-

6812TH SIGNAL SECURITY DETACHMENT (PROV)
APO 413 US ARMY

15 June 1945

The following is a brief description or the operations of the 6812th Signal Security Detachment in the European Theater of Operations from 1 February 1944 to 7 May 1945.

It was necessary to completely train the operators, engineers and technicians before the work could be begun. The contents of the following pages had to be thoroughly understood by each man.

The 6812th reached a degree of efficiency far above the greatest expectations. When operations ceased on VE day the Detachment was averaging in output runs per day approximately 38 o/o above that of the British units engaged in the same work. This seems almost incredible when it is understood that the British had the benefits of four years of experience. From the beginning of operations to VE Day the 6812th Signal Security Detachment found the solutions to a total of 425 German Enigma Keys.

DECODING GERMAN ENIGMA MACHINE MESSAGES

CHAPTERS.

Chapter I. Theory of Decoding and Decoding Machines.

Table of Contents .

DECODING ENIGMA MACHINE MESSAGES

1,October,1944.

DESCRIPTION OF ENIGMA MACHINE.

The Enigma machine is a portable, self contained cryptographic device used to encode or decode letter by letter in a reciprocal substitution system. Its three main elements are keyboard, stecker board(patch board) and Enigma wheel maze. The machine looks as shown.

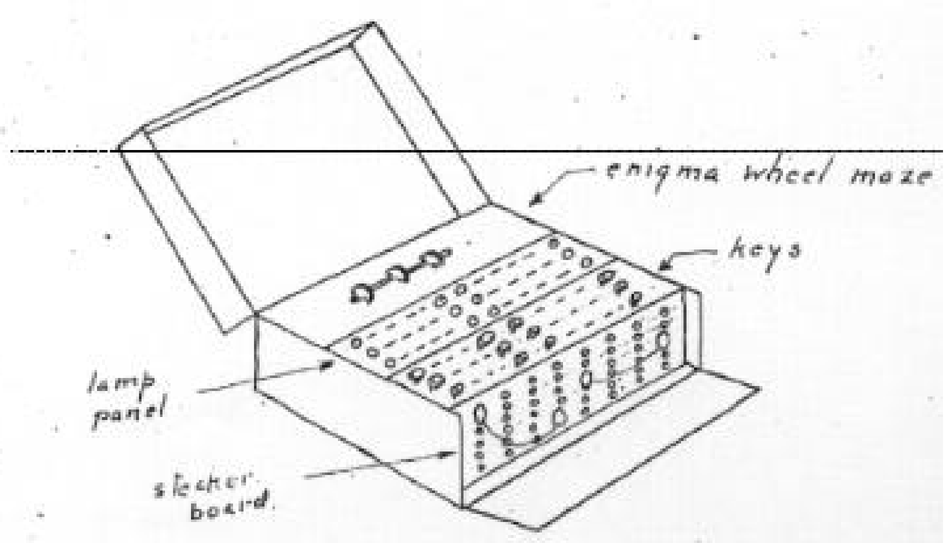


Fig. 1. Enigma Machine.

The keyboard consists of 26 typewriter type keys. The stecker board is made up of a total of 26 pairs of jacks arranged in 3 rows. Each pair includes one large and one small jack to permit inserting the plug in only one direction, The patching cords are two conductor cords equipped at each end with a plug with two prongs of unequal diameter. The enigma wheel maze consists of a current supply commutator, 3 movable wheels having 26 contacts on one face of the wheel cross connected to 26 contacts on the opposite face, and a reversing unit called an Umkehwalz (Uncle Walter). Two other move- able wheels are carried in a separate carrying case. The wheels look as shown.

