z to be entered via keyboard.

The secret Elementary Key remains stored when the unit is switched off unless it is not erased manually. Should the Elementary Key be erased, each time power is switched off, an internal setting must be changed (see "TECHNICAL DATA").

After switching on the GRETACODER 906, the display shows:

```
*KEY STORED
```

or

```
KEY
*KEY ERASED
```

depending on the Elementary Key-status.

Once the Elementary Key is stored, it is impossible to print out or display this Elementary Key.

3. The Auxiliary Key

consists of a combination of 10 letters from A to Y.

It is automatically generated at random for each enciphering procedure.

The Auxiliary Key acts as a modifier key and ensures that every message is enciphered with another ciphering program.

1.4. Security Precautions

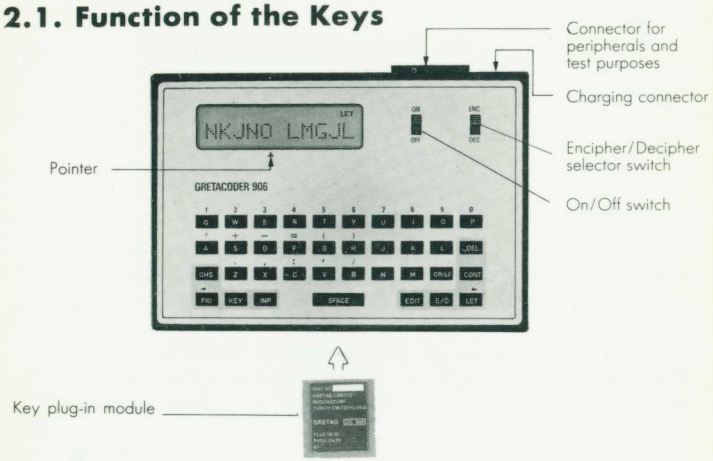
The high crypological security level of the hardware together with observation of the following security-rules give an optimal protection for your messages.

Security rules:

- The Elementary Key is a secret element and records of it have to be treated accordingly. Never note down the Elementary Key on the same sheet which contains source text.
- Never write plain and cipher text on the same sheet.
- If the GRETACODER 906 has to be left unattended the key plug-in module should be pulled out and kept in a secure place. Switch the unit off for this procedure.
- To enable correction of the Auxiliary Key in the event of transmission errors, repeat the Auxiliary Key twice at the end of the cryptogram.

2. KEYBOARD AND DISPLAY

2.1. Function of the Keys



CHS «Change sign»: Shifts from LET to FIG mode when deciphering

← **FIG** Shift from letter to figure or text shift to the left

KEY For entering the Elementary Key (Erases the stored Elementary Key)

INP «Input»: Clears memory and initiates the GRETACODER 906 be-fore source text input

EDIT Recalls text from memory and allows easy editing of text

E/D «Encipher/Decipher»: Starts operations according to position of switch ENC/DEC

→ **LET** Shift from figure to letter or text shift to the right

CR/LF «Carriage return/Line feed»: Display: €:

CONT «Continue»: For texts that exceed memory capacity or text addenda with the same Auxiliary Key

DEL
- Deletes last entered character
- Ends Edit modes «insert» and «iumd»

2.2. Explanation of the Display

Length of display: 11 characters
Above the text display the operating mode is indicated by the following abbreviations:

EDIT	The plain text or the cipher text can be changed or corrected
EDIT ■	Insert or jump mode
MEM	Text memory exceeded
KEY	Appears during input of the Elementary Key
BAT	Battery voltage too low
FIG	Keyboard is active for figures
LET	Keyboard is active for letters (normal operating mode)
▲	Characters are inserted or deleted in the editing mode at the position of this pointer.

Standard displays:

*KEY STORED	Elementary Key already entered
KEY *KEY ERASED	Ready for Elementary Key input
*** READY	Stand-by position
*** END ENC	End of enciphering operation
*** END DEC	End of deciphering operation

3. ENCIPHERING

3.1. Preparation and Entering the Elementary Key

1. Insert the key plug-in module. (Switch the unit off for this procedure.)
2. Set switch to «ON»
3. Display: `*KEY STORED`

   If "KEY STORED" is displayed and a new Elementary Key has to be entered

   press [KEY]

   and continue at point 4. If the already stored Elementary Key has to be used proceed according to chapter 3.2, point 8.

