# Turing’s Treatise on Enigma

# “Prof’s Book”

## Chapter 6

Dr. Alan M. Turing

# Editors' Preface

This document was written by the late Dr. Alan Turing while he worked as a cryptanalyst at Bletchley Park during the Second World War. The document has been obtained from the US National Archives and permission has been obtained from the Controller of Her Majesty's Stationery Office to publish the paper on the personal Web Page of Frode Weierud. The document has been faithfully retyped by the three editors, Ralph Erskine, Philip Marks and Frode Weierud. The original document was typed and had the style and layout of a typewritten document of that period. To make the re-edited presentation more pleasing the document has been both left and right justified and a more modern type font has been used. The page numbers of the original are given as numbers in square brackets. Apart from these modifications to the layout the document has the appearance of the original.

Where there are obvious typing errors these have been corrected in square brackets. In a few cases a superfluous letter(s) has been removed by putting the letter(s) in square brackets preceded by a slash, e.g. [/s]. The Editors' comments are in square brackets and in italic. Longer and more detailed comments are in numbered footnotes.

The Editors,

Ralph Erskine,
Philip Marks,
Frode Weierud, © February 1999

## Source:

National Archives and Records Administration (NARA), Record Group 457, NSA Historical Collection, Box 201, Nr. 964. The NARA copy has now been checked and verified against the copy in the Public Record Office (PRO) at Kew, London. The PRO copy is in HW 25/3.

## COPYRIGHT

**Updated: 8 February 2001**

[ 96 ]

# Chapter VI. The steckered Enigma. Bombe and Spider.

When one has a steckered Enigma to deal with one’s problems naturally divide themselves into what is to be done to find the Stecker, and what is to be done afterwards. Unless the indicating system is very well designed there will be no problem at all when the Stecker have been found, and even with a good indicating system we shall be able to apply the methods of the last two chapters to the individual messages. The obvious example of a good indicating system is the German Naval Enigma cipher, which is dealt with in Chapter VII. This chapter is devoted to methods of finding the Stecker. Naturally enough we never find the Stecker without at the same time finding much other information.

## Cribs.

The most obvious kind of data for finding the keys is a ‘crib’, i.e. a message of which a part of the decode is known. We shall mostly assume that our data is a crib, although actually it may be a number of constatations arising from another source, e.g. a number of CILLIs or a Naval Banburismus.

## FORTYWEEPYYWEEPY methods.

It is sometimes possible to find the keys by pencil and paper methods when the number of Stecker is not very great, e.g. 5 to 7. One would have to hope that several of the constatations of the crib were ‘unsteckered’. The best chance would be if the same pair of letters occurred twice in the crib (a ‘half-bombe’). In this case, assuming 6 or 7 Stecker there would be a 25% chance of both constatations being unsteckered. The positions at which these constatations occurred could be found by means of the Turing sheets (if there were three wheels) or the Jeffreys sheets. The positions at which this occurred could be separately tested. Another possibility is to set up the inverse rods for the crib and to look for clicks. There is quite a good chance of any apparent click being a real click arising because all four letters involved are unsteckered. The position on the right hand

[ 97 ]

wheel is given by the column of the inverse rod set-up, and we can find all possible positions where the click coupling occurs from the Turing sheets or the Jeffreys sheets. In some cases there will be other constatations which are made up from letters supposed to be unsteckered because they occur in the click, and these will further reduce the number of places to be tested.

These methods have both of them given successful results, but they are not practicable for cases where there are many Stecker, or even where there are few Stecker and many wheel orders.

## A mechanical method. The Bombe.

Now let us turn to the case where there is a large number of Stecker, so many that any attempt to make use of the unsteckered letters is not likely to succeed. To fix our ideas let us take a particular crib.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D | A | E | D | A | Q | O | Z | S | I | Q | M | M | K | B | I | L | G | M | P | W | H | A | I | V |
| K | E | I | N | E | Z | U | S | A | E | T | Z | E | Z | U | M | V | O | R | B | E | R | I | Q | T |

Presumably the method of solution will depend on taking hypotheses about parts of the keys and drawing what conclusions one can, hoping to get either a confirmation or a contradiction. The parts of the keys involved are the wheel order, the rod start of the crib, whether there are any turnovers in the crib and if so where, and the Stecker. As regards the wheel order one is almost bound to consider all of these separately. If the crib were of very great length one might make no assumption about what wheels were in the L.H.W. position and M.W. position, and apply a method we have called ‘Stecker knock-out’ (an attempt of this kind was made with the ‘Feindseligkeiten’ crib in Nov.’39), or one might sometimes make assumptions about the L.H.W. and M.W. but none, until a late stage about the R.H.W. In this case we have to work entirely with constatations where the R.H.W. has the same position. This method was used for the crib from the Schlüsselzettel of the Vorpostenboot, with success; however I shall assume that all

wheel orders are being treated separately. As regards the turnover one will normally take several different hypotheses, e.g.-

| | | | | | | |
|---|---|---|---|---|---|---|
| 1) | turnover between positions | | | 1 | and | 5 |
| 2) | „ | „ | „ | 5 | and | 10 |
| 3) | „ | „ | „ | 10 | and | 15 |
| 4) | „ | „ | „ | 15 | and | 20 |
| 5) | „ | „ | „ | 20 | and | 25 |

With the first of these hypotheses one would have to leave out the constatations in positions 2 to 4, and similarly in all the other hypotheses four constatations would have to be omitted. One could of course manage without leaving out any constatations at all if one took 25 different hypotheses, and there will always be a problem as to what constatations can best be dispensed with. In what follows I shall assume we are working the T.O. hypothesis numbered 5)[1] above. We have not yet made sufficiently many hypotheses to be able to draw any immediate conclusions, and must therefore either assume something about the Stecker or about the rod start. If we were to assume something about the Stecker our best chance would be to assume the Stecker values of A and E, or of E and I, as we should then have two constatations corrected for Stecker, with only two Stecker assumptions. With Turing sheets one could find all possible places where these constatations occurred, of which we should, on the average, find about 28.1. As there would be 626 hypotheses of this kind to be worked we should gain very little in comparison with separate examination of all rod starts. If

[1] Editors’ Note: Turing says hypothesis number 5 but the menu in Fig. 59 shows that the turnover hypothesis is number 4.

