10

NOTE ON POSSIBLE DEVELOPMENTS.

1. A letter is encoded on a German enigma machine by depressing a typewriter key which causes one or more of the three wheels to turn over. The actual encoding takes place after the turn over has taken place. The exact nature of the turn over depends on the positions of the middle and outer wheels, each of which has one special position which is known as its turn over position. (Wheels 6,7,8, have two turn over positions, but we shall not be concerned with these wheels in this note.) When a key is depressed there are three possibilities :-

    1. If neither the middle nor the outer wheel is in its turn over position, the outer wheel turns over and the other two wheels remain stationary.

    2. If the outside wheel is in its turn over position and the middle wheel is not, the middle and outside wheels turn over and the inside wheel remains stationary.

    3. If the middle wheel is in its turn over position, all three wheels turn over.

This turn over mechanism differs from the ordinary cyclometer mechanism in that all three wheels turn over whenever the middle wheel is in its turn over position, regardless of the position of the outside wheel.

The turn over position of a wheel is not determined by the absolute position of the wheel but by the position of the alphabet, whose setting relative to the wheel depends on the ringstellung. Thus, whatever the ringstellung may be, wheel 5 will always be in its turn over position when the letter Z is showing in the window.

The turn over positions are :-

E for wheel	2
J for wheel	4
Q for wheel	1
V for wheel	3
Z for wheel	5

2. Our problem is always to find the key for the day, i. e. the wheel order, ringstellung and stecker. Suppose first that we are working on information derived from cillies.
Consider a particular cilli from which we know that the indicators OJM, SHT give the message setting EDC for a message whose text is HYBGD EGVVX ....
We can make use of this cilli in three ways.

A). It will give a reduction in wheel order, telling us perhaps that the middle wheel must be 2 or 4 and the outside wheel 1, 3 or 5. We express this by saying that the cilli gives wheel orders 24/135.

B). We know that, when the German machine is set according to the correct key and the wheels are turned to the position OJM, the encode of SHT will be EDC.
In fact we know that the letter pairings E-S, D-H, C-T occur in machine positions OJN, OJO, OJP unless wheel 4 is in the middle, when the positions will be PKN, PKO, PKP.

C). We know that, when the German machine is set to the right key and when the wheels are turned to the position EDC, the decode of the text will be the original German message. In fact, when we assume a wheel order, we know the letters which must have been showing in the windows when each letter of the text was encoded.

Of these A. is always helpful as it reduces the number of wheel orders to be tried, B. may help us to make up menus and C. may help us to test the stories which satisfy these menus. (A menu consists of a number of letter pairings which are to occur in machine positions with prescribed letters showing in the windows. For any assumed wheel order and ringstellung the further assumption that a letter of the menu is steckered to a particular letter will imply certain stecker of other letters of the menu, and we say that a story is obtained when the stecker so obtained are not contradictory. Thus a story consists of a wheel order, a ringstellung, and a number of stecker pairs which, as far as we can tell from the information contained in the menu, may be correct.)

3. When the whole key is known, the process of passing from the encoded text of the EDC message to the original clear text may be divided into three stages.

i Each letter of the text is replaced by its stecker.
ii This letter is put through the machine at the appropriate position and gives another letter, which we call a count letter.
iii This count letter is replaced by its stecker, which we call a tape letter. original clear text of the message.

When we find the correct story from a menu, we shall only know a limited number of stecker. We shall only be able to obtain the count letters corresponding to those message letters whose stecker are known and we shall only be able to obtain the tape letters corresponding to count letters so obtained whose stecker are known. But, provided that we can obtain a reasonable number of tape letters, we may be able to guess some of the missing ones and so to complete the solution. So a possible method of testing a story is to obtain all the tape letters given by the story (a process known as running a tape), to see if they look like letters of clear text, and to try to guess some of the missing letters.

As an example, suppose that the key is :-
Wheel order 5 2 3 Ringstellung (English) K M T
Stecker K/K, N/N, Q/Q, T/T, V/V, X/X

A/H, B/G, C/Z, D/Y, E/J, F/I, L/S, M/W, O/U, P/R.
Suppose that the actual decoding of the message begins as follows :-

Text of coded message :-**HYBGDEGVVXRUVFCIJYVKEUMQYSPUSKOTCLY**.....
Steckered text :- **ADGBYJ BVVXPOVIZFEDVKJOWQDLROLKUTZSD**.....
Count letters :- **COLR POQXNOSSLFJGJNJFNLNOSSXMFPAHGJN**.....
Tape letters :- **Z USPRUQXN ULLSIEBENNEINSNULLXWIRHABEN**.....