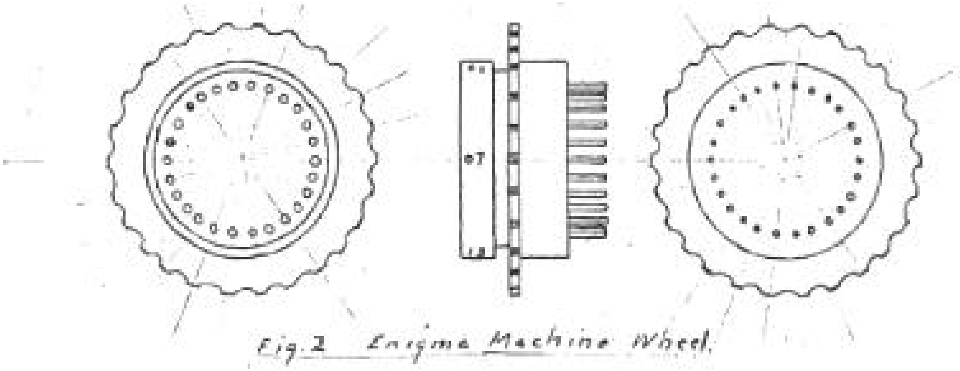


Fig.2 Enigma Machine Wheel.

Miscellaneous features include a rack for spare lamp bulbs ,a holder for the message being encoded or decoded, a holder for 2 spare cords, a shield to put over the lamp when it is desired to suppress the light from the set, and arrangements for testing lamps and cords.

PREPARATION OF ENIGMA MACHINE FOR OPERATION.

The operator of the enigma machine is supplied with a key sheet which specifies the Wheel Order, Ringstellung, and Stecker Board arrangement to be used each day. The key sheet reads horizontally each day and from bottom to top for successive days of the month. When the data for a day has been used, it is cut off and destroyed, so that in case of capture the data for previous days messages will

not be available to the enemy. From the information Wheel Order it is determined what 3 of the 5 available wheels shall be used for the day in question, and in what order they shall be inserted in the machine. The enemy army and air force use 3 out of 5 wheels, whereas the navy uses 4 out of 8 wheels. The data Ringstellung tells the operator at what point to set the tire or Ringstellung on the wheel. This tire is moveable when a catch is disengaged and may be set in any one of 26 positions. The rim of the tire is engraved with the numerals Ol to 26. The Stecker Board information on the key sheet tells the operator what letters are to be patched together. Certain letters are left unpatched in which case they are referred to as "self steckered" meaning that the elements of the twin jack are connected together by a short circuiting bar within the jack; The number of "self-steckered" letters usually does not exceed 6.

OPERATION OF THE ENIGMA MACHINE.

The operator presses a clear text key and reads the code letter from the lighted lamp for the encoding procedure, and vice versa for decoding.

The circuit operation of the machine is quite simple. When a key is depressed a mechanical linkage advances one or more wheels before any electrical circuits are closed. The number of wheels advanced depends on the position of an indentation on the tire of each wheel. To advance the second wheel the driving pawl must be able to drop into the indentation of the first wheel. Similarly for the third wheel. When the key is still further depressed an electrical circuit is closed as shown.

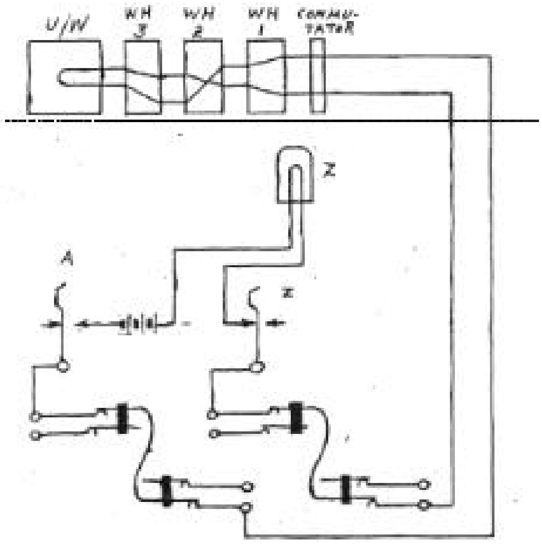


Fig 3. Enigma Machine Circuit.