there had not been any half-bombes in the crib we should have fared even worse. We therefore work all possible hypotheses as to the rod start, and to simplify this we try to find characteristics of the crib which are independent of the Stecker. Such characteristics can be seen most easily if the crib is put in to the form of a picture

[ 99 ]

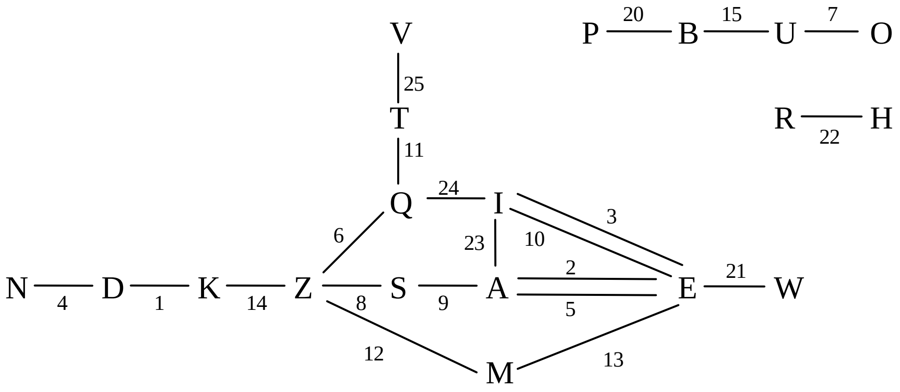


Fig. 59. Picture from KEINE ZUSAETZE crib.
Constatations 16 to 19 omitted to allow for turnover.

[*The figure shows one of the thyratron circuits connected to the 26 phase supply.*]

Fig. 60 Circuit for Pye simultaneous scanning

[ 100 ]

```
 2 5          3 10        2 23 3      2 9  8 6 24 3    13 12 8 9 5
 EAE          EIE         EAIE        EASZQIE          EMZSAE
              XHI
              IQW
              WAZ                                                     A /
              ZRU                                                     B /
              UBT                                                     C /
              TGM                                                     D /
              MDF                                                     E /
              FCV                                                     F /
              VON                                                     G /
              NEX                                                     H /
 XNW                                                                  I /
 WIO                                                                  J /
 OUF                                                                  K /
 FTK                                                                  L
 KQP                                                                  M /
 PAS                                                                  N /
 SMD                                                                  O /
 DBX[2]                                                               P /
              OVC                                                     Q /
              CFD                                                     R /
              DMG                                                     S /
              GTB                                                     T /
              BUR                                                     U /
              RZA                                                     V /
              AWQ                                                     W /
              QIH                                                     X /
              HXE                                                     Y /
              ENO                                                     Z /
              KPK
              PKP
              SLS
 IWN                      APJY
 NXB          YJY
 BDM                      PAYJ
 MSA          JYJ
```

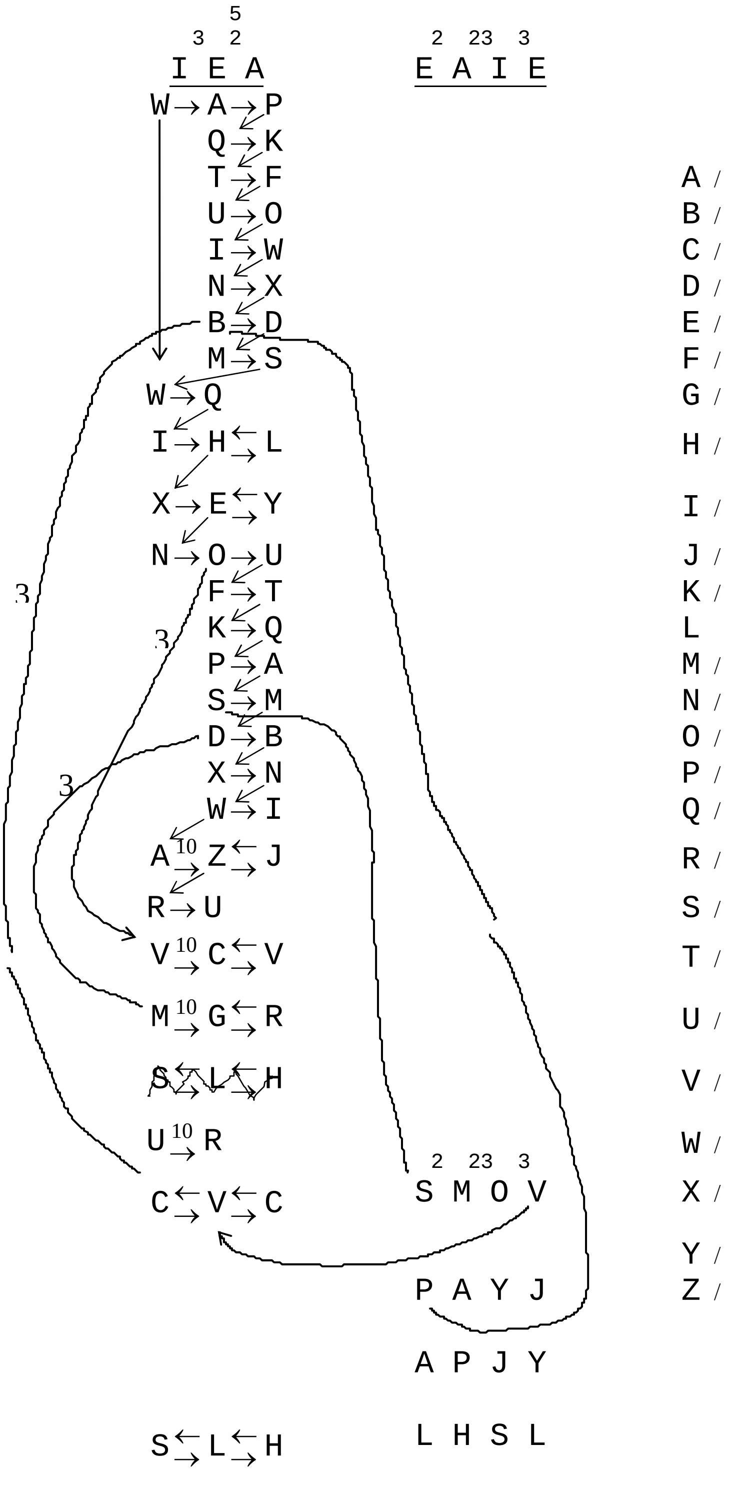
Fig. 61. Stecker deductions with crib on p. [97], with correct rod start and correct alphabets, but starting from an incorrect Stecker hypothesis E/X. All other incorrect Stecker values of E are deduced.

```
 2 5          3 10        2 23 3      2 9  8 6 24 3    13 12 8 9 5
 EAE          EIE         EAIE        EASZQIE          EMZSAE
 LHL          LSL         LHSL        LHIRWSL          LMRIHL
```

Fig. 62. Stecker deductions with same alphabets as Fig. 61, but from correct Stecker hypothesis E/L.