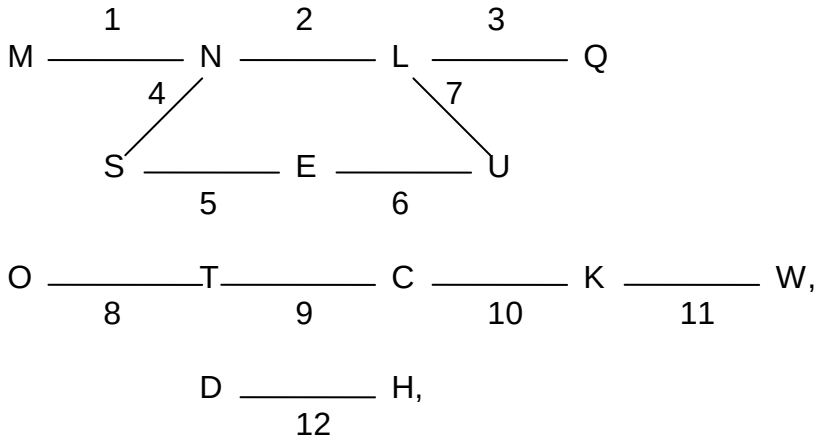
Inner wheel position :- **EEEEEEEEEEEEEEEEEEEEFFFFFFFFFFFFFFF**.....
Middle wheel position :- **DDDDDDDDDDDDDDDDDDEFFFFFFFFFFFFFFF**.....
Outer wheel position :- **DEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKL** .....

```
                    0         1          2         3
Place :-            1234567890123456789 012345678 9 0
```

Suppose also that we have four cillies.

i	Indicators	OJM, SHT	giving	message	setting	EDC	and	wheel	orders	24/135
ii	"	DTV, LKU	"	"	"	QWE	"	"	"	2413/35
iii	"	AAJ, TCN	"	"	"	OKL	"	"	"	524/13
iv	"	UVY, SNU	"	"	"	NML	"	"	"	3524/1352

We know from these cillies that the wheel order must be either _23 or _43. In fact we need only try six wheel orders, 123, 423, 523, 143, 243, 543. From these cillies we can obtain the menu :-



the machine positions being :-

1.	UVA		7.	UVB	
2.	AAM		8.	AAK	
3.	DUW		9.	OJP	FOR -23

4.	UVZ			PKP "	-43
5.	OJN for	-23	10.	AAL	
	PKN "	-43	11.	DUX	
6.	DUY		12.	OJO FOR	-23
				PKO "	-43

If this menu is run on Jumbo we shall obtain a large number of stories including the correct story, which will give wheel order 5 2 3, ringstellung KMT and stecker

M / W, N / N, L / S, Q / Q, E / J, U / O, T / T, C / Z, K / K.

We can run tapes on these stories, using the EDC message, and the tape obtained from the correct story would be :-

.....U.....L..E.E...NSNU.L.W.....E. etc.

This certainly looks as if it might be part of a German clear text and it would be easy to guess that

..NSNU.L

is really

EINSNULL,

from which the solution can be completed.

This example is rather a favourable one in that the cluster of letters NSNU.L is suggestive, but we can run a tape on the whole length of the EDC message and we should be most unlucky if the right tape did not contain a suggestive group of letters somewhere.
But although it should be easy to complete the solution once the correct tape is spotted, it may not be easy to discard all the wrong tapes. Jumbo would give about 500 stops and 136 stories for each wheel order, so that there would be in all over 800 tapes to run and examine.

The time factor is the most serious obstacle. The minimum time for a run on Jumbo is 20 minutes and we must add 11 seconds for each stop and 5 seconds for each story. The six wheel orders, run three at a time, would therefore take about 11 hours, excluding plugging and setting drums. At present we can only run tapes on an X-machine, and for each tape it is necessary to set the stecker and the ringstellung.
Even with a team of workers I doubt if more than 20 tapes could be run in an hour on one machine, so at least 40 hours work would be needed to do the job completely on one X-machine.
The time required to examine the tapes is difficult to guess.

6. It appears then that the four cillies we have been considering would give a theoretical solution but that with our present machinery this solution would take a great deal of time. It also seems evident that we cannot hope to deal with menus much weaker than the one we have considered, because the number of stories would be prohibitive. But we are sometimes able to make a shrewd guess at the ringstellung, and this makes a great deal of difference. Suppose for example that we only have the three cillies EDC, QWE and NML, allowing wheel orders 24 / 35. Then the menu :-

M — N — S — E — U — L—— Q

would give about 33,000 stories per wheel order, or about two per ringstellung. Since there are 12 wheel orders to try, we expect in all about 24 stories per ringstellung. If we could reduce the possible ringstellung to 3 x 3 x 3 = 27 we should have about 650 tapes. If we only had two cillies, EDC and NML, allowing the 18 wheel orders 24 / 135, the menu :-

E — S — N — M

would give about 15 stories per ringstellung for each wheel order, so we should have about 270 tapes to run for each ringstellung assumption.

7. In this last example the correct story, E / J, S / L, N / /N, M / W only gives the stecker of seven letters, so very few letters will show on the tape. We should only expect on e letter in thirteen places and the beginning of the tape would actually be :-

……E…N.N..L…….E.