"A" lamp cannot be lighted from the "A" key, etc., due to the breaking of the lamp circuit by the depression of key "A".

EMERGENCY STECKER BOARD PATCHING.

The operator is provided with am emergency method of obtaining stecker board patching to be used if the key sheet should be compromised. A word is furnished in advance. Let us assume the word is Christensen. He is instructed to write the first line of a square, using the alternate letters beginning with the first without repeating letters. He then builds the rest or the square row by row from the remaining letters or the alphabet.

```
CRSEN
ABDYG            NGLTYCAHMUZRB
HIJKL            IOVSDJPWEFKQX
MOPQT
UVWXY
Z
```

Beginning with the top letter of the last column he then writes the letters in two horizontal rows. The stecker board couplets then read vertically as N/I, G/O &.

SECURITY OF THE ENIGMA MACHINE.

The enigma machine is capable or a tremendous number of combinations. The selection of 3 wheels in a certain order introduces 5 x 4 x 3 combinations. The setting of the ringstellungs introduces 26 x 26 x 26 equals 17,576 combinations.

There are $\frac{26x25x24x23x22x21x19x17}{1x2x3x4x5x6}$ x15x13x11x9x7x5x3x1 combinations for patching the stecker board. This works out to 167,613,600x62,895 x 10,395/720 equals 152,418,964,472,775 combinations. Thus the total possible combinations introduced by all elements of the machine combined is 150 million,million,miliion.

FIRST STEPS IN "BREAKING" ENIGMA MACHINE MESSAGES - PREPARATION OF CRIB.

Messages are intercepted in the following form:

FM6 SEXTO l507 AB1 CD2 OMPQTZ NLPGA REHUB TODPQ - - - etc, etc.

The first six letter group (OMPQTZ) contains the indicators. This group is divided into two three letter groups thus (OMP QTZ) by either the receiving operator or the cryptanalyist. The first three letter group (OMP) is the external indicator and is used to set the wheels for decoding the second group (QTZ) or internal indicator to obtain the starting position.

In order to break the message we must try various assumed texts (cribs) derived from experience with the habits of the German operators and the type of traffic handled over the intercepted messages. It is known from call signs and direction finding what organizations (ground forces, air forces or navy) originate the messages and from what locality.

The German operator to encode his message is given the steckers, wheel order and ringatellung for the day, but not the starting position. He must pick six letters for this purpose, three for the starting position and three for a setting in which to encode the starting position. The selection of these letters is where carelessness creeps in to assist us in the "breaking". The operator is apt to pick easy stereotyped combinations, such as the first three letters on the top and middle rows of the enigma machine keyboard (QWE AST), and use them repeatedly. One operator with a girl friend back in Germany by the name of Cillie continuously used the six letters of her name. The term "Cillies" has come to be applied to all sorts of stereotyped phraseology, of which the following are examples:

"Quiet night" - - used by operator in North Africa.
"Wine barrels on hand" - -. used by operator in Czechoslovakia.
"RAF plane over airport" - - used by obliging operator in France.
"Good morning" - - used by operator in Norway.

The first step therefore in "breaking" a message is to guess at the text. For instance in the code written above we will assume the following text:

```
N L P G I R E H M B  T 0 D P Q       (intercepted)
A N X R 0 B I N S 0  N         (assumed text)  (To Goering)
```

The nest step is to attempt to "break" the rest of the message on the basis of the assumed text.

HAND SOLUTION.

It would be impossible to 'break" a message within reasonable time by all possible enigma machine combinations by hand processes. If it were attempted the following would be a likely procedure.

Any particular enigma machine setting involves 4 unknowns to the person "breaking" the message, namely - "stecker board patching", "wheel order", "ringstellung", and "starting point". Since stecker board patching is the largest variable, it is more efficient to make assumptions as to the other unknowns and try all possible patching combinations.