[2] Editors' Note: Turing has written DBN but it must be DBX.

[ 100a ][3]



[3] Editors' Note: This figure, which has no caption or other explanation, follows page 100 but the page itself is not numbered. We have decided to label the page 100a. The appearance is that of worksheet more than a figure that belongs to the text.

[ 101 ]

like Fig. 59. From this picture we see that one characteristic which is independent of the Stecker is that there must be a letter which enciphered at either position 2 or position 5 of the crib gives the same result. This may also be expressed by saying that there must be a letter such that, if it is enciphered at position 2, and the result re-enciphered at position 5 the final result will be the original letter. Another such condition is that the same letter enciphered successively at the positions 3, 10 must lead back to the original letter. Three other conditions of this kind are that the successive encipherments at positions 2, 23, 3 or at 2, 9, 8, 6, 24, 3 or at 13, 12, 8, 9, 5 starting from the same letter as before must lead back to it. There are other such series, e.g. 13, 12, 6, 24, 3 but these do not give conditions independent of the others. The letter to which all these multiple encipherments are applied is, of course, the Stecker value of E. We shall call E the ‘central letter’. Any letter can of course be chosen as ‘central letter’, but the choice affects the series of positions or ‘chains’ for the multiple encipherments. There are other conditions, as well as these that involve the multiple encipherments. For instance ‘the Stecker values’ of the letters in Fig. 59 must all be different. The Stecker values for E, I, M, Z, Q, S, A are the letters that arise at the various stages in the multiple encipherments and the values for W, T, V, N, D, K can be found similarly. There is also the condition that the Stecker must be self-reciprocal, and the other parts or ‘webs’ of Fig. 59, P-B-U-O and R-H will also restrict the possibilities somewhat. Of these conditions the multiple encipherment one is obviously the easiest to apply, and with a crib as long as the one above

[ 102 ]

this condition will be quite sufficient to reduce the possible positions to a number which can be tested by hand methods. It is actually possible to make use of some of the other conditions mechanically also; this will be explained later.

In order to apply the multiple encipherment condition one naturally wants to be able to perform the multiple encipherments without Stecker in one operation. To do this we make a new kind of machine which we call a ‘Letchworth Enigma’. There are two rows of contacts in a Letchworth Enigma each labelled A to Z and called the input and output rows: there are also moveable wheels. For each position of an ordinary Enigma there is a corresponding position of the Letchworth Enigma, and if the result of enciphering F at this position is R, then F on the input row of the Letchworth Enigma is connected to R on the output row, and of course R on the input row is connected to F on the output row. Such a ‘Letchworth Enigma’ can be made like an ordinary Enigma, but with all the wiring of the moveable wheels in duplicate, one set of wires being used for the journey towards the Umkehrwalze, and the others for the return journey. The Umkehrwalze has two sets of contacts, one in contact with the inward-journey wiring of the L.H.W. and one in contact with the outward-journey wiring. The Umkehrwalze wiring is from the one set of contacts across to the other. In the actual design used there were some other differences; the wheels did not actually come into contact with one another, but each came into contact with a ‘commutator’ bearing 104 fixed contacts. These contacts would be connected by fixed wiring to contacts of other commutators. These contacts of the commutators can be regarded as physical counterparts of the ‘rod points’ and ‘output points’ for the wheels.

[ 103 ]

If one has two of these ‘Letchworth Enigmas’ one can connect the output points of the one to the input points of the other and then the connections through the two Enigmas between the two sets of contacts left over will give the effect of successive encipherments at the positions occupied by the two Enigmas. Naturally this can be extended to the case of longer series of Enigmas, the output of each being connected to the input of the next.

Now let us return to our crib and see how we could use these Letchworth Enigmas. For each of our ‘chains’ we could set up a series of Enigmas. We should in fact use 18 Enigmas which we will name as follows

| | | |
|---|---|---|
| A1, A2 | with the respective positions | 2, 5 |
| B1, B2 | | 3, 10 |
| C1, C2, C3 | | 2, 23, 3 |
| D1, D2, D3, D4, D5, D6 | | 2, 9, 8, 6, 24, 3 |
| E1, E2, E3, E4, E5 | | 13, 12, 8, 9, 5 |

By ‘position 8’ we here mean ‘the position at which the constatation numbered 8 in the crib, is, under the hypothesis we are testing, supposed to be enciphered’. The Enigmas are connected up in this way: output of A1 to input of A2: output of B1 to input of B2: output of C1 to input of C2, output of C2 to input of C3: etc. This gives us five ‘chains of Enigmas’ which we may call A, B, C, D, E, and there must be some letter, which enciphered with each chain gives itself. We could easily arrange to have all five chains controlled by one keyboard, and to have five lampboards shewing the results of the five multiple encipherments of the letter on the d[e]pressed key. After one hypothesis as to the rod start had been tested one would go on to the next, and this would usually involve simply moving the R.H.W. of each Enigma forward one place. When 26 positions of the R.H.W. have been tested the M.W. must be made to move forward too. This movement of the wheels in step can be very easily done mechanically, the right hand wheels all being driven continuously from one shaft, and the motion of the other wheels being controlled by a carry mechanism.

[ 104 ]

It now only remains to find a mechanical method of registering whether the multiple encipherment condition is fulfilled. This can be done most simply if we are willing to test each Stecker value of the central letter throughout all rod starts before trying the next Stecker value. Suppose we are investigating the case where the Stecker value of the central letter E is K. We let a current enter all of the chains of Enigmas at their K input points, and at the K output points of the chains we put relays. The ‘on’ points of the five relays are put in series with a battery (say), and another relay. A current flows through this last relay if and only if a current flows through all the other five relays, i.e. if the five multiple encipherments applied to K all give K. When this happens the effect is, essentially, to stop the machine, and such an occurrence is known at Letchworth as a ‘straight’. An alternative possibility is to have a quickly rotating ‘scanner’ which, during a revolution would first connect the input points A of the chains to the current supply, and the output points A to relays, and then would connect the input and output points B to the supply and relays. In a revolution of the scanner the output and input points A to Z would all have their turn, and the right hand wheels would then move on. This last possible solution was called ‘serial scanning' and led to all the possible forms of registration being known as different kinds of 'scanning'. The simple possibility that we first mentioned was called 'single line scanning'. Naturally there was much research into possible alternatives to these two kinds of scanning, which would enable all 26 possible Stecker values of the central letter to be tested simultaneously without any parts of the machine moving. Any device to do this was described as 'simultaneous scanning'.