Although it might be possible to finish the solution if one knew which was the right tape, it would clearly be difficult to pick out the right one from a large number of tapes. This difficulty can be overcome by taking counts instead of running tapes. In this last example, when a story can only be expected to give the stecker of about seven letters, we should expect to obtain about one count letter for every four letters of text. The count letters obtained from a false story will be a random selection of the 26 letters of the alphabet but those obtained from the correct story will be a random selection from the stecker of letters of the German clear text and therefore have a language distribution. Suppose then that for each story, instead of examining the tape letters, we examine the count letters and count the number of times each letter of the alphabet occurs as a count letter. Suppose that the letters A, B, C ....Z occur as count letters n1, n2, n3, ..., n26 times and that

$$n_1 + n_2 + n_3 + \ldots\ldots + n_{26} = N$$

If we calculate the value of

$$\frac{\Sigma\, n(n-1)}{N\,(N-1)}$$

we should expect to obtain about 1 /15 for a language distribution and about 1 /26 for a purely random distribution.

This test for a language distribution is surprisingly effective. It is even possible to find a solution with only one cilli, provided that we can reduce the ringstellung to two or three and provided that the cilli message is long enough. But the efficiency of the test depends on the number of letters in the count (i.e. the value of N) and on the number of stories to be tested. When a good count is obtained the next stage is to try to guess other stecker which give counts fitting in with the language distribution of the original count. When there are a lot of stories and the value of N is not large, there is a danger that a good many false stories may give good

counts and that the process of finding the right count may take a prohibitive amount of time. It is difficult to disprove a good count which arises from a false story.

8.

In dealing with a particular problem we can calculate the number of stories that are to be expected and the number of stecker that each story is likely to give. We should then be able to calculate the length of message on which we must run a tape or take a count in order to be able to pick out the right story from the wrong ones. Unfortunately we shall not be able to make this second calculation until we have had experience of large numbers of tapes and counts. Finally we shall have to calculate the time that the operation will take, and decide whether it is practicable. In choosing between tapes and counts the following considerations must be borne in mind. When a good knowledge of the ringstellung enables us to use a very weak menu, such as an open three chain, the stories will give too few stecker for tapes and we must use counts. When we have no knowledge of the ringstellung we shall only be able to use fairly strong menus: when the menus contain a lot of letters the stories which arise will give a lot of stecker and it will probably be more profitable to run tapes. In intermediate cases, when tapes would show up the solution, it may be quicker to take counts because a shorter length of message would be needed.

9. There is another important fact that has not yet been mentioned. We know that of the 26 letters, six are self steckered while the remaining 20 are steckered to ten pairs. In fact rather less than a quarter of the letters are self steckered. Thus, when a menu contains a long chain we shall only be taking a small risk if we assume that one, two, or possibly three letters of the chain are self steckered. Also when a menu contains a main chain and a subsidiary chain, both of reasonable length, it will be highly probable that some letter of the main chain is actually steckered to some letter of the subsidiary chain. Thus in the example given above, in which the main chain contains seven letters and the subsidiary chain five, we could decide to take the risk of assuming that the correct story will involve the stecker of all letters of both chains and that at least two of these letters will be self steckered. At present we can do this in two ways. We can examine all the stories produced by Jumbo and select those which satisfy the assumption: this means that Jumbo will waste a lot of time producing stories that are not wanted. Alternatively we can assume first that one letter of the main chain, say M, is self steckered, which will divide the number of stops by 26; if this fails to produce a solution, we can then assume that N is self steckered and try again; if this fails we can assume L is self steckered and so on.

The subsidiary chain idea needs a little explanation.(⊕) Suppose the menu we have chosen as an example is run on Jumbo as a double input job with inputs at M and O. The majority of stops will occur in positions where there are straights on both inputs which are not connected through the diagonal board. For instance in a false position there may be straights on the p and y lines and the stecker M / P may involve N / E, L / B, Q / F, S / S, and U / Z. The straights on Oy will probably give a contradiction, for instance, O / Y may involve C / Z, but Jumbo cannot spot this contradiction because the stecker assumption M / P does not directly imply the stecker C / Z which contradicts U / Z.

11. What can we do about it ? There seem to be two possible developments.

1. To produce a super Jumbo which will work faster, which will make use of the probability of self stecker, and which will have some form of subsidiary chain control.

2. To produce a super test plate which will be capable of running a large number of tapes and of taking a large number of counts in a reasonable time.

We will consider these developments in turn.

SUPER JUMBO

12. The operations performed by the present Jumbo may be summarised as follows :-

(a) Preselected stopping :- A stop occurs when the input is not full, i.e. when some line of the input is not connected to all other lines.

(b) Scanning the input :- Each line of the input is inspected to find out whether there is a straight.

(c) Testing a straight :- With current entry on a line which has been found to give a straight, the machine gun examines each row of the diagonal board and looks for contradictions.