Ringstellung has 2 effects; (a) it changes the position of the "turnover point" at which the slower wheel is advanced by a faster wheel, and (b) it changes the designation of the "starting point" of the wheel. The first effect can be neglected by choosing a portion of the message (crib) sufficiently small to assume that no turnover took place. The second effect can be determined on a relative basis by setting all ringstellungs to a preselected point and finding a relative starting point.

The hand process then resolves into assuming a wheel order and starting point and solving for a stecker board patching that will give the assumed text. This is best done by using an enigma machine with "self steckering" (straight patching) on the stecker board as shown below.

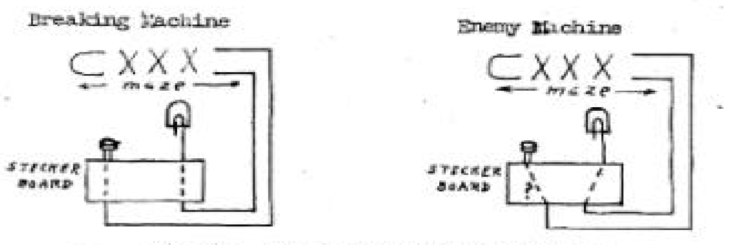


Fig. 4. Method of Deriving Steckers.

Starting with the first pair of letters in the cipher and assumed text (N/A), the first step is to assume that A is steckered to B. In order to determine what transposition takes place when B is put into the maze, we press key B and get lamp X. If our assumption that A is steckered to B is right, then X had to be steckered to N to give the encodement of A indicated by the message. Let us now verify this. Press key X. According to our previous assumptions this is steckered
to N and should give the same effect as pressing key N on the enemy machine for the 2nd pair of letters (L/N). Suppose the Q lamp lights. Then Q would have to be steckered to L. Press key N. According to previous assumptions this is steckered to X and would give the same effect as pressing key X on the enemy machine for the 3rd pair of letters (P/X). Suppose L lamp lights. Then P would have to be
steckered to L but this is a contradiction of the result obtained for the 2nd pair of letters.

CY COUPLE	ASSUMED STECKERS	PRESS KEY	OBTAIN LAMP	DERIVED STECKER	
N/A	A/B	B	X	X/N	
L/N		X	Q	Q/L	
P/X		N	L	P/L	--contradiction

It is then necessary to start the process over by making a new assumption that A is steckered to C and going through The process until no contradiction is obtained after all 26 assumptions have been made.

If no good results are obtained, assume a new starting point. Having exhausted the possibilities of starting points assume new wheel orders.

If every man, woman and child in the British Isles were given an enigma machine, they would have to try 3,000,000 possibilities on each starting position on each wheel order and would work their whole life to break one key.

BOMBE (MACHINE) SOLUTIONS.

A machine called the "bombe" is used to expedite the solution. The first machine was built by the Poles and was a hand operated multiple enigma machine. When a possible solution was reached a part would fall off the machine onto the floor with a loud noise. Hence the name "bombe". The machine we use contains the equivalent of the wheels, uncle walters, current input and stecker arrangements of 36 enigma machines and is motor driven. The machine looks as shown.