[ 105 ]

The solution which was eventually found for this problem was more along mathematical than along electrical engineering lines, and would really not have been a solution of the problem as it was put to the electricians, to whom we gave, as we thought, just the essentials of the problem. It turned out in the end that we had given them rather less than the essentials, and they therefore cannot be blamed for not having found the best solution. They did find a solution of the problem as it was put to them, which would probably have worked if they had had a few more months experimenting. As it was the mathematical solution was found before they had finished.

## Pye simultaneous scanning

The problem as given to the electricians was this. There are 52 contacts labelled A…Z, A',…,Z'. At any moment each one of A,…,Z is connected to one and only one of A',…,Z': the connections are changing all the time very quickly. For each letter of the alphabet there is a relay, and we want to arrange that the relay for the letter R will only close if contact R is connected to contact R'.

The latest solution proposed for this problem depended on having current at 26 equidistant phases corresponding to the 26 different letters. There is also a thyratron valve[*] for each letter. The filaments of the thyratrons are given potentials corresponding to their letters, and the grids are connected to the corresponding points A',…,Z'. The points A,…,Z are also

[ 106 ]

given potentials with the phase of the letter concerned. The result is that the difference of potential of the filament and the grid of thyratron A oscillates with an amplitude of at least $2\pi\frac{E}{27}$, [$2E\sin\frac{\pi}{26}$], E being the amplitude of the original 26 phase supply, unless A and A' are connected through the chain, in which case the potentials remain the same or differ only by whatever grid bias has been put into the grid circuit[4]. The thyratrons are so adjusted that an oscillation of amplitude $2\pi\frac{E}{27}$ will bring the potential of the grid to the critical value and the valve will 'fire'. The valve is coupled with a relay which only trips if the thyratron fails to fire. This relay is actually a

[*] A thyratron valve has the property that no current flows in the anode circuit until the grid potential becomes more negative than a certain critical amount, after which the current continues to flow regardless of the grid potential, until the anode potential is switched off.

[4] Editors' Note: Turing is using an approximation to describe the amplitude, the real expression has been added by the editors in square brackets. It has been independently derived by Donald Davies and Martin Slack and we are grateful for their help in explaining the details of this circuit.

'differential relay', with two sets of windings, one carrying a constant current and the other carrying the current from the anode circuit of the thyratron. Fig. 60 shews a possible form of circuit. It is probably not the exact form of circuit used in the Pye experiments, but is given to illustrate the theoretical possibility.

## The Spider

We can look at the Bombe in a slightly different way as a machine for making deductions about Stecker when the rod start is assumed. Suppose we were to put lamp-boards in between the Enigmas of the chains, and label the lamp-boards with the appropriate letters off figure [*number missing*]. For example in chain C the lampboard between C1 and C2 would be labelled A. The key-board, if we were using one, could be labelled with the 'central letter'. Now when we depress a letter of the key-board we can read off from the lamp-boards some of the Stecker consequences of the hypothesis that the depressed letter is steckered to the central letter; for one such consequence could be read off each lampboard, namely that the letter lighting is steckered to the name of the lamp-board.

[ 107 ]

When we look at the Bombe in this way we see that it would be natural to modify it so as to make this idea fit even better. We have not so far allowed for lengthy chains of deductions; the possible deductions stop as soon as one comes back to the central letter. There is however no reason why, when from one hypothesis about the Stecker value of the central letter we have deduced that the central letter must have another Stecker value, we should not go on and draw further conclusions from this second Stecker value. At first sight this seems quite useless, but, as all the deductions are reversible, it is actually very useful, for all the conclusions that can be drawn will then be false, and those that remain will stand out clearly as possible correct hypotheses. In order that all these deductions may be made mechanically we shall have to connect the 26 contacts at the end of each chain to the common beginning of all the chains. With this arrangement we can think of each output or input point of an Enigma as representing a possible Stecker, and if two of these points are connected together through the Enigmas then the corresponding Stecker imply one another. At this point we might see how it all works out in the case of the crib given above. This crib was actually enciphered with alphabets which, when corrected for their Stecker, are those given below, the numbers over the crib constatations giving the column headings.[5] The alphabets most used below are 2, 3, 5, 10, 23, and these are reproduced here for reference

[5] Editors' Note: The alphabets have been generated by a one wheel Enigma machine consisiting of the Umkehrwalze (UKW) and wheel III (Green) from the Railway Enigma.

| 2 | 3 | 5 | 10 | 23 |
|---|---|---|---|---|
| XN | XH | MD | TB | LV |
| AP | BU | JZ | IH | WC |
| QK | EN | CV | RU | DI |
| CV | PK | SA | XE | OM |
| TF | QI | YE | CV | XU |
| UO | AW | GR | JY | FT |
| MS | OV | PQ | DF | JP |
| BD | JY | NW | SL | GE |
| IW | DM | LH | ON | AY |
| JZ | RZ | BX | QW | NB |
| GR | SL | FU | AZ | HS |
| YE | GT | OI | PK | ZQ |
| HL | FC | KT | GM | RK |

[ 108 ]

In Fig. 61 at the top are the chains, with the positions and the letters of the chain. In each column are written some of the letters which can be inferred to be Stecker values of the letters at the heads of their columns from the hypothesis that X is a Stecker value of the central letter E. By no means all possible inferences of this kind are made in the figure, but among those that are made are all possible Stecker values for E except the right one, L. If we had taken a rod start that was wrong we should almost certainly have found that all of the Stecker values of E could have been deduced from any one of them, and this will hold for any cribs with two or more chains. Remembering now that with our Bombe one Stecker is deducible from another if the corresponding points on the lamp boards are connected through the Enigmas, a correct rod start can only be one for which not all the input points of the chains are connected together; the positions at which this happens are almost exactly those at which a Bombe with simultaneous scanning would have stopped.