(d) Printing stecker :- When a story is obtained the stecker are typed out.

(e) Restarting :- After (c) or (d) the machine is automatically restarted.

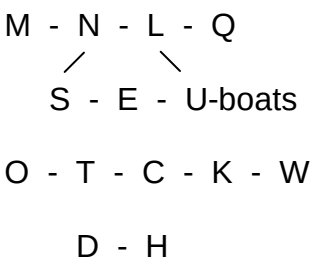
⌖ Sorry ! I am not explaining the subsidiary chain idea here, but I am pointing out that the double input method does not make full use of the subsidiary chain . See also page IX.

The times taken by the various operations are approximately :-

Stopping and restarting.....4 secs.
Scanning the input.....3 secs.
Testing a straight.....4 secs.
Printing a stecker.....5 secs.

In addition the time taken for a run without stops is about twenty minutes. Jumbo has three banks and each bank has to wait while the stops on the other banks are being investigated.

13. Consider again the menu :-



and suppose that it is being run as a single input job with input at M. For ordinary running the current enters the machine at an arbitrarily chosen line of the input, say the a - line. In any position the current reaches those points of the diagonal board which correspond to stecker implied by M / A. The existence of a straight on the y line of the input means that M / Y does not imply any other stecker of M, and the machine will detect the straight by the fact that current does not reach the y line of the input. In order to test the straight the machine must change the current entry from the a line to the y line of the input, so that the points of the diagonal board reached by the current will be those corresponding to stecker implied by M / Y. When this has been done, the machine gun can examine the rows of the diagonal board for contradictions of the form N / Z, E / Z.

If we had used the double input method, with the second input at O, Jumbo would only stop when a straight on the M input is accompanied by a straight on the O input. Suppose that at a particular stopping place there is one straight on each input, say on the y and x lines. Then the stop can only give the true story if all the stecker implied both by M / Y and by O / X involve no contradictions. Unfortunately it will very often happen that M / Y does not imply a stecker of any letter of the subsidiary chain, so that, when the current entry line is changed to My, Jumbo is unable to make use of the subsidiary chain and will consequently let through a number of false stories. However, if we are prepared to take the risk of assuming that some letter of the main chain is actually steckered to some letter of the subsidiary chain, we could reduce the number of stories by insisting that a story must involve stecker of the letters of the subsidiary chain. It could be arranged that the machine gun would discard a straight on My unless current reaches some point of the O row of the diagonal board when the current entry line is My. This stunt will be known as " subsidiary chain control" and can only be brought into action when the current entry is on the straight which is to be tested.

14. We will now consider what can be done when each point of the diagonal board is associated with a relay. Suppose first that we have 676 two point relays wired as follows.

In the diagram there are two sets of 26 terminals S and T, a battery B, a coil C and 676 relays A / A, A / B, ...Z / Z corresponding to the points of the diagonal board. When the relay A / B goes up, the terminal B of S is connected to the terminal A of T, unless some other relay in row A and to the right of A / B is also up. When two or more relays of the same row are up, current passes through the coil C but not otherwise.

If in any position of the super Jumbo we want to test a stecker assumption M / Y we must first arrange that the current entry line is My. All relays corresponding to stecker implied by M / Y will go up, and any contradiction causes current to pass through coil C. When there is no current through C the stecker can be recorded by disconnecting the battery circuit, putting current in at the terminals A, B, C.....Z of S and recording where the current comes out at T.

15. Two refinements are possible. Suppose we add three more points to the relays representing self stecker A / A, B / B,.....Z / Z and wire them as follows :-

Then, when we are testing the assumption M / Y , current from 1 will reach p if three or more self stecker are implied by M / Y, while the current will reach q, r or s if precisely two, one or no self stecker are implied. By this device, which I will call “diagonal selection”, we can reject any story which contains less than a prescribed number of self stecker. We can also introduce subsidiary chain control by insisting that current must pass from battery B via coil C to terminal O of T, which will happen if and only if M /Y implies a stecker of O.

16. It appears then that a stecker assumption can be thrown out instantaneously for any one of the following reasons :-

1. A contradiction.
2. Insufficient self stecker.
3. Failure to get on to a subsidiary chain.

Moreover this process can be done at the scanning stage and there is no need for uniselectors, even for printing out stecker. In fact we have arrived at a possible super Jumbo, which we call super Jumbo “A”, whose processes would be :-

(a) Stopping :- Exactly as on Jumbo. A stop indicates a straight on some line of the input.

(b) Scanning and testing :- The current entry line is moved to each line of the input in turn and the testing is done by the 676 relay circuit.

(c) Printing stecker :- With current entry on the line which gives the story the stecker are typed out by means of the sets of terminals S and T.

(d) Restarting :- As on Jumbo .

The times would probably be approximately :-

Stopping and restarting……4 secs.
Scanning and testing……3 secs.
Printing stecker……5 secs.