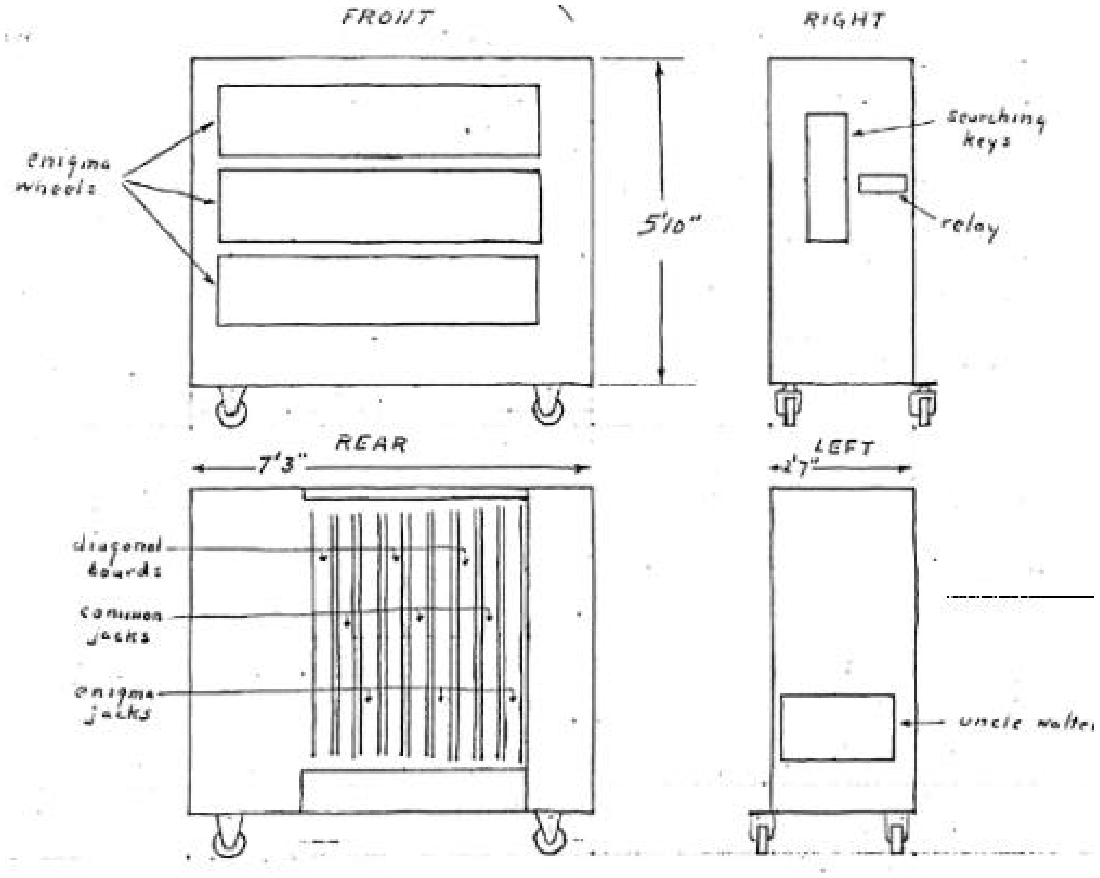


Fig. 5. General Features of The Bombe.

On the front of the bombe are three banks of enigma wheels, 12 enigmas to a bank, and 3 wheels to an enigma. The middle bank also includes three indicator wheels which read the relative ringstellung position at any point in the run. On the right side of the bombe are found the searching keys and also the relay indicator which reads the stecker of the input letter for any stop. On the rear of the machine are found the jacks on which the menu is plugged. Three columns jacks serve one bank of enigmas, the left hand set of three columns serve the top bank of enigmas, the middle set of three columns serve the middle bank of enigmas, &.

Three uncle walters are located on the left side of the bombe. The right hand uncle walter serves the top bank of enigmas, the middle uncle walter the middle bank of enigmas ,&. The uncle walter and the diagonal board remains fixed ,and the wheels are rotated through all possible positions.

The bombe is designed to try simultaneously 26 steckers of the input letter on as many enigmas as there are possible pairs leading to steckers(indicated by the crib). The test of 26 possible steckers is made at each position of the wheels. The wheels are advanced through 17,576 positions in each run. Each enigma has the same wheel order and is set to a starting position which bears the same relation
to ZZZ that the actual machine bore to its "starting point".

The DIAGONAL BOARD is made up of 26 jacks of 26 contacts each, representing all possible steckering of each letter to itself and each other letter. The purpose of the board is to ensure that all steckers obtained are legal(good), conforming to the characteristics of the German machine and that no illegal contradictions (bad steckers) are shown. A miniature diagram for 6 letters is shown.

