

SECRET

207

THE NETHERLANDS GOVERNMENT

DESCRIPTION
of the
ECOLEX MARK I AND II

Edited by the Netherlands Government

OCTOBER 1ST, 1954

POSTAL ADDRESS: WU/NATO CYPHER EXECUTIVE - 155A BADHUISWEG

THE HAGUE - THE NETHERLANDS

SECRET

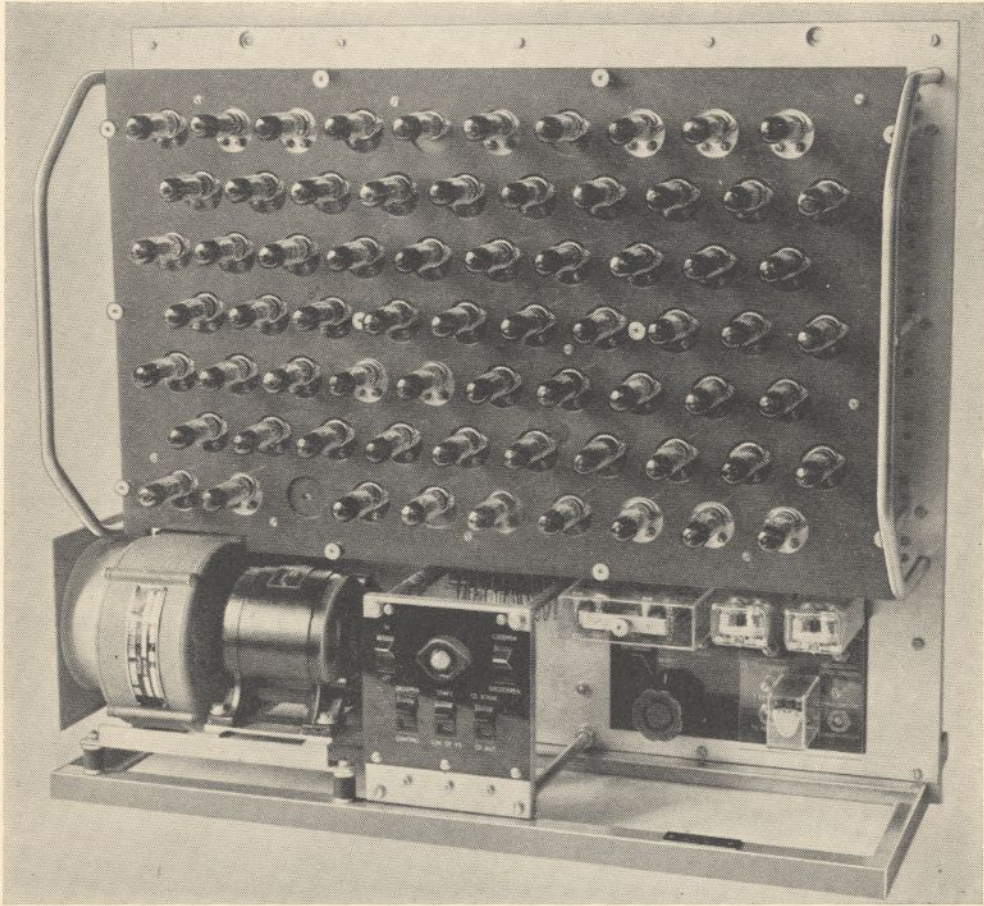
6

THE NETHERLANDS GOVERNMENT

DESCRIPTION

of the

ECOLEX MARK I AND II



Inside view of the ECOLEX Mark I

INTRODUCTION

The Laboratories of the Netherlands Government at The Hague have worked for nine years now on the development of a cryptographic equipment, based on the 'one-time-pad' system. The first type was a cryptographic apparatus with electro-mechanical switching means (relays), with which considerable experience was gained over a period of six years. The need that was felt for an equipment operating at higher speeds, was the reason why in 1949 a start was made to develop a cryptographic equipment capable of carrying out the enciphering and deciphering electronically and at the normal teleprinter speed of 400 letters per minute, whilst, at the same time, the crypto text might be transmitted as well as received direct via a normal teleprinter line.