If we ran the menu straightforwardly on super Jumbo “A”, the 500 stops would take about 60 minutes and the 136 stories would take about 11 minutes more. Of course the super Jumbo would only have one bank, so each of the six wheel orders would have to be run separately and the time for the whole job excluding plugging and setting drums, would be about 9 hours. This is not a very sensational improvement on Jumbo’s time of 11 hours.

If we decide to use subsidiary chain control and to assume at least two letters of the 12 to be self steckered (the chances involved are about 3 to 1 and 8 to 1 on) the number of stories would be reduced from 136 per wheel order to about two per wheel order. But the number of stops would still be 500, so the running time for the whole job would only be reduced by an hour to 8 hours.

17. The trouble with super Jumbo "A" is that its refinements do not cut down the number of stops and only reduce the time taken by an ordinary stop from 11 SCEs. to 7 SCEs. Let us consider therefore whether it would be better to make a definite self stecker assumption M / M, and, if this fails, to try N / N, L / L, etc. When we assume M / M we can fix the current entry line at Mm for the whole run and reject every position which doe not give a story without stopping the machine, by means of the 676 relays. We can also use diagonal selection and subsidiary chain control while the machine is running. Also the machine would be less complicated than super Jumbo "A". The chief snag about the machine would be the difficulty of deciding how many assumptions M / M, N / N, etc. ought to be tried without success before failure is admitted. The process of the machine, which we will call super Jumbo "B", would be :-

(a) Preselected stopping :- The machine will only stop for a story. If desired it will only stop for a story which includes stecker of letters of a subsidiary chain and at least a prescribed number of self stecker.

(b) Printing stecker :- As before.

(c) Restarting :- As before.

The times would be :-

Stopping and restarting..... 4 secs.
Printing stecker..... 5 secs.

With our specimen menu and without diagonal selection or subsidiary chain control the machine would stop 13 times per run, so the time for a run would be about 22 minutes. So it would take 2 hours 12 minutes running time to try one self stecker assumption on the six wheel orders. If we use subsidiary chain control and assume at least two self stecker, the machine would stop less than once a run, so the running time would be reduced slightly.

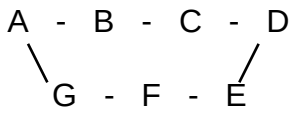
18. It appears then that our specimen menu neither of the super Jumbos would be a spectacular improvement on the present Jumbo. But suppose now that the link L-U is removed from the menu, so that the main chain becomes open. On Jumbo this weakened menu would give 13,000 stops and 3,300 stories, so the running time would be prohibitive.

Super Jumbo "A" could not avoid 13,000 stops, but Super Jumbo "B", using subsidiary chain control and assuming at least two self stecker, would only stop about seven times a run.

Thus for weak menus involving two chains of reasonable length super Jumbo "B" is a very powerful machine.

The same is true for menus consisting of a single chain. For example an open ten chain would give over 7,000 stops per wheel order on Jumbo or on super Jumbo "A"", while on super Jumbo "B" the number of stops per run would be about 70. By assuming two letters self steckered the number of stops could be reduced to about 36.

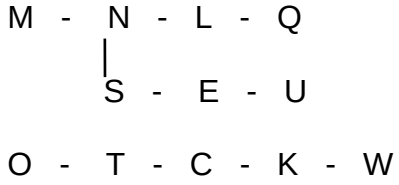
19. A further refinement of the idea of subsidiary chain control; might be worth while on super Jumbo “B”. Suppose that from four cillies it is only possible to make a menu of the form :-



H - I J - K L - M N - O P - Q,

i.e. a closed seven chain and five two chains. Although it would be unwise to assume that the correct story will get on to any particular two chain, it would be quite reasonable to assume that it will get on to some one or even on to two of the subsidiary chains, and this would considerably reduce the number of stories. If such an assumption were made, it would also be reasonable to assume that the correct story contains two self stecker.

20. It is worth considering yet another possible super Jumbo, “C”, which would use the principle of the assumed self stecker and would be able to make use of diagonal selection and subsidiary chain control but which would not need 676 relays. Consider the modified menu :-



on which machine “B” showed up so well. Suppose that we first assume M / M. With input at M and current entry line m we should arrange that the machine will only stop when then current does not reach any other line of the input, i.e. when there is a straight on Mm. We could quite easily arrange that the machine will only stop if the current reaches some point of the O row of the diagonal board and some self stecker point other than M / M. This give s us subsidiary chain control and diagonal selection. The procedure would be :-

(a) Preselected stopping :- The machine will only stop for a straight on Mm. If desired it will only stop for a straight which gets on to the subsidiary chain and which gives a prescribed number of self stecker.

(b) Testing : - The straights will be tested by a machine gun.

(c) Typing stecker :- Also by machine gun.

(d) Restarting :- As before.

The times would be :-

Stopping and restarting..... 4 secs.
Scanning and testing..... 4 secs.
Printing stecker..... 5 secs.

