Mark-III Scrambler & Aircraft Printer
Type 31

(Without Control Unit)

Scrambler

2350 - max. RPMs
2100 - min RPMs
250 - Range

1 1/4 % 20

@ 2150 R.P.Ms. - 75 W.P.M.

4450
2225

.1124
2225 | 250.0
2225
2750
2225
5250
4450
8000

450
60
27000
81
6,21(000 (36,000)
15
36

the control rotors are stepped

If 20 messages ~~are more~~ ~~with a length~~ of 400 letters or more in length are encrypted "in depth" ~~are assumed~~ it is assumed that the plain can be read by elementary methods —

If 20 messages of 400 or more letters in length are encrypted "in depth" it is assumed that they ~~may~~ can be read (~~the plain text found~~) by elementary methods.

overall
The cycle of the machine has weak points at considerable intervals — of variable length & depending upon the rotor arrangements in the alphabet and the index maze settings.

With possession of the machine and rotors it is possible to rig up a series of test messages in depth & with knowledge of exactly where the weak points fall it is possible to proceed along the general manner of solution in depth of the ECM — this contingency is not possible to enemy cryptanalysts & therefore is to be discounted.

→ This particular "chambered solution" can be easily blocked by careful selection of index rotors so that the right hand or #10 rotor ^shifted^ has a handling of 2 & the left hand or ~~the~~ slow rotor has a handling of 3 -

this however greatly reduces the number of available stepping combinations & would ~~[illegible]~~ somewhat decrease the overall security of the machine.

Therefore if messages in depth of 30 should ever get to be a common occurrence - ~~[illegible]~~ key lists would have to be prepared observing the above precaution -

---

With 30 in depth
&

With sufficient depth to permit reading the plaintext by elementary methods (~~[illegible]~~) & the [illegible] traffic compromise:

1. Set of rotors - 2 plain & cipher compromises on the same day, in depth on rotors #1, #3, #4, #5. Each message at least 150 letters long.

Effect: All five rotors are identified. The initial settings are recovered and all traffic for the day can be read -

compromise

2. Same conditions as in (1) but using changeable tires on the rotors -

Effect: Rotors #1 and #2 can be identified.

compromise

3. Set of rotors (~~10~~ rotors). 2 cipher messages enciphered on the same day using the same message indicator. A different plain text crib of 5 to 10 letters in length for each message at the same position of the texts.

Effect: Rotor order, initial setting & stepping pattern are recovered. Read all traffic for the day. This solution can not be obtained with existing machinery in a practical length of time. If rotor order is known then solution is very practical -

The special circuitry on the left hand endplate, combined with the 12 banked ~~inputs~~ & the 2 two banked stepping contacts, serve to give exactly 50 % energization to the remaining 12 individual ~~contacts~~ on the right end plate, and at the same time give a "random-and-flat" distribution of keying characters (of the 5 unit baudot code) to any 5 of these 12 ~~contacts~~. This is ~~important~~ extremely ~~important~~ for the 5 contacts controlling the ~~so~~ 5 polarity reversing relays in order to give a "random-and-flat" substitution key. The 4 individual contacts on the left end plate (which control transposition relays and the remainder the "set-up" relay) have approximately 50 % energization.

There is a manually operated switch which makes the necessary change from decipher to encipher. This switch is necessary because — although the substitution (polarity reversal) is self-reciprocal, the transposition is not. And furthermore the transposition has to be introduced at different points in the circuit for enciphering and deciphering. The engineering features are somewhat complicated and beyond the scope this paper. The exact action of the machine can best be understood by a careful study of the machine itself and its wiring diagram.