HAGELIN-CRYPTOS

SECRET

Cryptographic Data Sheet Typex Mark 22 (Short title - BID/08/2)

General Description

1 - The Typex Mark 22 is a modified version of the U.K. general purpose cypher machine the Typex Mark 2. It is an electro-mechanical off-line cypher machine power driven, keyboard operated with two printers, an output printer and a check printer.

The cryptographic element of the machine comprises:

a) A permuting reciprocal maze with five 26-point rotors and a pluggable reflector.

b) A pluggable stecker at the input/output of the maze.

Employment

2 - The Typex Mark 22 is used by all British Services for intra and inte service communications down to the following levels+

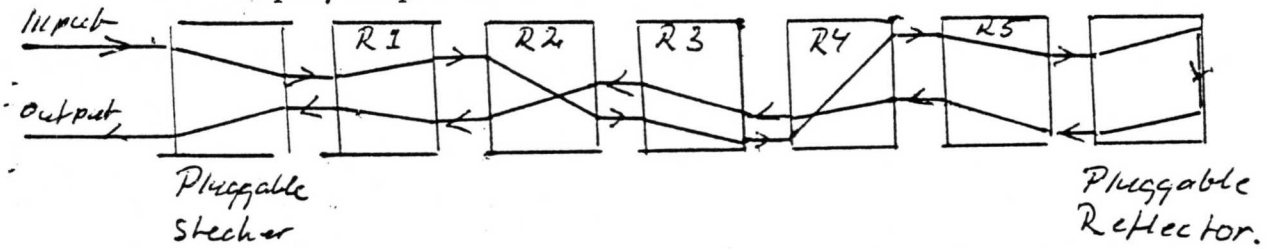
RN - down to destroyers

Army - down to Brigade H.Q.

R.A.F. - down to group H.Q.

Crypto-principle

3 - The cryptographic principle employed is a five rotor reciprocal permuting maze with a pluggable reflector and pluggable stecker at input/output end.



R1 and R5 stop each time befor encypherment
R2 steps when R1 is notched and/or R2 is notched
R3 steps when R2 is notched and/or R3 is notched
R4 steps when R3 is notched.

4 - Five hollow rotors are employed in the machine at any one time. Ea rotor consists of a housing with a rotatable alphabet tyre having nine turnover notches at the following points relative to the alph

A C E I N Q T V Y

For each machine setting the alphabet/notch tyre can be set at an the 26 possible angular positions relative to the rotor housing.

5 - In each hollow rotor is fitted an insert with scrambled wiring. The insert angular position is fixed in relation to the rotor housing but inserts may be fitted either in the straight or reversed position i.e. either side may be adjacent to the hollow rotor contacts. For any machine setting the five inserts are chosen from a set of fourteen inserts each differently wired and identified by the letters A-N.

Procedures

6 - Messages cyphered in Typex Mark 22 are limited to a maximum of 450 groups made up of three crypto-Sections none of which may exceed 150 groups. At the end of each crypto-section Rotor 1 is advanced one position by hand before proceeding with encypherment of the next crypto-Section. The group "22222" is inserted in the cypher text to indicate where this procedure has taken place.

7 - Bisection of messages is employed. Each message is bisected at a rand point before encypherment, the second part being encyphered first followed by the first part.

8 - Variable spacing is employed. The procedure followed is to encypher one, two or three spaces after each word in a random order so that in any one message each type of space is used approximately the same number of times.

9 - Message indicators are encyphered. Two message indicators are chosen random from a book of disguised indicators. The two disguised indicat are transmitted, the rotors are set to the true version of the first disguided indicator and the true version of the second disguised indicator is encyphered. The resultant five letter cryptogram is use as the true message. Where one message indicator book is used for encyphering messages on more than one key list the first disguised indicator may also be used as a system indicator.

Keying Materials

10- The Rotor Arrangement Key List contains the following information:

The first line (reading from left to right)	The position in which the inserts are to be placed in the scrambler unit for the day in question	E LR JR A FR (R = insert the reverse positio
The second line (reading from left to right)	The tyre settings to be on the hollow rotors in which the above inserts are fitted.	M J P I M

11 - The Crossover/Plugboard key contains settings for the pluggable reflector and stecker. It may be printed on the rotor arrangement key list. These settings may change daily or less often, not less than once every five days as may be directed.

The setting is in the form:

Crossover / Plugboard Key List		
Day	AB CD EF GH I	..... YZ
1	LF NT ZR VE 0	..... IB

Vertical pairs are used for the stecker setting, e.g. A connected to L, B to F etc.

Horizontal pairs in the lower, scrambled alphabet are used for the reflector setting e.g. L is connected to F, N to T etc.

12 - Disguised Indicators are contained in a messahe indicator book in the following form:

True Indicator	Disguised Indicator	True Indicator	Disguised Indicator
A0000	LGHTR	A0051	XEPAZ
0001	HMNCL	A0052	NGMPN
0002	SFOCD	A0053	OWQMA
0003	LECNF	A0054	AXSTO
0004	ABDCO	A0055	LFVLE
0005	TPFFN	A0056	DOTFN
0006	CWFNA		

Books contain not less than 10.000 and not more than 50.000 disguise and true indicators.

Traffic Testrictions

13 - The macimum load on any one rotor arrangement is 1.000 messages or 100.000 groups.

Classifications

14 - Types Mark 22 used as described above is considered secure for traf of the highest classification.

ds