It was considered very important to find a possibility to establish crypto channels between two correspondents in such way as to enable, at one end, the enciphering and deciphering to be carried out electronically, whereas, at the other end, these operations could be carried out by hand. In this way an office handling a few messages would not be forced to purchase expensive equipment. This last consideration meant the use of the 26 letters of the alphabet in the crypto text, as otherwise the cryptograms could not be transmitted via the public telegraph services and the morse-system. In addition the possibility was considered, however, to establish crypto traffic over so-called 'point-to-point' channels of normal teleprinter lines. The exterior form of the crypto message is, for such communications, of secondary importance, so that use might be made of the 32 symbols of the telegraphic alphabet.

The experience gained and the considerations described above have resulted in the development of two apparatus which meet the practical as well as the cryptographic requirements.

ECOLEX MARK I

The Ecolex Mark I (*Electronic, COde, teLEX*) is a crypto apparatus which, operating with a 26 letter system, enciphers a plain text with the aid of a key text into a crypto text and conversely deciphers a crypto text with the aid of a key text into the original plain text. The Ecolex Mark I can be used 'on-line' as well as 'off-line'; in both cases ordinary teleprinters can be used. Since it is necessary to enable the 'space' to be enciphered from the plain text, the K (French, Italian, Spanish), X (Dutch) or Z (English) have, according to the language used, been replaced by the 'space' symbol, so that, consequently, the plain text message may contain 25 letters of the alphabet and the 'space' symbol. The enciphering may be carried out in 'groups' as well as in 'continuous sequences'; in the former case the outward form of the cryptogram is then determined by the shape of the key tape. If, for instance, a key tape is used with 10 groups of 5 letters on a line and with a space of two lines between the lines, the crypto text will then show the same outward form.]

The enciphering in groups should be carried out with two tapes (one tape containing the plain text message and one tape containing the key text). The crypto text can be transmitted at once and direct by the apparatus itself via a teleprinter line (fig 1a).

The crypto text may, if necessary, be obtained in the form of a perforated tape, which can be used for possible later telegraphic transmissions to one or more correspondents (fig 1b).

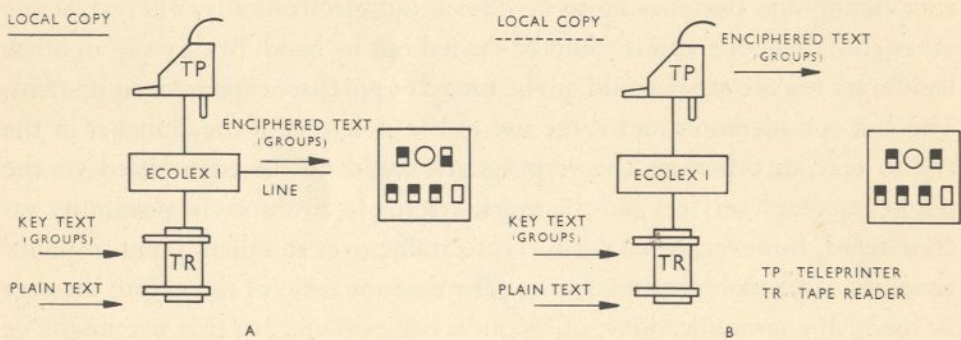


Fig 1. Enciphering of a plain text with a key text in groups.
 a. Ecolex Mark I connected to teleprinter line.
 b. Ecolex Mark I connected as local ciphering unit.

For deciphering one may start from a teleprinter line direct (fig 2a) as well as from a received crypto tape (fig 2b) in which case the deciphered text is printed on a teleprinter in the form of 50 letters on a line (including spaces).