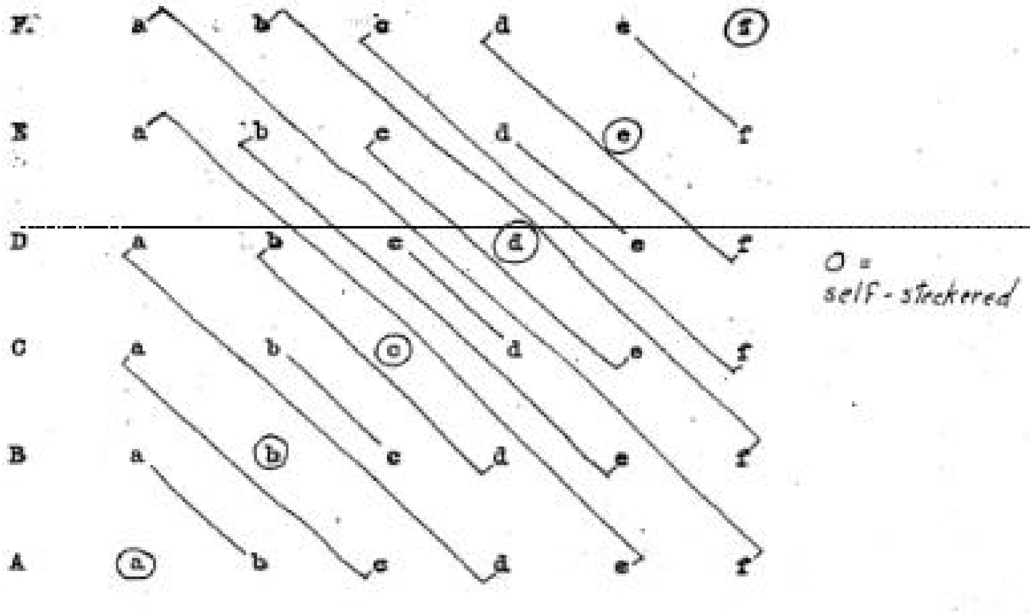


Fig. 6. Partial Diagonal Board

The diagonal board is arranged so that all reciprocals are permanently wired together, i.e. if A is connected to f then F is connected to a. When encoding or decoding on the German machine current is present on only one out of 26 possible circuits.
Conversely a correct stecker will be obtained on the bombe when the diagonal board has only one set of contacts (a "straight") without current - current is on all other 25 circuits. The use of the diagonal board may be understood from the following menu:

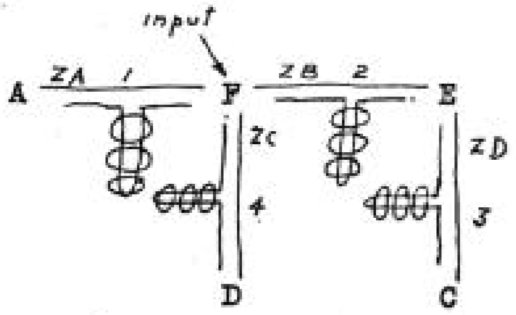
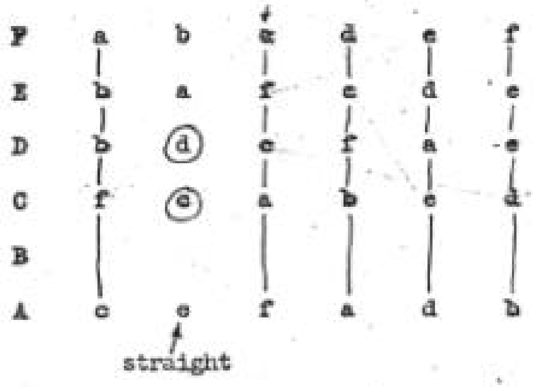


Fig. 7. Sample Menu.

With such a menu set up on a bombe the following paths through the enigmas were found by test to exist when the bombe stopped.



