THE CLICK MACHINE

41

General Theory.

The machine is designed to deal only with unsteckered enigmas, or enigmas whose stecker are known.

It will try a short crib (usually 7 or 8 letters) in all positions of a message, and find the positions which give 7 or 8 consistent rod pairings.
“Wrong” stops (analogous to legal contradictions on the Bombes) also occur, but can be reduced by insisting on “1 confirmation” or “2 confirmations” on the rods .
The machine has switches called “Reminder switches” and these enable it to distinguish between stops with 1 confirmation, 2 confirmations etc..

The machine consists of the right-hand ends of eight enigmas - i.e. the right-hand wheel and the stecker of each enigma. The eight wheels are on the front of the machine and the eight stecker boards on top.

Normally the wheels are set initially at positions A, B, C ------H and they move round keeping the same relative distances.

The crib and message (unsteckered, if we are dealing with a steckered enigma) are punched out on cards. Each card contains the crib and a stretch of 7 or 8 letters and the text of the message. Thus for a message 200 letters long there would be about 200 cards. The cards are fed into the machine one by one. For each card the wheels make a complete revolution, thus trying all the 26 rod positions.
E.g.: Suppose that the 27th card is in the machine and that the letters punched on it are :-

T Q V L I R M J (unsteckered enigma text).
S V J Q B O T X (unsteckered crib).

When the 11th rod position is being tried the eight wheels will be in the positions :-

11 12 13 14 15 16 17 18 respectively.

Current is fed from the card as follows :-

into the first wheel at T and S
“ “ second “ “ Q and V
“ “ third “ “ V and J

“ “ eighth “ “ J and X

The current comes out on the “inner” side of the wheels at letters which correspond to the rod pairs given by T and S, Q and V, V and J etc.. Suppose the rod pairs are,

L S T I J T X X
H R C H N E M S

A necessary condition for the crib position and rod position to be right is that these 8 rod pairings should be completely consistent. In practice the right position would probably have one or two confirmations on the rods.

Examination of rod pairings for consistency is not an easy thing to do mechanically, and it is necessary to use an approximation method. Consider the sub-groups of the above set of 8 rod pairs. These may consist of 2, 3, 4, 5, 6 or 7 separate rod pairs, and the total number of such sub-groups is about 250. It is then clear that if EVERY sub-group of the 8 rod pairs contains an EVEN number of different letters, then the 8 rod pairs are consistent; for any inconsistency must be of the form

T J

L L

and the sub-group containing only these two inconsistent pairs contains 3 different letters. If it were possible to examine all sub-groups and reject positions where any of them was odd, we should have a perfect machine for our purpose. But to do this would require 250 sets of 26 relays: A compromise is effected by examining only 12 sub-groups chosen in a representative manner. It is then hoped that any inconsistency will cause at least one of these chosen sub-groups to be odd.

Six sub-groups are examined during what is called “Normal” running, and six more during “Column Change” running. All jobs are always run both “Normal” and “Column Change” and only stops appearing in both runs are relevant.

The examination is done by six sets of 26 relays, which are energised from the outputs of the “half-enigmas”. The actual sub-groups are as follows :-

“Enigma” outputs.

	1	2	3	4	5	6	7	8
Normal I								
II								
III								
IV								
V								
VI								
	1	2	3	4	5	6	7	8
Column I								
Change II								
III								
IV								
V								
VI								

There is a set of relays VII which examines the total number of different letters in all the 8 pairings. This total number must of course be even.
Thus the condition for a stop is that ALL the sub-groups AND the total shall be even.

N.B.

Positions where the crib crashes on the text are tested in the same way. (It would be difficult to cut out these positions automatically). A crash is equivalent to a “pair” which contains only one letter. “One” is odd, and it is hoped that this “odd” pair will cause at least one of the sub-groups to be odd. In fact it generally does do so.

Remainder Switches.

These switches serve to distinguish between stops with 1 confirmation, 2 confirmations etc.. Let l be the total number of different letters in all the 8 rod pairs. For an 8 letter crib,

l = 16	no confirmation
l = 14	1 confirmation
l = 12	2 confirmations
l = 10	3 confirmations
	etc.

A further set of relays VIIa is wired to count this number l “ in the scale of 5” when, of course,

16 becomes	“remainder 1”
14 becomes	“remainder 4”
12 becomes	“remainder 2”
10 becomes	“remainder 0”
	etc..

By putting on a remainder switch all stops with that particular remainder are ELIMINATED.
Thus, if we are assuming 1 confirmation put on remainder switch 1
if we are assuming 2 confirmations put on remainder switch 1 & 4
if we are assuming 3 confirmations put on remainder switch 1, 4 & 2
etc..

N.B. For a 7-letter crib the corresponding remainders are :-
1 confirm. remainder 4 ; 2 confirms. remainders 4 & 2 ; 3 confirms. remainders 4,2 & 0

Preparation of Jobs

It is best if the author of a job can personally see Mr. Freeborn, or his deputy, about details of running a job.

Enigma text :- should be unsteckered and written out, preferably in rows of 25 letters.
Doubtful letters must not be left blank.
Cribs :- should be unsteckered and numbered.
Stecker :- “straight stecker” should always be specified (for Pocket “QWERTY stecker” are used).
Remainders :- should be specified for each message-crib combination.
Order :- for a long job the order of running of the various cribs etc. should be indicated.
Results :- are usually sent from Block C by tube to the M.R. (Extension 13).
The author’s name should be attached to the job.

Testing of Results.

The result sheets appear as rows of 25 dots interspersed with letters. A letter V after 17 dots of a certain line denotes a stop where the crib starts at the 18th. position of that particular line of text and in the 22nd (Vth) rod position. Thus the rod position corresponding to any printed letter refers to the crib position of the dot immediately following it.

Only stops appearing in both "Normal" and "Column Change" runs need be tested. Stops are best tested by using punched masks for the message and for the various cribs and finding exactly what the rod-pairings are. A set of consistent rod pairings is then tested on the catalogues or the Jeffrey's sheets in the usual way.

"Wrong" stops may, of course, occur in which all the 12 chosen sub-groups are even, but in which the rod-pairings are not consistent. An occasional one of these should be tested fully as a check on the machine.

The respective sets of 7 or 8 letters of the message (which are punched on the cards 0 are usually printed out as well, and sent over with the stop sheets for easy reference.

Numbers of Stops.

Most jobs have so far been run as follows :-

(1) 8-letter cribs with remainders 1 & 4 (i.e. assuming at least 2 confirmations).
(2) 7-letter cribs with remainder 4 (i.e. assuming at least 1 confirmation).

The number of stops are then approximately,

(1) 2 per 100 letters of message per end wheel.
(2) 6 per 100 letters of message per end wheel.

However, most of the stops in (2) are consistent, while quite a number of the stops in (1) are contradictory. So in general, a 7-letter crib produces a smaller proportion of "wrong" stops than an 8-letter crib. These figures are almost entirely empirical, and I should like to see the results of all click jobs run in order to compile more accurate ones.

Risks.

The risks in assuming 1 confirmation, 2 confirmations etc. on the rods are as follows :-

7-letter crib.

remainder 4 (i.e. 1 confirmation)	risk = 13.8%
remainders 4 & 2 (i.e. 2 confirmations)	risk = 55.2%

8-letter crib.

remainder 1 (i.e. 1 confirmation)	risk = 6.6%
remainders 1 & 4 (i.e. 2 confirmations)	risk = 36.3%

O.H. Lawn.
16. 10. 43