This is roughly the idea of the ‘spider’. It has been described in this section as a way of getting simultaneous scanning on the Bombe, and has been made to look as much like the Bombe as possible. In the next section another description of the spider is given.

## The Spider. A Second Description. Actual Form.

In our original description of the Bombe we thought of it as a method of looking for characteristics of a crib which are independent of Stecker, but in the last section we thought of it more as a machine for making Stecker deductions. This last way of looking at it has obviously great possibilities, and so we will start afresh with this idea.

In the last section various points of the circuit were regarded as having certain Stecker corresponding to them. We are now going to carry this idea further and

[ 109 ]

have a metal point for each possible Stecker. These we can imagine arranged in a rectangle. Each point has a name such as Pv: here the capital letters refer to ‘outside’ points and the small letters to 'inside letters'; an outside letter is the name of a key or bulb, and so can be a letter of a crib, while an inside letter is the name of a contact of the Eintrittwalze, so that all constatations obtained from the Enigma without Stecker give information about inside letters rather than outside. Our statements will usually be put in rather illogical form: statements like 'J is an outside letter' will usually mean 'J is occurring in so and so as the name of a key rather than of a contact of the Eintrittwalze'. The rectangle is called the 'diagonal board' and the rows are named after the outside letters, the columns after the inside letters. Now let us take any constatation of our crib e.g. $\genfrac{}{}{0pt}{}{Q}{I}$ at 24. For the position we are supposed to be testing we will have an Enigma set up at the right position for encoding this constatation, but of course without any Stecker. Let us suppose it set up for the correct position, then one of the pairs in the alphabet in position 24 is OC: consequently if Qo then Ic (i.e. if outside letter Q is associated with inside o then outside I is associated with inside c). Now if we connect the input of the (Letchworth) Enigma to the corresponding points of the diagonal board on line Q and the output to line I then since the "o" input point is connected to the "c" output point we shall have Qo on the diagonal board connected to Ic through the Letchworth Enigma. We can of course put in a Letchworth Enigma for every constatation of the crib, and then we shall have all the possible deductions that can be made about the association of inside and outside letters paralleled in the connections between the points of the diagonal board. We can also bring in the reciprocal property of the Stecker by connecting together diagonally opposite points of the diagonal board, e.g. connecting Pv to Vp. One can also bring in other conditions about the

[ 110 ]

Stecker, e.g. if one knows that the letters which were unsteckered on one day are invariably steckered on the next then, having found the keys for one day's traffic one could when looking for the keys for the next day, connect together all points of the diagonal board which correspond to non-steckers which had occurred on the previous day. This would of course not entirely eliminate the inadmissible solutions, but would enormously reduce their number, the only solutions which would not be eliminated being those which were inadmissible on every count.

One difference between this arrangement and the Bombe, or the spider as we described it in the last section, is that we only need one Enigma for each constatation.

Our machine is still not complete, as we have not put in any mechanism for distinguishing correct from incorrect positions. In the case of a crib giving a picture like Fig. 59 where most of the letters are connected together in one 'web' it is sufficient to let current into the diagonal board at some point on some line named after a letter on the main web, e.g. at the Ea point in the case of the crib we have been considering. In this case the only possible positions will be ones in which the current fails to reach all the other points of the E line of the diagonal board. We can detect whether this happens by connecting the points of the E line through differential relays to the other pole of our current supply, and putting the 'on' points of the relays in parallel with one another and in series with the stop mech[*anism*]. Normally current will flow through all the differential relays, and they will not move. When one reaches a position that might be correct the current fails to reach one of these relays, and the current permanently flowing in the other coil of the relay causes it to close, and bring the stopping mechanism into play. Mostly what will happen is that there will be just one relay which closes, and this will be one connected to a point of the diagonal board which corresponds to a Stecker which is possibly correct: more accurately, if this Stecker is not correct the position is not correct. Another possibility is

[ 111 ]

that all relays close except the one connected to the point at which current enters the diagonal board, and this point then corresponds to the only possible Stecker. In cases where the data is rather scanty, and the stops therefore very frequent, other things may happen, e.g. we might find four relays closing simultaneously, all of them connected together through the Enigmas and the cross connections of the diagonal board, and therefore none of them corresponding to possible Stecker.

In order for it to be possible to make the necessary connections between the Enigmas, the diagonal board and the relays there has to be a good deal of additional gear. The input and output rows of the Enigmas are brought to rows of 26 contacts called ‘female jacks’. The rows of the diagonal board are also brought to female jacks. The 26 relays and the current supply are also brought to a jack. Any two female jacks can be connected with ‘plaited jacks’ consisting of 26 wires plaited together and ending in male jacks which can be plugged into the female jacks. In order to make it possible to connect three or more rows of contacts together one is also provided with ‘commons’ consisting of four female jacks with corresponding points connected together. There is also a device for connecting together the output jack of one Enigma with the input of the next, both being connected to another female jack, which can be used for connecting them to anywhere else one wishes.

On the first spider made there were 30 Enigmas, and three diagonal boards and ‘inputs’ i.e. sets of relays and stopping devices. There were also 15 sets of commons.

[ 112 ]

Figs 63, 64 shew the connections of Enigmas and diagonal board in a particular case. The case of a six-letter alphabet has been taken to reduce the size of the figure.

The actual origin of the spider was not an attempt to find simultaneous scanning for the Bombe, but to make use of the reciprocal character of the Stecker. This occurred at a time when it was clear that very much shorter cribs would have to be worked than could be managed on the Bombe. Welchman then discovered that by using a diagonal board one could get the complete set of consequences of a hypothesis. The ideal machine that Welchman was aiming at was to reject any position in which a certain fixed-for-the-time Stecker hypothesis led to any direct contradiction: by a direct contradiction I do not mean to include any contradictions which can only be obtained by considering all Stecker values of some letter independently and shewing each one inconsistent with the original hypothesis. Actually the spider does more than this in one way and less in another. It is not restricted to dealing with one Stecker hypothesis at a time, and it does not find all direct contradictions.

Naturally enough Welchman and Keen set to work to find some way of adapting the spider so as to detect all direct contradictions. The result of this research is described in the next section. Before we can leave the spider however we should see what sort of contradictions it will detect, and about how many stops one will get with given data.