4. Display: `KEY *KEY ERASED`
5. Enter the 16 letters of the Elementary Key.
6. During the entry of the Elementary Key letters can be deleted by pressing

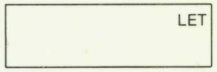
   key [DEL]

7. Enter a 17th letter and the Elementary Key is stored.

   Display: `*KEY STORED`

3.2. Entering the Plain Text

8. Press [INP] Display:



The GRETACODER 906 is ready for the input of plain text now. The symbol LET indicates that the unit is in the «letter shift».

Message: "Please send immediately 250 new . . ."

9. Enter the text character by character. Every character is immediately displayed. Errors can be deleted by pressing

   key [DEL] (deletes the last character)

   or [INP] (deletes the whole text).

10. For entering figures

    press [FIG]

    Then the unit is in the «figure shift» Display:

11. Enter figures and

    press [LET] Display:

12. Enter remaining text. If the memory is full, the sign MEM appears and new letters are not accepted. Proceed according to chapter 3.4.

13. Your message is stored in an internal memory now. This text can be reviewed and edited by following the instructions under chapter 5 «EDITING» or it can be enciphered directly according to chapter 3.3.

3.3. Enciphering Operation

14. Set ENC/DEC selector switch to «ENC»

15. Press [E/D] until
    Auxiliary Key is displayed e.g. `SAJUN YPPLQ`

    Repeted pressing of the E/D key may be necessary when enciphering very short messages or after editing.

16. Write down the Auxiliary Key. It forms the first two five-letter groups of your cryptogram.

17. Press [←FIG] and the next two five-letter groups are displayed. Write down the groups.

    Display: e.g. `NHBOK LOEDH`

18. Repeat until display shows: `*** END ENC`

19. Press [←FIG] again and the unit is reset to stand-by position. Reviewing is no longer possible.

    Display: `*** READY`

20. Add the Auxiliary Key twice at the end of your written cryptogram now.

Note: During the enciphering operation it is possible to review the previously displayed two five-letter groups. The Auxiliary Key cannot be displayed again.

Press [LET] and cipher text moves one display length (two if reviewing starts from position*** END ENC) to the right.

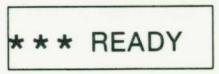
3.4. Special Procedures

Long messages

These are messages exceeding the capacity of the memory.

1. Enter the plain text following standard procedure (chapter 3.1 and 3.2) until input of characters is no longer possible and the display shows:

2. Now encipher the text according to chapter 3.3 point 14 to 19.
3. When display shows:



   then
4. Press [CONT], whereupon the display shows:

The unit is in Input-mode again and the rest of the source text can be entered.

Note: Having pressed the CONT-key the memory is cleared

5. Encipher according to chapter 3.3.
   The CONT-key makes sure that the second part of the message is enciphered with the same Auxiliary Key as for the first part.

6. Repeat this procedure if the rest of the text still exceeds memory capacity.

7. Add the Auxiliary Key twice at the end of your written cryptogram.

Enciphering the same (or a modified) message with a new Elementary Key.

1. Enter a message and encipher it according to chapter 3.1, 3.2 and 3.3.
   Display: `*** READY`

2. Press [KEY] Display: `KEY`
   `* KEY ERASED`

3. Enter new Elementary Key according to chapter 3.1. Then the display shows:
   `* KEY STORED`

4. Press [EDIT]
   The beginning of the message appears.

5. Edit the message if necessary (see chapter 5.)

6. Encipher the message according to chapter 3.3.

4. DECIPHERING

4.1. Preparation and Entering the Elementary Key

1. Follow the same procedure as described under chapter 3.1. until display shows:

* KEY STORED

4.2. Entering the Cryptogram

2. Check the three Auxiliary Key's of the cryptogram
   Due to transmission errors they may be different.

   Example of cryptogram:

SAJ**D**N YPPLQ	1st Auxiliary Key
NBHKO LOEDH	Cipher text
: :	
LIDNJ BFBIE	
SAJUN YPPLQ	2nd Auxiliary Key
SAJUN YPPL**C**	3rd Auxiliary Key

   The letters that occur twice are considered to be correct.
   The correct Auxiliary Key of the example reads as follows: SAJUN YPPLQ

3. Press [INP] Display:

LET

   The GRETACODER 906 is ready for entering the cryptogram now.