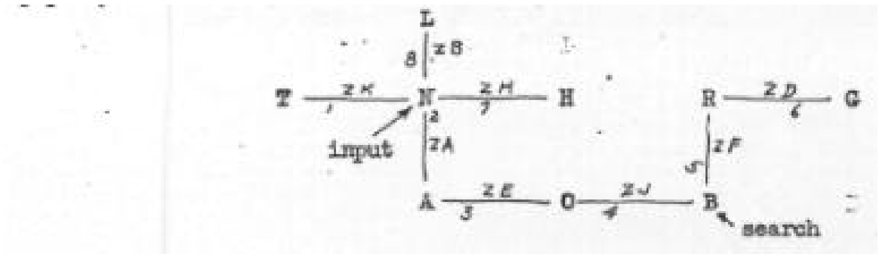
Potential By	Applied At	Puts potential On
Searching Key	F(c)	E(f),D(c),C(a), A(f)
Diagonal Board	C(f)	F(a),E(b),D(b), A(c)
"	F(e)	E(d),D(a),C(e), A(d).
"	C(d)	F(f),E(e),D(e), A(b).
"	E(e)	F(d),D(f),C(b), A(a).

Fig. 8. Formation of Straight.

There is no potential on the remaining path and the machine stopped indicating that at the particular wheel order and relative ringstellung a stecker of A to E would meet the condition. B to F does not apply because B in not on the menu. C and D are self steckered.

PREPARATION OF MENU.

A menu is a means of preparing information in pictorial form for the setting up of the bombe. Referring back to the intercepted message and assumed text on page 3, the following would be a menu prepared to "break" this message.



```
      ZZZ ABCDE FGHIJ K
OMP QTC   NLPGA REHMB TODPQ
          ANXRO BINS0 N
          ++ ++ + + + +
```

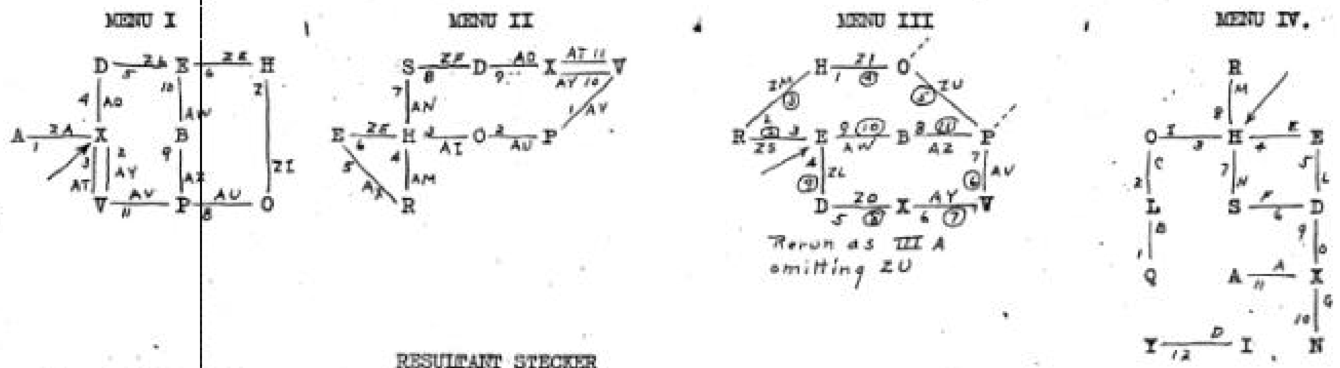
Fig. 9. Typical Menu.

N was selected as the letter on which to build the menu because it occurs most frequently within the crib. Under wheel position ZZB N decodes as L, at ZZK as H, and at ZZK as T. The input of a menu is the letter joining the most closures ,or the largest number of links. This input is put at N as the point from which the menu is most electrically balanced. The search point is selected as the second best input position and must be 2 or more links away from the input, to ensure best performance of the bombe. This search point is put at B to reduce current flow through enigmas between N-A, A-O, O-B. The German SOP is to change starting position every 250 letters.