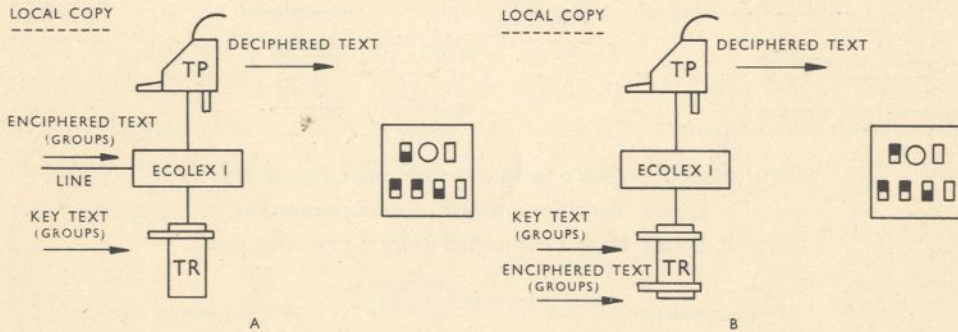


Fig 2. Deciphering of an enciphered text in groups.
 a. Ecolex Mark I connected to teleprinter line.
 b. Ecolex Mark I connected as local ciphering unit.

The synchronization of the perforated tapes prior to the enciphering and deciphering of the messages, takes place in a fully automatic way.

The crypto messages obtained in the way outlined above can be transmitted via the public telegraph services and the morse-system and may, if necessary, be deciphered by hand by correspondents who have a page-copy of the key text and the deciphering square available.

The Ecolex Mark I is also capable of operating in a 26 letter system with a 'continuous' key text. In this case the symbols 'carriage return', 'line feed' and 'letter-shift' are transferred, without being enciphered, from the plain text into the crypto text, the 'space' symbol, however, is actually enciphered.

The result of this is that the lengths of the lines in the crypto text are equal to those in the plain text. In deciphering the crypto text the symbols 'carriage return', 'line feed' and 'letter shift' are taken over again from the crypto text into the deciphered text, so that the form of the plain text has been retained. In order to camouflange in the crypto text short lines from the plain text these lines may be supplemented in the plain text by means of 'spaces' (fig 3a and b, fig 4a and b).

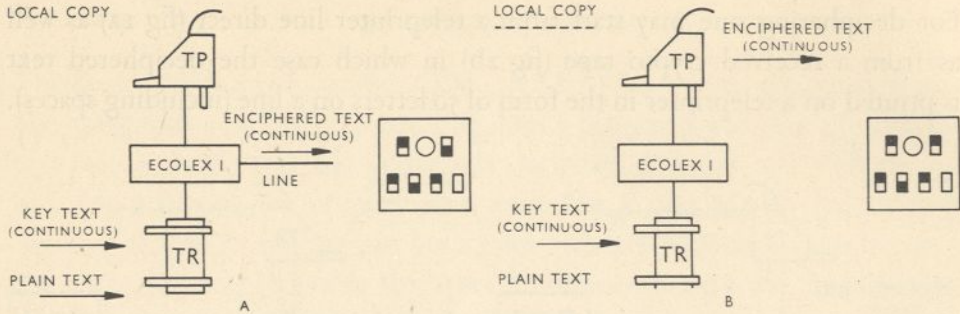


Fig 3. Enciphering of a plain text with a continuous key text.
 a. Ecolex Mark I connected to a teleprinter line.
 b. Ecolex Mark I connected as local ciphering unit.