4. Enter the correct Auxiliary Key

   Press [SPACE] between the groups

5. Enter cipher text in 5-letter groups

6. Corrections:

   Press [DEL] to delete the last entered letter

   Press [INP] to erase the entire text in memory

7. Do not enter the last two Auxiliary Key's.

8. If the memory is full, the sign MEM appears and new letters are not accepted. Proceed according to chapter 4.4.

9. The cryptogram is stored now. It can be reviewed and edited according to the instructions of chapter 5 «EDITING» or it can be deciphered directly following chapter 4.3.

4.3. Deciphering Operation

10. Set ENC/DEC selector switch to «DEC»

11. Press [E/D] The first 11 plain text characters are displayed:

    PLEASE SEND

12. Write down text if required

13. Press [←FIG] , 11 further characters are displayed:

    IMMEDIATEL

14. Press [←FIG] until display shows:

    *** END DEC

    End of deciphering process, plain text is complete.
    If text is not legible see ''Special Procedures'', chapter 4.4.

15. During the deciphering operation it is possible to review the previously displayed text.

    Press [→LET] and plain text moves one display length (two if reviewing starts from position * * * END DEC) to the right.

16. Press [←FIG] again to reset the unit to stand-by position

    Display: *** READY

4.4. Special Procedures

Long messages

These are messages exceeding the capacity of the memory. The procedure is similar to the enciphering of long messages.

1. Enter the cryptogram until MEM appears on the display.
2. Decipher the cryptogram according to chapter 4.3.
3. When display shows `*** READY`
   then
4. Press [CONT] and enter the rest of the cryptogram.
5. Decipher the rest of the cryptogram.
6. Repeat this procedure if the rest of the cryptogram still exceeds memory capacity.

Message can not be deciphered

Elementary Key may be wrong:

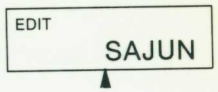
1. Press [KEY]
2. Enter Elementary Key (see chapter 3.1.)

   Display: `*KEY STORED`
3. Press [EDIT]
4. Press [E/D] Plain text should be legible now.

Auxiliary Key may be wrong:

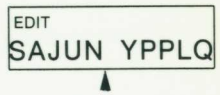
1. Press [EDIT]

   Display shows the first five-letter group of the Auxiliary Key



2. Press [←FIG] 5 times

   Display shows the entire Auxiliary Key:



3. If necessary correct the Auxiliary Key following the instructions in chapter 5 «EDITING».

Text consists of signs instead of letters:

A wrong cipher text character may result in a letter/figure shift in the plain text. The plain text then will consist of figures and symbols instead of letters or vice versa.
As soon as this occurs during deciphering:

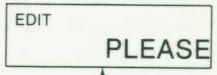
1. Press [CHS] The plain text shifts from letter to figure mode or vice versa. If the error was due to this shift, text is legible now.

5. EDITING PLAIN TEXT OR CRYPTOGRAMS

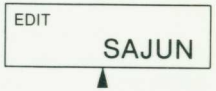
This mode allows to recall a text from the internal memory and to review and alter it. Editing operations can be executed during input or encipher or decipher operation or after having entered a plain or cipher text.

1. Press [EDIT] The beginning of the stored text is displayed.

Display if plain text entered:



Display if cryptogram entered:



2. The GRETACODER 906 is in the EDIT mode now and some keys of the keyboard have special editing functions.

5.1. Editing Functions

Press key	The following function is executed:
← [FIG]	Text moves one step to the left
→ [LET]	Text moves one step to the right

[B] The beginning of the text is displayed

[E] The end of the text is displayed

[J] Jump mode. The symbol ■ appears

Display:

[←FIG] Text moves batchwise to the left

[→LET] Text moves batchwise to the right

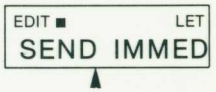
End «Jump mode» by pressing SPACE or A, B, E, I, or E/D with simultaneous execution of the corresponding command.

[D] Drop. The first character to the right of the pointer is deleted. Text moves to the left.