First of all let us simplify the problem and consider only ‘normal’ stops, i.e. positions at which by altering the point at which the current enters the diagonal board to another [*point?*] on the same line one can make 25 relays close [*illegible, may be: and there is only one such point*]. The current will then be

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 5 out, D | 5 out, E | 5 out, F | 5 out, A | 5 out, B | 5 out, C | |
| Input jack | Fa | Fb | Fc | Fd | Fe | Ff | |
| | 5 in, A | 5 in, B | 5 in, C | 5 in, D | 5 in, E | 5 in, F | |
| Enigma 5 | | | | | | | (arriving from $\genfrac{}{}{0pt}{}{F}{C}$) |
| | 5 out, A | 5 out, B | 5 out, C | 5 out, D | 5 out, E | 5 out, F | |
| Output jack | Ca | Cb | Cc | Cd | Ce | Cf | |
| | 5 in, D | 5 in, E | 5 in, F | 5 in, A | 5 in, B | 5 in, C | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 out, F | 1 out, D | 1 out, E | 1 out, B | 1 out, C | 1 out, A | |
| Input jack | Fa | Fb | Fc | Fd | Fe | Ff | |
| | 1 in, A | 1 in, B | 1 in, C | 1 in, D | 1 in, E | 1 in, F | (arriving from ) |
| Enigma 1 | | | | | | | (constatation $\genfrac{}{}{0pt}{}{F}{A}$) |
| | 1 out, A | 1 out, B | 1 out, C | 1 out, D | 1 out, E | 1 out, F | |
| Output jack | Aa | Ab | Ac | Ad | Ae | Af | |
| | 1 in, F | 1 in, D | 1 in, E | 1 in, B | 1 in, C | 1 in, A | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 2 out, B | 2 out, A | 2 out, D | 2 out, C | 2 out, F | 2 out, E | |
| Input jack | Aa | Ab | Ac | Ad | Ae | Af | |
| | 2 in, A | 2 in, B | 2 in, C | 2 in, D | 2 in, E | 2 in, F | |
| Enigma 2 | | | | | | | (arriving from $\genfrac{}{}{0pt}{}{A}{C}$) |
| | 2 out, A | 2 out, B | 2 out, C | 2 out, D | 2 out, E | 2 out, F | |
| Output jack | Ca | Cb | Cc | Cd | Ce | Cf | |
| | 2 in, B | 2 in, A | 2 in, D | 2 in, C | 2 in, F | 2 in, E | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 3 out, F | 3 out, D | 3 out, E | 3 out, B | 3 out, C | 3 out, A | |
| Input jack | Ca | Cb | Cc | Cd | Ce | Cf | |
| | 3 in, A | 3 in, B | 3 in, C | 3 in, D | 3 in, E | 3 in, F | |
| Enigma 3 | | | | | | | (arriving from $\genfrac{}{}{0pt}{}{C}{E}$) |
| | 3 out, A | 3 out, B | 3 out, C | 3 out, D | 3 out, E | 3 out, F | |
| Output jack | Ea | Eb | Ec | Ed | Ee | Ef | |
| | 3 in, F | 3 in, D | 3 in, E | 3 in, B | 3 in, C | 3 in, A | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 4 out, C | 4 out, E | 4 out, A | 4 out, F | 4 out, B | 4 out, D | |
| Input jack | Ea | Eb | Ec | Ed | Ee | Ef | |
| | 4 in, A | 4 in, B | 4 in, C | 4 in, D | 4 in, E | 4 in, F | |
| Enigma 4 | | | | | | | (arriving from $\genfrac{}{}{0pt}{}{E}{F}$) |
| | 4 out, A | 4 out, B | 4 out, C | 4 out, D | 4 out, E | 4 out, F | |
| Output jack | Fa | Fb | Fc | Fd | Fe | Ff | |
| | 4 in, C | 4 in, E | 4 in, A | 4 in, F | 4 in, B | 4 in, D | |

Fig. 63. Spider connections with Enigma for 6 letter alphabet and crib $\begin{matrix}1&2&3&4&5\\A&C&E&F&F\\F&A&C&E&C\end{matrix}$

alphabets $\begin{matrix}1&2&3&4&5\\AF&AB&AF&AC&FC\\BD&CD&BD&BE&BE\\EC&EF&DE&DF&DA\end{matrix}$. Names of contact are given in purple ink, contacts to which they are connected in green. Connections of diagonal board to Enigmas Fig. 64.

[ 114 ]

| | | | | | |
|---|---|---|---|---|---|
| Aa<br>1 out, A<br>2 in, A | Ab Ba<br>1 out, B<br>2 in, B | Ac Ca<br>1 out, C<br>2 in, C | Ad Da<br>1 out, D<br>2 in, D | Ae Ea<br>1 out, E<br>2 in, E | Af Fa<br>1 out, F<br>2 in, F |
| Ba Ab | Bb | Bc Cb | Bd Db | Be Eb | Bf Fb |
| Ca Ac<br>2 out, A<br>3 in, A<br>5 out, A | Cb Bc<br>2 out, B<br>3 in, B<br>5 out, B | Cc<br>2 out, C<br>3 in, C<br>5 out, C | Cd Dc<br>2 out, D<br>3 in, D<br>5 out, D | Ce Ec<br>2 out, E<br>3 in, E<br>5 out, E | Cf Fc<br>2 out, F<br>3 in, F<br>5 out, F |
| Da Ad | Db Bd | Dc Cd | Dd | De Ed | Df Fd |
| Ea Ae<br>3 out, A<br>4 in, A<br>Input A,<br>current enters | Eb Be<br>3 out, B<br>4 in, B<br>Input B<br>(relay) | Ec Ce<br>3 out, C<br>4 in, C<br>Input C | Ed De<br>3 out, D<br>4 in, D<br>Input D | Ee<br>3 out, E<br>4 in, E<br>Input E | Ef Fe<br>3 out, F<br>4 in, F<br>Input F |
| Fa Af<br>4 out, A<br>1 in, A<br>5 in, A | Fb Bf<br>4 out, B<br>1 in, B<br>5 in, B | Fc Cf<br>4 out, C<br>1 in, C<br>5 in, C | Fd Df<br>4 out, D<br>1 in, D<br>5 in, D | Fe Ef<br>4 out, E<br>1 in, E<br>5 in, E | Ff<br>4 out, F<br>1 in, F<br>5 in, F |

Fig. 64. Connections of diagonal board. See Fig. 63. ‘Input’ is at E. Correct hypothesis E/A. The square in this figure represents contacts. As in Fig. [63] the purple letters are names and green letters shew the contacts to which they are connected.