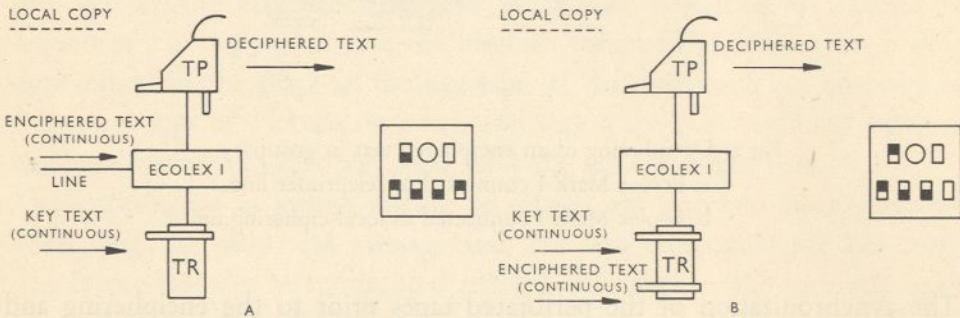


Fig 4. Deciphering of a continuous enciphered text.
 a. Ecolex Mark I connected to teleprinter line.
 b. Ecolex Mark I connected as local deciphering unit.

It is obvious that the division into paragraphs with possible indented lines including the formation of pages can be done without any adjustment. The plain text may, in case a continuous key text is used, be fed by using a perforated tape (fig 3a and b) as well as by using the keyboard of the teleprinter (fig 5).

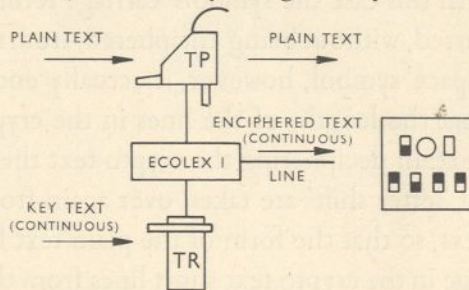


Fig 5. Enciphering of a plain text with a continuous key text using the keyboard of the teleprinter.

When use is made of a tape of the plain text an automatic transmitter may, if so desired, be inserted in order to reproduce the plain text on the teleprinter during the enciphering.

As described above when operating with a key text in groups, the Ecolex Mark I can also prepare a continuous crypto text in the form of a perforated tape, which can afterwards be sent to the correspondents.

Another special provision has been made which renders it possible to carry on, with the aid of a continuous key text, a during the transmission enciphered teleprinter conversation; in that case the apparatus switches automatically from transmitting to receiving and vice versa (fig 6).

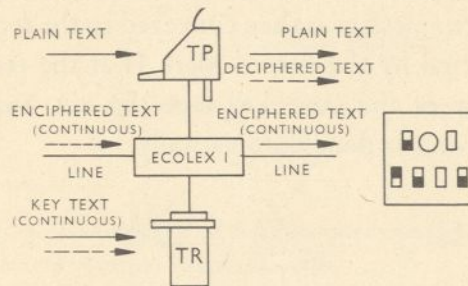


Fig 6. Enciphered conversation between two partners.

Both sending and receiving (dotted lines) conditions are shown in one diagram.

The apparatus is provided with a device against operational errors.

When the Ecolex Mark I is in the enciphering position it is not possible to transmit a plain text message without its being enciphered.

The switchboard of the Ecolex Mark I containing 6 two-position switches is shown in each of the preceding figures and in detail in fig 7.

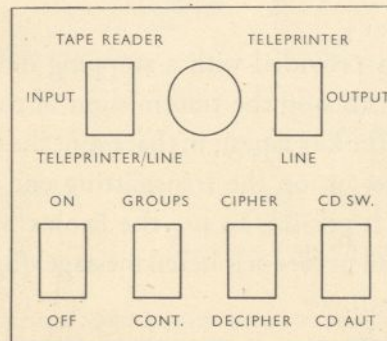


Fig 7. Switchboard of the Ecolex Mark I.

ECOLEX MARK II

The Ecolex Mark II has been mainly developed to be used in the case of 'point-to-point' teleprinter connections. Unlike the Ecolex Mark I, the Ecolex Mark II system is based on the 32 symbols of the telegraph alphabet, as in the case of point to point connections the outward form of the crypto message is of minor importance.

