

(Without Control Unit)

Scrambler

2350 - Max RPMs
2100 - Min RPMs
250 - Range

11/4/60

@ 2150 RPMs - 75 W.P.M.

11/50
2225#
2225 | 250.0
 | 2275
 | 2750
 | 2275
 | 525
 | 4750
 | 8000

450
60
2960
8
6,210.00 (36,000)
15
36

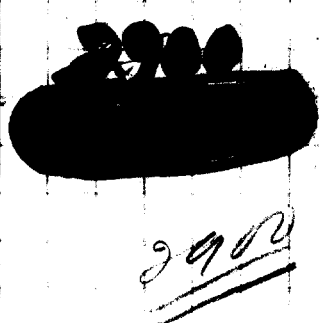
The control rotors are stepped

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

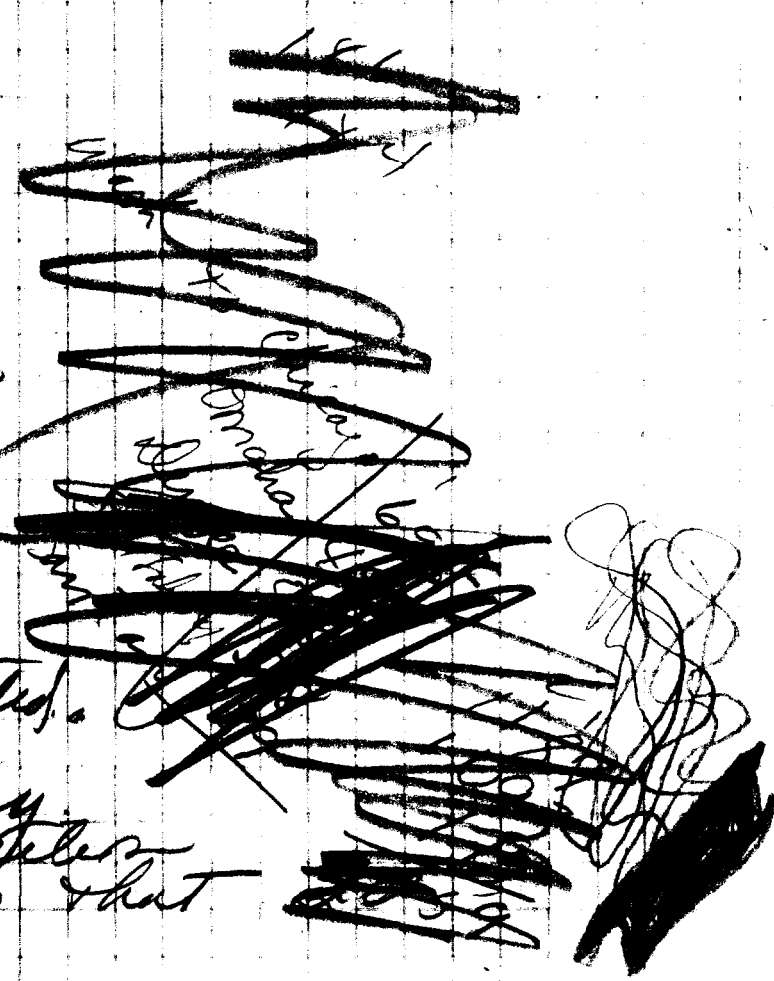
If 20 messages of 400 or more letters in length are encrypted "in depth" it is assumed that they may can be read ~~(the plain text found)~~ by elementary methods.

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 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 so discounted. This particular "chamber solution" can be easily blocked by careful alteration of index rotors so that



The right hand ^{alphabet} or #10 rotor has
a handling of 2 of the left hand
or ~~the~~ right rotor has a handling of 3.

This however, greatly reduces the
number of available stepping
combinations & would ~~greatly~~ somewhat
decrease the overall security
of the machine.

Therefore if messages in depth
of 30 should ever get to be a
common occurrence ~~now~~
Key tests would have to be
prepared observing the above
precaution.

with 30 in length

With sufficient depth to permit
reading the plaintext by elementary
methods (~~such as~~ ~~above~~), the ~~is~~
traffic

compromise:

1. Set 2 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 2 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 text.

Effect

Rotor order, initial settings & 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 end plate, combined with the 12 ^{banded} inputs & the 2 two banded 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 band at code) to any 5 ^{of these} contacts. This is ~~important~~ extremely important for the 5 contacts controlling the 5 polarity reversing relays in order to give a "random-and-flat" substitution key. The 4 individual contacts on the left end plate (3 of 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 of this paper. The exact action of the machine can best be understood by a careful study of the machine itself and its wiring diagram.