[ 115 ]

entering at a correct Stecker if the position is correct. Let us further simplify the problem by supposing that there is only one ‘web’, i.e. that the ‘picture’ formed from the part of the crib that is being used forms one connected piece, e.g. with the crib on p [*missing, presumably 97*] we should have one web if we omit the constatations

$\overset{P}{B}, \overset{B}{U}, \overset{U}{O}, \overset{R}{H}.$

Some of the constatations of the web could still be omitted without any of the letters becoming disconnected from the rest. Let us choose some set of such constatations, in such a way that we cannot omit any more constatations without the web breaking up. When the constatations are omitted there will of course be no ‘chains’ or ‘closures’. This set of constatations may be called the ‘chain-closing constatations’ and the others will be called the ‘web-forming constatations’. At any position we may imagine that the web-forming constatations are brought into play first, and only if the position is possible for these are the chain-closing constatations used. Now the Stecker value of the input letter and the web-forming constatations will completely determine the

Stecker values of the letters occurring in the web. When the chain closing constatations are brought in it will already be completely determined what are the corresponding 'unsteckered' constatations, so that if there are c chain-closing constatations the final number of stops will be a proportion $26^{-c}$ of the stops which occur if they are omitted. Our problem reduces therefore to the case in which there are no closures. It is, I hope, also fairly clear that the number of stops will

[ 116 ]

not be appreciably affected by the branch arrangement of the web, but only by the number of letters occurring in it. These facts enable us to make a table for the calculation of the number of stops in any case where there is only one web. The method of construction of the table is very tedious and uninteresting. The table is reproduced below

| No. of letters<br>on Web | H-M factor[6] |
|---|---|
| 2 | 0.92 |
| 3 | 0.79 |
| 4 | 0.62 |
| 5 | 0.44 |
| 6 | 0.29 |
| 7 | 0.17 |
| 8 | 0.087 |
| 9 | 0.041 |
| 10 | 0.016 |
| 11 | 0.0060 |
| 12 | 0.0018 |
| 13 | 0.00045 |
| 14 | 0.000095 |
| 15 | 0.000016 |
| 16 | 0.0000023 |

No. of answers = $26^{4-c}$ × H-M factor
c is number of closures

A similar table has also been made to allow for two webs, with up to five letters on the second. To the case of three webs it is not worth while and hardly possible to go. One can often get a sufficiently good estimate in such cases by using common-sense inequalities, e.g. if we denote the H-M factor for the case of webs with m, n, and p letters by H(m,n,p) we shall have the common-sense inequalities

$$\frac{H(m,3,2)}{H(m,0,0)} < \frac{H(m,3,0)}{H(m,0,0)} \cdot \frac{H(m,2,0)}{H(m,0,0)}$$

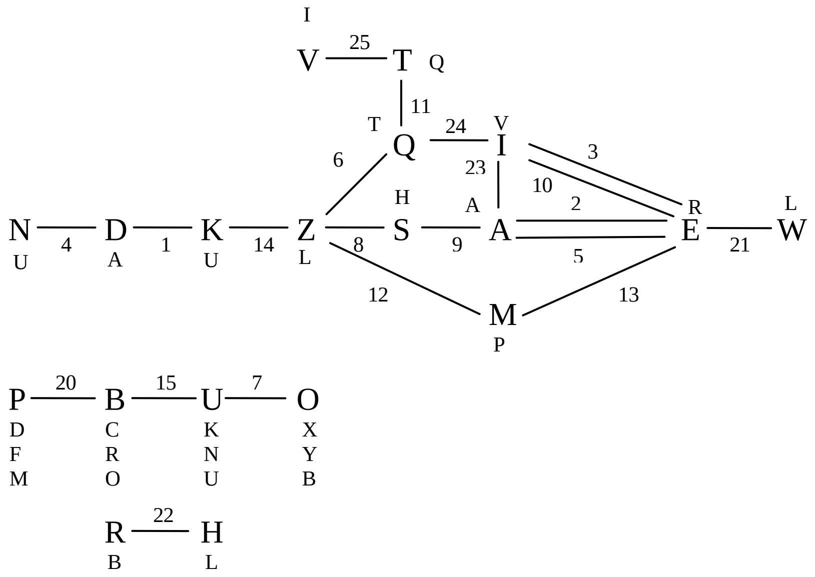
$$H(m,3,2) > H(m,4,0)$$

[6] Editors' Note: In the PRO copy there is a hand-written note, written by Joan Murray (formerly Joan Clarke of Hut 8), explaining that H-M stands for Holland-Martin of the British Tabulating Machine Company.

[ 117 ]

To see what kind of contradictions are detected by the machine we can take the picture, Fig. 59 and on it write against each letter any Stecker values of that letter which can be deduced from the Stecker hypothesis which is read off the spider when it stops. This has been done in Fig. 65 for a case where the input was on letter E of the diagonal board, and the relay R closed when the machine stopped; if the position of the stop were correct at all the correct Stecker would be given by the points of the diagonal board which were connected to Er, and they will also be the direct consequences of the Stecker hypothesis E/R. As we are assuming that R was the only relay to close this relay cannot have been connected to any of the others, or it would have behaved similarly. We cannot therefore deduce any other Stecker value for E than R, and this explains why on the ‘main web’ in Fig. 65 there is only one pencil letter against each ink letter. Wherever any pencil letter is the same as an ink letter we are able to write down another pencil letter corresponding to the reciprocal Stecker or to the diagonal connections of the board. In one or two cases we find that the letter we might write down is there already. In others the new letter is written against a letter of one of the minor webs; in such a case we clearly have a contradiction, but as it does not result in a second set of pencil letters on the main web the machine is not prevented from stopping. There are other contradictions; e.g. we have Z/L, W/L, but as L does not occur in the crib this has no effect.

[ 118 ]



Relevant parts of alphabets

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| AU | AR | RV | AU[7] | AR | TL[8] | KX<br>NY<br>UB | LH | AH |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| RV | QT | LP | PR[9] | LU | CK<br>RN<br>OU | | | |
| 19[10] | 20 | 21 | 22 | 23 | 24 | 25 | | |
| | DC<br>FR<br>MO | RL | BL | AV | TV[11] | | | |

Fig. 65. Illustrating the kind of position at which the spider will stop. Here the input letter may be supposed to be E and the relay which closed R. The Stecker values of the letters, which are consequences of the hypothesis E/R are written against the letters. There are contradictions such as Z/L, W/L: P/D, P/F, P/M which are not observed by the spider.