With the menu under consideration, using subsidiary chain control and diagonal selection as before, machine “C” would stop about 80 times and would produce the same stories as “B”,

i.e. about 7 per run. The time taken per run would therefore be about 31 minutes for “C” against 21 minutes for “B”, a 50% increase. For an open ten chain, machine “C” would stop about 120 times and give about 36 stories, so the time for a run would be about 39 minutes for “C” against 25 minutes for “B”, rather more than a 50% increase. In fact “B” is the better machine.

A SUPER TEST PLATE

21. In order to make use of cilli menus which are going to give a large number of stories we need a machine which will take counts and run tapes very quickly, Suppose that we are using the EDC message that we talked about earlier in this screed. Suppose also that we have a large number of stories on wheel order 1 2 3. In order to explain what the machine has to do we will imagine that the test plate enigma has drums similar to those of the hand enigmas, with moveable alphabets. Each story gives a ringstellung and a set of stecker. To run a tape, both input and output stecker must be set up according to the story, and the alphabets on the wheels must be set according to the ringstellung given by the story. The drums must then be set to EDD. The drums must turn in succession to the machine positions shown on page III, and in each position the machine must try to decode the corresponding letter, printing a dot when there is no decode. For taking a count the process is the same except that the output is self steckered and the letters which emerge are counted instead of being printed.

It is hoped to do this by two sets of cards, message cards and story cards. Whatever type of Jumbo is doing the job will record its stories on punched cards. When one of these cards is handed to the test plate the stecker will be automatically set up and the test plate enigma will be set at the right position for the first letter of the message. The letters of the text of the message will be recorded on another set of cards and as these pass through the machine the wheels will turn round, the current will go in at the right places, and the tape will be run or the count taken.

22. The turn over presents a difficulty. It is clear that the machine cannot do the business of setting the alphabet discs and then setting the wheels. It will have to set the wheels by rotating the shafts, so the wheels must be fixed relative to the shafts. Consequently the turn over control mechanism cannot be attached to the shafts, for the turn over does not depend on the position of the wheels but on the place in the message. In fact for wheel order - 2 3 the middle wheel must turn over immediately after places 19, 45, 71, etc., and in addition both middle and inner wheels must turn over after place 20. When wheel orders - 4 3 are being run the middle wheel must still turn over after places 19, 45, 71, etc., but the double turn over of both inner and middle wheels must take place after place 150.

23. Perhaps the setting and turn over mechanism can best be understood as follows :-

Suppose first that Jumbo has two sets of recording discs, A and B, the disc A having counter clockwise alphabets and the disc B having clockwise alphabets.
These discs are to rotate with Jumbo's drums. Suppose also that the super test plate has two sets of wheels P and Q. The first set of wheels P are ordinary enigma drums chosen from drums 1, 2, 3, 4, 5; they have fixed counter clockwise alphabets set to English ZZZ ringstellung. The second set of wheels Q are intended to control the turn over of the P wheels. they also have fixed counter clockwise alphabets and are chosen from five differently wired wheels Q1, Q2,.....Q5. Each of these wheels has one special position, called its "carry position" and these positions are :-

Q wheel		1	Q
"	"	2	E
"	"	3	V
"	"	4	J
"	"	5	Z

(These are of course the turn over positions of the German enigma wheels)

As a message is being run through the test plate, the sets of wheels P and Q move together and the turn over of both sets is regulated as follows :-

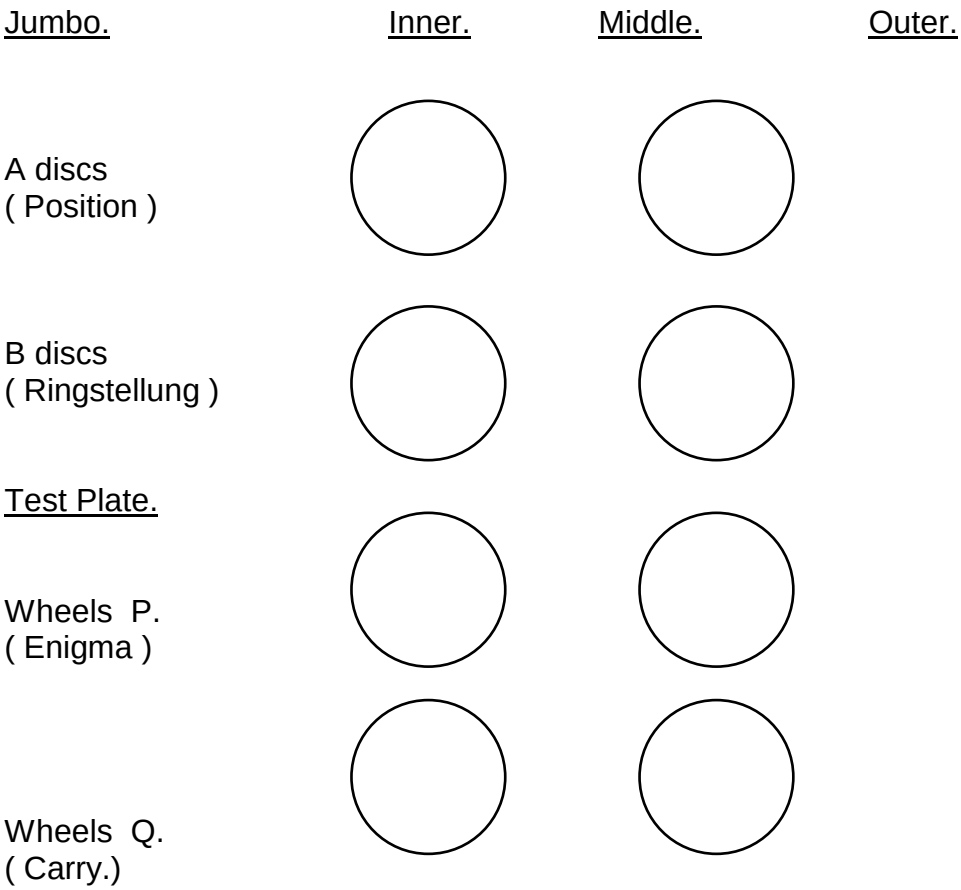
i If neither the middle nor the outer Q wheel is in its carry position, only the outer wheels turn over.

