MOST SECRET

THE "ORANGE ATTACHMENT" TO A BOMBE

In order to have any real chance of breaking into a key on a steckered enigma we need some sort of Bombe, and the essential thing on the Bombe is the diagonal board. But when the enigma is unsteckered, or – what is equally satisfactory – when the steckers are known, the key can often be broken by hand methods (using catalogues etc.), and no mechanical device is required.

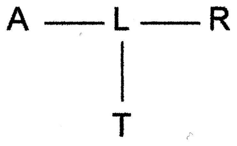
However, in certain cases (e.g. when our information is slight, or when the enigma has a complicated turnover motion), the catalogue methods become either impossible or most laborious; the use of a machine is then essential. Cases also arise in which some, but not all, of the stecker are known. These are included in the same category, and will also be discussed.

PRESENT METHOD

At present jobs of this kind are often run on the Bombes. The method is to put shorting plugs into each row of the diagonal board which corresponds to a letter x whose stecker is known. These plugs are arranged to short out every letter of the row except the stecker of x. The connections between disconnected constatations (crib pairings) are made via the permanent wiring of the diagonal board.

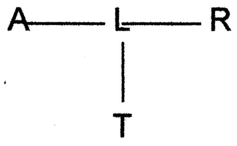
EG. 1

Menu



Stecker: A/T L/X R/V etc.

Bombe Copy

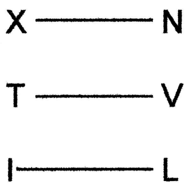


Shorting Plugs: At, Ta, Lx, Rv

This menu is effectively a "0 letters and 4 closures".

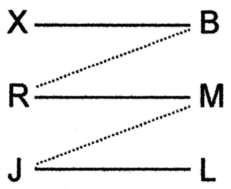
EG. 2

Menu



Stecker: X/S N/R T/B V/J I/M L/L

Bombe Copy



Shorting Plugs Xs, Br, Rb, Mj Jm,and Ll

This menu is effectively a "0 letters and 4 closures".

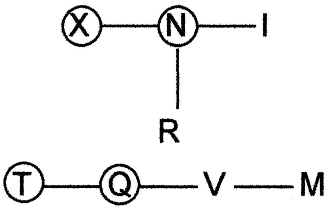
EG.3

Menu	Bombe Copy
X — ? — N	X — ? — B
T — ? — V	R — ? — M
I — ? — L	J — ? — L
Stecker: as above	Shorting plugs: as above

This procedure is exactly the same as for EG. 2.

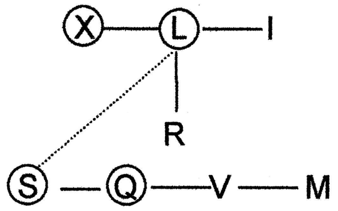
E.G. 4

Menu



Stecker X/A N/S T/L Q/B C/E only

Bombe Copy



Shorting Plugs:Xa, Ax; Ls, Sl; Nt, Tn; Qb, Bq; Ce, Ec.

The menu is effectively a "4 letter and 3 closures". Owing to the restriction on the steckers of the 4 letters I, R, V & M (they cannot be steckered to any of the 10 letters X, A, -------C, E), the number of stops is only about two per wheel-order

---

All jobs of this sort, of course, require a small number of enigmas. Consequently they are often put, for instance, on the spare enigmas remaining over when we are running a two-at-a-time menu. But, however small the number of enigmas is, we cannot run the menu on more than 4 banks, since the ordinary machine has only 4 inputs. Further, the input can always be put at a letter whose stecker is known, and so the same relay will always come up when there is a straight.

These jobs occur both in Hut 6 and Hut 8. In Hut 6 we sometimes run three constatations with known stecker – as in Eg.s 1 & 2; or three "banbury" constatations with known stecker, as in EG.3. Orange is the ordinary case of Eg.4. In Hut 8 this sort of job (for a 3-wheel machine) can usually be done by hand methods.

However, and this is the important point, these menus arise also on the Shark 4-wheel machine, and for 4-wheel problems hand methods become quite a different affair: they are either extremely laborious or quite impossible.

Now when we run these menus on a Bombe we do not use very much of the Bombe. We use only a small number of enigmas per bombe, only one of the 26 relays of the input, and (except for Orange menus (Eg.4) we only use the diagonal boar for joining disconnected constatations. So it has been suggested that a special attachment to a 4-wheel Bombe should be made for these jobs. This attachment would be able to be used with any 4-wheel Bombe; and it would run menus on a large number of banks. It would be designed primarily for 4-wheel problems – i.e. the menus would usually consist of four constatations, not three; but it would be extremely useful for the 3-wheel jobs which are at present run so uneconomically on the existing machines.

PROPOSALS

Two schemes have so far been suggested for the Bombe – both designed to give the necessary connections with as simple a plugging system as possible. The two schemes are set out below.

For 4-wheel jobs four constatations – for which all the stecker are known – will be needed on a menu. So, with a 36 enigma machine, we shall need just 9 "inputs". Each input will consist of only one relay, and the stopping and/or recording mechanism will be as simple as possible. (3-wheel jobs – using three constatations – will of course need only three enigmas, and it might be worth while to have 12 "inputs" and so run these jobs 12 times.)

Scheme A. (The old scheme suggested more than a year ago).

Each input and output of an enigma will be associated with a set of 26 pluggable sockets, and each terminal will be taken to one of these sockets. Thus the enigmas can be plugged up either by using the separate sockets or by using 26-way plaits plugged between the ordinary inputs and outputs. A menu of known pairings will be plugged up as a single circuit, and when the circuit is closed the sensing relay will operate.