The key tape to be used in this case contains all 32 symbols. This has made it possible to use all 32 symbols also in plain text messages. By means of a teleprinter or a tape reader the plain text is fed into the Ecolex Mark II (fig 8a and b). The apparatus is connected with the teleprinter line in the normal way. The crypto message is then conveyed to the receiving point along this line and deciphered by the Ecolex Mark II at the receiving end of the line, by using a copy of the same key tape (fig 8c). Switching over from transmitting to receiving is done automatically.

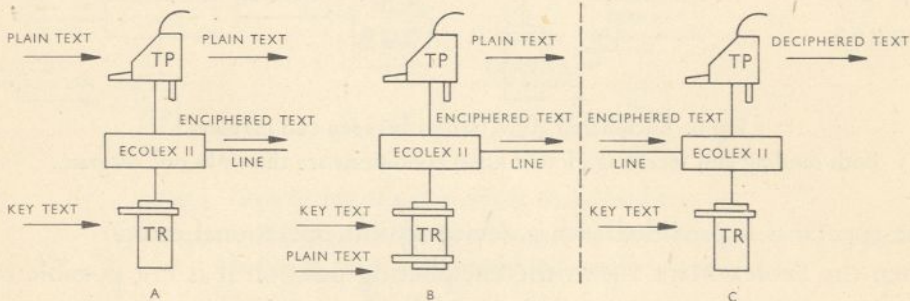


Fig 8. Enciphering and deciphering with the Ecolex Mark II.

- a. Plain text on keyboard
 b. Plain text in perforated tape } enciphering.
 c. Enciphered text incoming from line on receiving end.

The apparatus has been provided with a stopping device which enables the receiving correspondent to stop the transmission of the message (e.g. in case of desynchronization of the key tapes); in that event the transmission is stopped and an alarm lamp lights up on the transmitting end of the line.

By means of a switch it is possible to use the Ecolex Mark II connection for plain text messages instead of for enciphered messages (fig 9a or 9b transmitting end, fig 9d receiving end).

For synchronization purposes it is possible to transmit the key tape (fig 9c transmitting end, fig 9d receiving end).

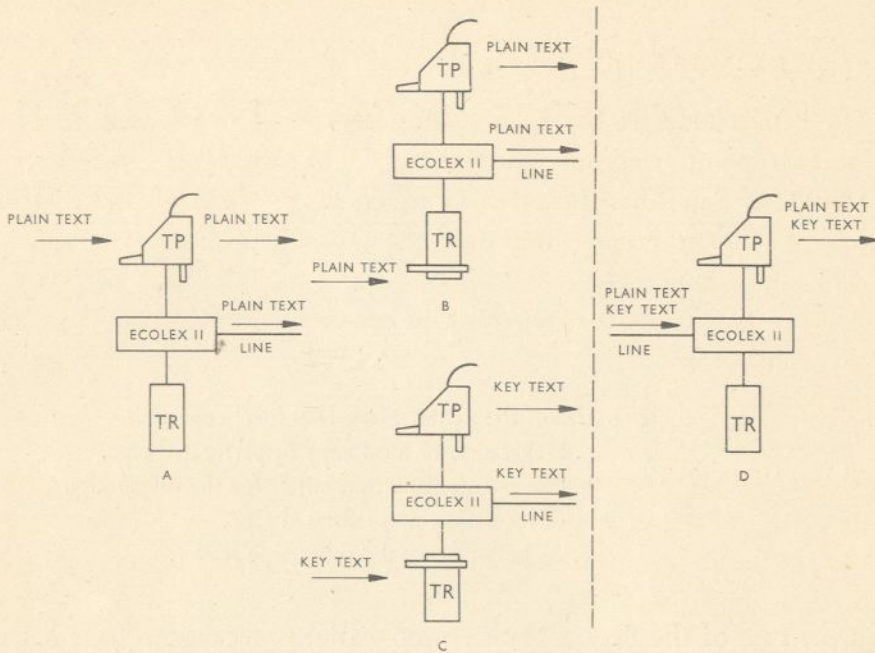


Fig 9. Transmission of non-encrypted messages.