ii If the outer Q wheel is in its carry position, and the middle wheel is not, the middle and outer wheels turn over, while the inner wheels remain stationary.

iii If the middle Q wheel is in its carry position, all six wheels turn over.

(It will be noticed that the inner Q wheel does no work and may be ignored.)

The whole set up is as follows :-



When Jumbo is plugged up at the beginning of a run, the A discs are set to the position EDD, while the B discs give the Ringstellung, which is recorded on the story card, and the A discs give the position at which the P wheels of the test plate have to be set for the beginning of the message.

Suppose for example that the first two stories obtained on wheel order 1 2 3 give the readings :-

	A discs	B discs
1.	EFH	ZXV
2.	FIG	YUW

To test the stories on wheel order 1 2 3, P and Q wheels 1, 2 , 3 , are put on the test plate and both sets are first turned to position EDD. When the first story card is put in the machine, the P wheels are automatically reset at EFH, while the Q wheels remain at EDD. The message is then run off. When the second story is put into the machine, the P wheels must be automatically reset at FIG and the Q wheels at EDD, when the message will be run through again. In fact every time a new story card is put in, the Q wheels are always reset to the same position EDD, while the P wheels are set to certain distances from the original setting EDD, these distances depending on the ringstellung recorded by the B discs of Jumbo. The actual readings of the P wheels are those of the A discs of Jumbo when the story was obtained.

The A discs on Jumbo have only been introduced to assist the explanation. They will not exist on the actual machine. Also, as has already been pointed out, only two of the Q wheels are actually needed, the middle and outer ones.

SUPER JUMBO AGAIN

24. So far we have been thinking of our super Jumbo as a machine for trying all the 17576 possible ringstellung, and of course this will be its main job. But we should also like to be able to use the machine in the following way.

Suppose that we have only the one cilli EDC giving 18 wheel orders 24 / 135, but that we have good reason for supposing that the German ringstellung is either NNU or. NNV. (For wheel order 5 2 3 German NNU is English KMT.) We can only produce the menu :-

E - S, D - H, C - T,

We should like to be able to set up the super Jumbo according to this menu, turn it to the two ringstellung positions, and in those positions only make it record on punched cards the stories arising from each of the stecker assumptions

E / A, E / B,.....E / Z

D / A, D / B,.....D / Z
C / A, C / B,.....C / Z

These stories could then be tested by taking counts on the super test plate and the correct stories should stand out provided that the EDC message is long enough.
In our example there would be three correct stories,

1)	E / J	S / L
2)	D / Y	M / A
3)	C / Z	T / T.

25. Incidentally it is obvious that a Super Jumbo could be made to run a tape on a short stretch of a message, but it hardly seems worth arranging for this because it would only be useful in a few cases and the super test plate will do the job.

CRIBS.

26. So far we have only been considering menus derived from cillies. It is clear that super Jumbo "B" would also be very useful for weak crib menus, but it is not so easy to apply tapes and counts to crib menus. Suppose for example that we have the crib :-

Z U S P R U Q X N U L L
H Y B G D E G V V X R U

but we do not know that the message setting is EDC.
We can make up the menu :-

Suppose first that we have no idea of the ringstellung. We have no idea of the position of the turn over in the message and we simply have to hope that there is no turnover of the middle wheel during the stretch of the crib. Accordingly we make up the menu on the assumption that the machine positions are ZZA, ZZB, ..., ZZL with some ringstellung. We take the assumptions D / D, R / R, L / L, ... in turn and we can assume that the true story will get on to one of the three subsidiary chains and that it will involve at least one other self stecker.