Scheme B (Suggested by W.G.W.)

We shall have a variety of shorting plugs – about 12 for each letter of the alphabet. The plug 'X', for instance, will have all its terminals except 'X' itself commoned together; 'X' will be taken out to a single lead. These plugs will be put into the ordinary enigma inputs and outputs, and their single leads will all be plugged into a common. Current will be fed in on the commoned terminals of each plug. A relay will attach to the common which contains the single leads and when this relay is not energised the machine will stop.

In illustration of these two schemes the two ways of running the same job are shown below:

EG. 5

Menu

$A \overset{1}{\text{————}} T$

$L \overset{2}{\text{————}} V$

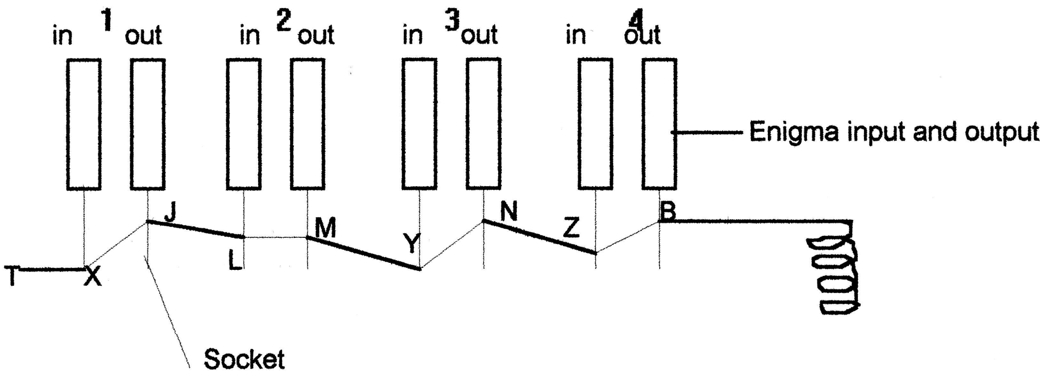
$I \overset{3}{\text{————}} N$

$R \overset{4}{\text{————}} S$

Steckers:- A/X T/J L/L V/M I/Y N/N R/Z S/B etc.

EG.5 (Diagrams)

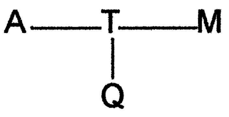
SCHEME A:-



SCHEME B:

EG.6

Menu



STECKERS: I———R

Here in Scheme A we plug each enigma separately and make, as before, a single circuit to the relay. In Scheme B we should take the enigmas meeting at 'T' out to an ordinary common, and take our "T" shorting plug from this common to the relay common. We should thus need only one "T" shorting plug per bank.

The case of knowing <u>some</u> but not all of the stecker is special, and will need special treatment. Scheme B can be made to deal very satisfactorily with it; Scheme A cannot.

The case of knowing some but not all of the stecker is special, and will need special treatment. Scheme B can be made to deal very satisfactorily with it; Scheme A cannot.

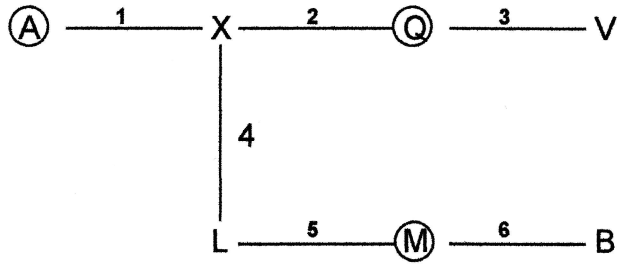
Suppose that x is a letter whose stecker is known, and y is a letter whose stecker is unknown. On our menu there will be, probably, 3 or 4 of the letters x and about 4 of the letters y (as in Eg 4 above). Since the number of y letters is small we may ignore the reduction factor due to the elimination of illegal contradictions between them. This factor will in fact be nearly 1. With this reservation the job can be run just as well if we simply short out the x letters from the possible steckers for the y letters. This, of course, will not need a diagonal board.

The method for this shorting, suggested by W.G.W., is as follows: The machine is fitted with a set of female sockets (about 24 in number); call these α. These sockets will each have 26 terminals and will take the ordinary 26-way double-ended jacks. The separate terminals of these sockets are taken out to another set of 26 similar sockets (β), so that all the A terminals of the sockets α are taken to 24 of the 26 terminals of one of the sockets β, all the B terminals of the sockets α are taken to another of the sockets β, etc. etc.

Then if we wish to eliminate the x letters as possibilities for the steckers of the y letters we simply plug each of the y letters (by 26-way plaits) into one of the α sockets, and put shorting plugs (with all 26 terminals commoned) into the sockets β wish correspond to the x letters.

EG. 7

Menu



Stecker known: A/R Q/T M/N D/S I/Z only.

Plugging – Scheme B :-

It is suggested that the shorting on the sockets β could be done for all banks by the same plugs – i.e. that we should only need one set of 24 α sockets and one set of 26 β sockets, and that it would not be necessary to have separate ones for each bank.

It is clear that Scheme B is definitely the better scheme of the two – and for two reasons:-

1. It can be constructed as a reasonably simple attachment which can be used with any Bombe. A special Bombe is not needed. Scheme A would require either a much more bulky attachment or a re-designed Bombe.

2. By making a negative test (of non-energised points) it enables impossible stecker to be eliminated by means of shorting plugs. Scheme A makes a positive test, and this procedure cannot therefore be applied.

Finally it should be emphasised that this note is not intended as a statement of a proposed policy or a proposed design. It is simply an attempt to describe what is meant by, and what is involved in, "known stecker" problems.

O.H.L.

29.12.42