[7] Editors' Note: Originally ND, but ND are the menu letters. Should be AU.

[8] Editors' Note: Originally QL, should be TL.

[9] Editors' Note: Originally ME, but ME are the menu letters. Should be PR.

[10] Editors' Note: The table in the Treatise has column 20 positioned under column 19 and all the subsequent column shifted one place to the left with a column 26 added to the end. This is clearly an error. There is no column 19 in this menu as the four constatations 16 to 19 have been left out as explained on page 98 due to the turnover hypothesis selected.

[11] Editors' Note: Originally QI, but QI are the menu letters. Should be TV

[ 119 ]

## The machine gun

When using the spider there is a great deal of work in taking down data about stops from the machine and in testing these out afterwards, making it hardly feasible to run cribs which give more than 5 stops per wheel order. As the complete data about the direct consequences of any Stecker hypothesis at any position are already contained in the connections of the points of the diagonal board it seems that it should be possible to make the machine do the testing itself. It would not be necessary to improve on the stopping arrangement of the spider itself, as one could use the spider as already described, and have an arrangement by which, whenever it stopped a further mechanism is brought into play, which looks more closely into the Stecker. Such a mechanism will be described as a machine gun, regardless of what its construction may be.

With almost any crib the proportion of spider stops that would be passed by a machine gun as possible would be higher than the ratio of spider stops to total possible hypotheses. Consequently the amount of time that can economically be allowed to the machine gun for examining a position is vastly greater than can be allowed to the spider. We might for instance run a crib which gives 100 spider stops per wheel order, and the time for running, apart from time spent during stops might be 25 minutes. If the machine gun were allowed 5 seconds per position, as compared with the spider’s 1/10 second only 8 minutes would be added to the time for the run.

[ 120 ]

When the spider stops, normally the points of the diagonal board which are energised are those corresponding to supposedly false Stecker. Naturally it would be easier for the machine gun if the points energised corresponded to supposedly correct Stecker. It is therefore necessary to have some arrangement by which immediately after the spider stops the point of entry of the current is altered to the point to which the relay which closed was connected, or is left unaltered in the case that 25 relays closed. Mr. Keen has invented some device for doing this, depending entirely on relay wiring. I do not know the details at present, but apparently the effect is that the machine does not stop at all except in cases in which either just one relay closes or 25 relays close. In the case that 25 relays close the current is allowed to continue to enter at the same point, but if just one relay closes the point of entry is changed over to this relay. This method has the possible disadvantage that a certain number of possible solutions may be missed through not being of normal type. This will only be serious in cases where the frequency of spider stops is very high indeed, e.g. 20%, and some other method, such as ‘Ringstellung cut-out’ is being used for further reducing the stops. An alternative method is to have some kind of a ‘scanner’ which will look for relays which are not connected to any others. Which method is to be used is not yet decided*.

At the next stage in the process we have to see whether there are any contradictions in the Stecker; in order to reduce the number of relays involved this is done in stages. In the first stage we see whether or not there are two different Stecker

* Now has been decided to use scanner.

values for A, in the second whether there are two different values for B, and so on. To do this testing we have 26 relays

[ 121 ]

which are wired up in such a way that we can distinguish whether or not two or more of them are energised. When we are testing the Stecker values of A we have the 26 contacts of the A line of the diagonal board connected to the corresponding relays in this set. What is principally lacking is some device for connecting the rows of the diagonal board successively to the set of relays. This fortunately was found in post-office standard equipment; the clicking noise that this gadget makes when in operation gives the whole apparatus its name. If we find no contradictions in the Steckers of any letter the whole position is passed as good. The machine is designed to print the position and the Stecker in such a case. Here again I do not know the exact method used, but the following simple arrangement seems to give much the same effect, although perhaps it could not be made to work quite fast enough. The Stecker are given by typing one letter in a column headed by the other. When any letter is being tested for Stecker contradictions the relays corresponding to the Stecker values of the letter close. We can arrange that these relays operate corresponding keys of the typewriter, but that in the case that there is a contradiction this is prevented and some special symbol is typed instead shewing that the whole is wrong. When no relay closes nothing is typed. The carriage of the typewriter is not operated by the keys but only by the space bar, and this is moved whenever there is a change of the letter whose Stecker are being examined.

[ 122 ]

## Additional gadgets

Besides the spider and machine-gun a number of other improvements of the Bombe are now being planned. We have already mentioned that it is possible to use additional data about Stecker by connecting up points of the diagonal board. It is planned to make this more straightforward by leading the points of the diagonal board to 325 points of a plug board; the plug board also has a great many points all connected together, and any Stecker which one believes to be false one simply connects to this set.

Another gadget is designed to deal with cases such as that in which there are two ‘webs’ with six letters and no chains on each. A little experiment will shew that in the great majority of cases with such data, when the solution is found, the Stecker value of a letter on either web will imply the whole set of Steckers for the letters of both webs: in the current terminology, “In the right place we can nearly always get from one web onto the other”. If however we try to run such data on the spider, even with the machine gun attachment, there will be an enormous number of stops, and the vast majority of these will be cases in which “we have not got onto the second web”. If we are prepared to reject these possibilities without testing them we shall not very greatly decrease the probability of our finding the right solution, but very greatly reduce the amount of testing to be done. If in addition the spider can be persuaded not to stop in these positions, the spider time saved will be enormous. Some arrangement of this kind is being made but I will not attempt to describe how it works.

With some of the ciphers there is information about the Ringstellung (Herivelismus) which makes certain stopping

[ 123 ]

places wrong in virtue of their position, and not of the alphabets produced at those positions. There is an arrangement, known as a ‘Ringstellung cut-out’ which will prevent the machine from stopping in such positions. The design of such a cut-out clearly presents no difficulties of principle.

There are also plans for “majority vote” gadgets which will enable one to make use of data which is not very reliable. A hypothesis will only be rejected if it contradicts three (say) of the unreliable pieces of data. This method may be applied to the case of unreliable data about Stecker.

[Pages 124 – 128 missing][12]

[12] Editors’ Note: The pages 124 to 128 are missing from the archive copy of the original. This includes the PRO copy.