After pressing «D»

[I] Insert mode. The symbol ■ appears and unit is set to letter mode

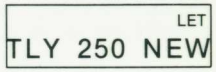
Display:



Any text may be entered at the pointer position now. The existing text on the left side of the pointer moves one step to the left.
The insert mode must be terminated by pressing

[DEL] after the insertion.

[A] Append mode. The unit jumps back from EDIT mode to input mode. The symbol EDIT disappears and the end of the previously entered text appears on the display:



The unit is in letter shift again.

After correction of the text

key [E/D] is to be pressed again, if necessary several times. A new cipher process is started with a new Auxiliary Key.

This also applies for reviewing the text without any modifications.

6. TECHNICAL DATA

6.1. Specifications

Dimensions:	185 x 130 x 30 mm (L x D x H)
Weight:	600 g
Temperature range:	Operating: 0°C to + 50°C Storage: – 15°C to + 70°C
Batteries:	4 x 1.2 V, size AA (UM 3) Ni Cd — low battery indication via display. With fully charged batteries it is possible to operate the GRETACODER 906 for about 36 hours.
Battery charger:	110/220 VAC 50/60 Hz
Keyboard:	— alphanumeric keyboard with 28 keys — 9 control keys
Display:	Liquid cristal display (LCD) for 11 characters in 5 x 7 dot matrix plus 7 control indicators
Text memory:	719 characters
Editing commands:	— character shift/insert/delete — block shift
Cryptology:	highest security nonlinear cipher generator
Combiner Key (secret):	— stored in pluggable EPROM — key diversity: 10^{38}

Elementary Key (secret):	— 16 letters — key diversity: 10^{22}
Auxiliary Key (non secret):	— automatically and randomly generated — 10 letters — key diversity: 10^{14}
Keystream period:	10^{54} characters
Recursion length:	10^{9} characters
Cipher text:	Groups of 5 letters A - P
Compatibility:	The following GRETACODER can be programmed to use the same cipher law as the GRETACODER 906 does: GRETACODER 505, on-line/off-line telex encryption unit GRETACODER 805, off-line encryption unit SP 300 GCA, cipher teleprinter

6.2. Accessories

	Part No
Battery charger	40.79.21
Bag for charger	40.79.29
Key plug-in module	40.79.00
Leather bag for unit	40.79.20
Operating manual	98.10.39
NiCd battery (4 needed)	13.09.03
Military metal case	40.79.23
GRETAG Key Generator GKG1	40.73.61

6.3. Maintenance

The GRETACODER 906 is a fully solid state unit and requires no periodic maintenance, but the built-in batteries have to be kept in a charged state.
With fully charged batteries it is possible to operate the GRETACODER 906 for about 36 hours.

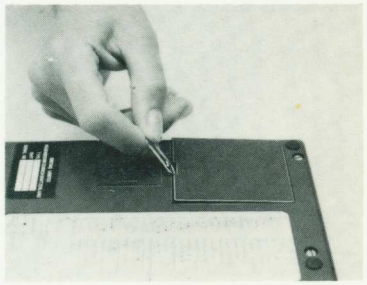
Recharging of batteries:

Connect the unit to the supplied battery charger for about 24 hours. Operate the unit with the battery charger connected whenever this is possible. An overcharging is impossible. Use only the supplied charging device, otherwise the GRETACODER 906 may be damaged.

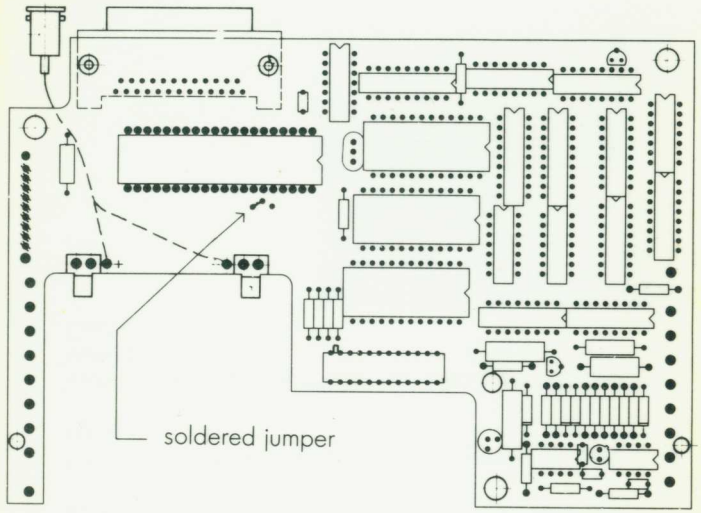
Replacement of batteries:

Open the battery cover carefully, proceed according to figure.