At the beginning of the run suppose that the discs A and B are set to ZZA and ZZZ. Suppose that the first two stories occur in positions in which the discs read :-

	A discs	B discs
1.	ZCF	ZWU
2.	BFB	XTY

Then in order to test the stories by running tapes on the whole message, the starting positions of the P wheels of the super Test Plate must be ZCF and BFB.

The trouble is that we do not know where the turn over is in the message. Suppose that we make the test plate turn over after places 26, 52, 78, ... with no triple turn over. Suppose also that we make the machine type out the tape in rows of 26. Of course each tape will start off with some of the letters

Z USPRUQXNULL.

We have already assumed that there is no middle wheel turn over in this stretch, so in the tape arising from the correct story the letters which occur under this stretch, i.e. in the first 12 places of each row of the tape, will be correct unless there happens to be a triple turn over. We shall therefore have a good chance of finding the correct story if we only examine the first twelve letters of each row of the tape.

We can run tapes in this way with the mechanism described in para. 23 as follows:-

Suppose the stories are on wheel order 5 2 3.
The P wheels are then wheels 5, 2 and 3 and are set to position ZZA. Only one Q wheel is used; it is put on the outer shaft and set to the position immediately after its carry position. (For example, if the second Q wheel is used, its carry position is E, so it should be set to F). The machine is then run exactly as before.

If we are unlucky and a triple turn over takes place in the message, as actually happens in the example, then after this triple turn over the inner and middle wheels should each be one place further on than we have supposed. We could allow for this possibility by running another set of tapes with the P wheels set to AAA instead of ZZA.

We can only take counts effectively by arranging that letters are only counted in the positions of the machine corresponding to the first twelve places of each row of the tape. This can easily be done by inserting dummy message cards for the message letters that are not to take part in the count.

Suppose now that, in addition to the short crib we have a good knowledge of the ringstellung. This means that we are no longer obliged to take risks with the turn over, but it also means that we must use the super Jumbo and the super test plate rather differently. On the super Jumbo, provided that the outer wheels are the slow moving ones, we can allow for the turn over by changing the menu during the run. On the super test plate we do not require the carry wheels because we knows the turn over position of each of the enigma wheels. We only need to be able to set the turn over positions of the P wheels by means of plugs. We can then run tapes or take counts over the whole message.

Usually we shall only have an approximate knowledge of the ringstellung, but this will only mean that we shall have to be rather cunning in the way we use the machine in certain parts of the ringstellung range.

SUMMARY

28. It seems that we should go for the 676 relay super Jumbo, that we have called “B”, and for a super test plate that will run tapes and take counts. Incidentally I spoke of 676 relays in order to make the diagram easy to draw. As pairs of relays such as A / B and B / A always operate together, each pair of two point relays can be replaced by one four point relay. The required features are :-

Super Jumbo :-

One bank only.
Ringstellung cut out, but all wheels to English ZZZ.
Consecutive stecker shorting, but no stecker board.
Current entry on an assumed stecker. No scanning.
676 relays or their equivalent.
Alternative subsidiary chain control. (A story must get on to one or two of a number of subsidiary chains.)
Diagonal selection. (A story must include at least a prescribed number of self stecker.)
Preselected stopping only comes into operation when the assumed stecker

i implies no contradiction.
ii implies stecker of the letters of one or two of a number of subsidiary chains.
iii implies a prescribed number of self stecker.

Recording of stories on cards by punching and printing.
(Ringstellung recording is preferable to position recording.)

Normally one assumed self stecker will be tried in all positions of the bombe, i.e. on a complete run.

Sometimes we shall only want to investigate a few positions of the bombe and in each of these positions we shall want to record the stories obtained by assuming that a particular letter is steckered in turn to A, B, C,.....Z.

The inner enigma wheels are to be the fast moving ones, and any device which enables the wheels to be reset accurately during a run will be a great advantage.

Super Test Plate
Setting of enigma drums and stecker by insertion of a story card.
Current entry line in successive positions of the enigma to be controlled by a set of message cards.

Tape running :- Both input and output stecker to be set up by the story card. The letters that come out of the enigma to be typed in rows of 26, with dots to represent missing letters.

Count taking :- Only the input stecker to be set up by the story card. The output to be self steckered. The letters that come out of the enigma to be counted.

Turn Over :- Two alternatives for controlling turn over are required :-

1. The method which makes use of carry wheels (or an equivalent method). These carry wheels must be automatically reset to a prescribed zero position, whenever a new story card is inserted. The enigma wheels also have zero positions, but when a story card is inserted the enigma wheels are set at certain distances from their zero position, these distances being different for different stories, whereas the carry wheels are always set to their zero positions. In fact the relative distance between the setting of each carry wheel and the corresponding enigma wheel is changed by the insertion of a story card.

2. Control by plugs which fix the turn over positions of the enigma wheels.

1.9.41.