- a. Text on keyboard
 b. Text in perforated tape
 c. Key text in perforated tape
 d. Receiving end.
- } transmitting end.

In special cases the Ecolex Mark II can be used as a local unit so that previous enciphering respectively subsequent deciphering is possible (fig 10a and b). The preparation of local copies or perforated tapes both from keyboard or tape reader also can be done (fig 11a, b and c).

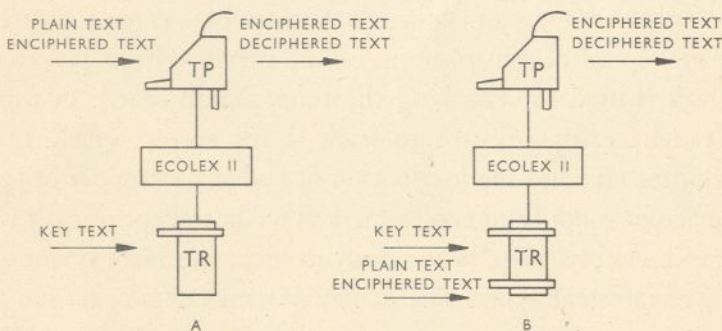


Fig 10. Use of Ecolex Mark II as local ciphering unit.

- a. Text on keyboard.
 b. Text in perforated tape.

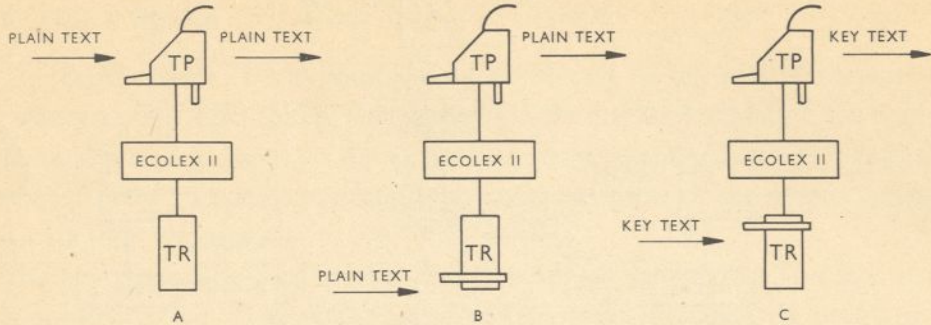


Fig 11. Use of the Ecolex Mark II as local copy unit.
 a. Preparation of local copy or perforated tape.
 b. Use as automatic transmitter for the preparation of local copy or perforated tape.
 c. As b, but using the other tape reader.

In the case of the Ecolex Mark II, too, various precautions have been taken in order to avoid errors in the operation of the cryptographic equipment. The Ecolex Mark II can cooperate with the Sigtot apparatus.

GENERAL OBSERVATIONS

The Ecolex Mark I and Ecolex Mark II can be connected to a mains of 110/127/220 volts 50/60 cycles. Voltage variations of + 15 to - 30% are allowed. The teleprinter speed of the apparatus can be switched from 45 $\frac{1}{2}$ to 50 Bauds. A tuning fork is used for checking the transmission speed. In this way the apparatus can be easily adjusted to work at the correct speed. In order to facilitate maintenance and the localisation of faults the number of component parts of the Ecolex Mark I and Ecolex Mark II has been kept as small as possible. The electronic circuits have been constructed in the form of plug-in units. There are five different types. The Ecolex Mark I contains 68 plug-in units, 68 double triodes and about 600 rectifier cells. The Ecolex Mark II contains 22 plug-in units, 22 double triodes and about 250 rectifier cells. In respect of both apparatus letters of patent have been applied for.