Insert nickel-cadmium (NiCd) batteries type NCC50CF,
Voltage 1.2 V
Capacity 0,5 Ah.

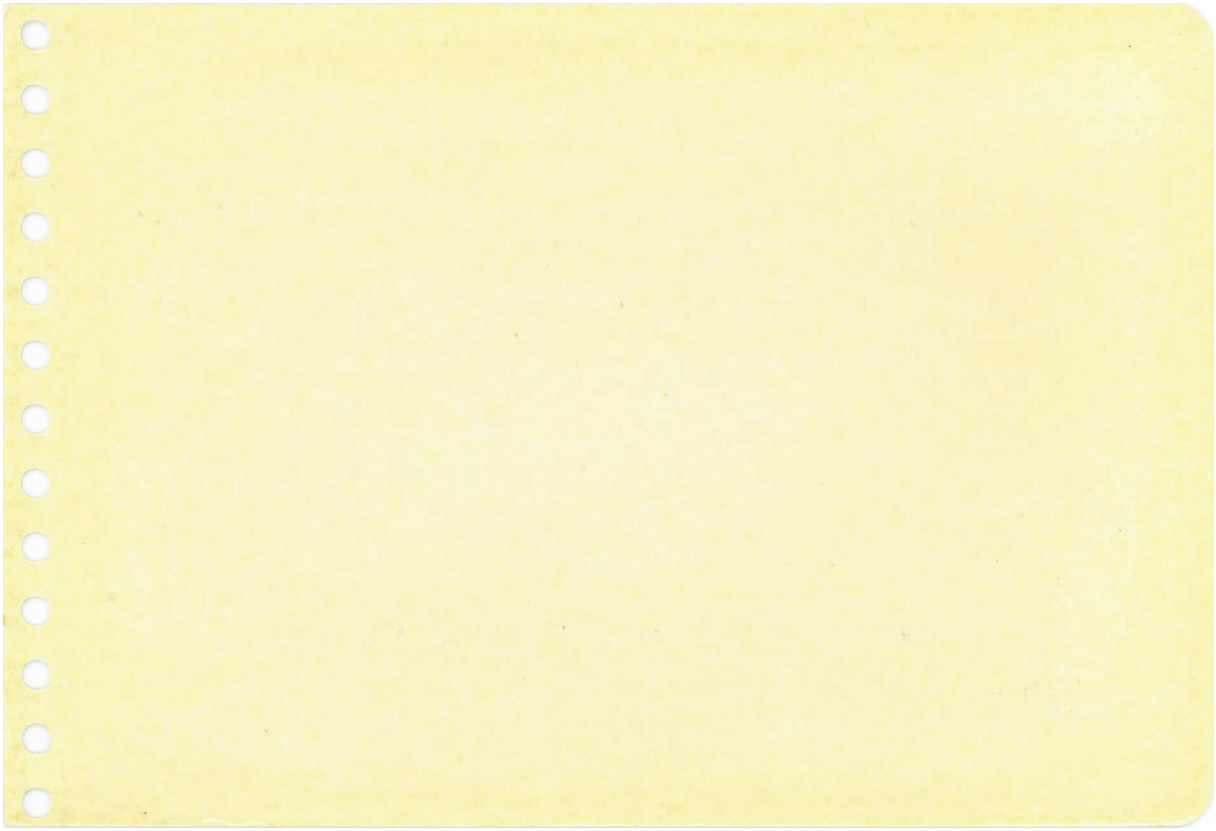


Position of internal soldered jumper



In this position the Elementary Key remains stored when the unit is switched off (factory setting).

If the jumper is set to this position (to be performed by trained personnel only) the Elementary Key is erased by switching the unit off.



GRETAG COMMUNICATIONS SECURITY

GRETAG Limited
Althardstrasse 70 CH-8105 Regensdorf/Zürich, Switzerland, Telephone (01) 842 11 11, Telex 53950

GRETAG 98.10.39 BA 8109 E Printed in Switzerland