The menu should be numbered in one continuous chain, making sure that the commons will be between numbers at the beginning or end of the bank of enigmas when possible. Commons should not be used in a closure unless absolutely necessary. Always start numbering at the end of a chain, or part of the menu where an odd number of enigmas converge, to avoid the use of an extra lead and/or common. A good general principle is to so number the menu that the operator can
plug it up using the minimum number of cords and commons.

PREPARATION OF MENUS TO DETERMINE TURNOVER POINT

```
                                              ABCDE FGHIJ KLMNO PQRST UVWXY Z
                        CCM      FAW          XQOYH SNZHI KDMHD SPGRV PPBEV PHEFE SZKYU WGZPF SI
                                              ALLIE DXBOM BERSX WEREX OVERX HERLI NXLAS TXNIG HT
operators wheel      encoded   I              ZZ-                ZA-
setting to en-       wheel     II             ZZ-        ZA-
code real wheel      setting   III
setting                        IV
```



Stop That Brought Up Job.

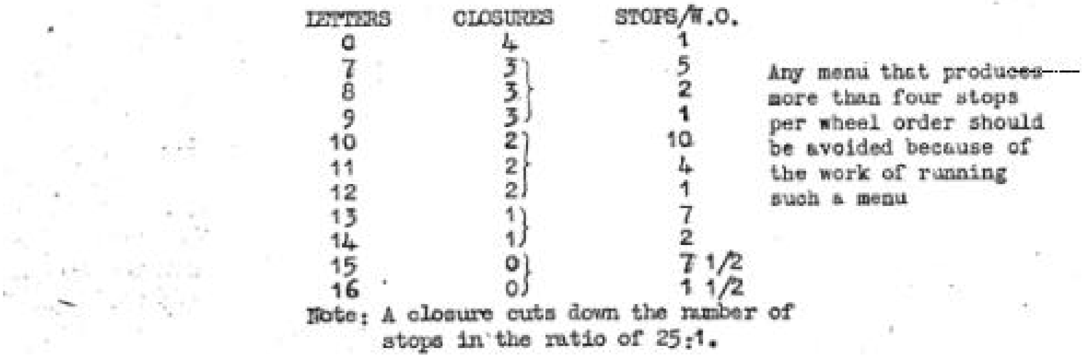
```
        186
        GZT

E       Y
R       V"
H       A
O       S
P       D"
B       (B)
V       R"
X       Q
D       P"

        (1)
        2"
```

RESULTANT STECKER

A	H	N	N
B	B	O	S
C	K	P	D
D	P	Q	X
E	Y	R	V
F	M	S	O
G	U	T	Z
H	A	U	G
I	W	V	R
J	L	W	I
K	C	X	Q
L	J	Y	E
M	F	Z	T

Fig. 10. Preparation of Menu.

The importance of closures in a menu is illustrated by the following abbreviated letter-closure table.



LETTERS	CLOSURES	STOPS/W.O.
6	4	1
7	3	5
8	3	2
9	3	1
10	2	10
11	2	4
12	2	1
13	1	7
14	1	2
15	0	7 1/2
16	0	1 1/2

Any menu that produces more than four stops per wheel order should be avoided because of the work of running such a menu

Note: A closure cuts down the number of stops in the ratio of 25:1.

Fig. 11. Abbreviated Letter Closure Table.

SETTING UP MENU ON BOMBE.

The first step in setting up a menu on a bombe is to insert the proper wheels in the enigmas. To assist in this operation the following color code for painting The wheels is used.

1.	- Red	5.	- Light Brown
2.	- Maroon	6.	- Blue
3.	- Green	7.	- Black
4..	- Yellow	8.	- Silver.

the next step is the plugging of the bombe. Certain general rules have been adopted for plugging. On outside links the inner end of the enigma is patched to the outlying letter. The following menu will be used to illustrate plugging.

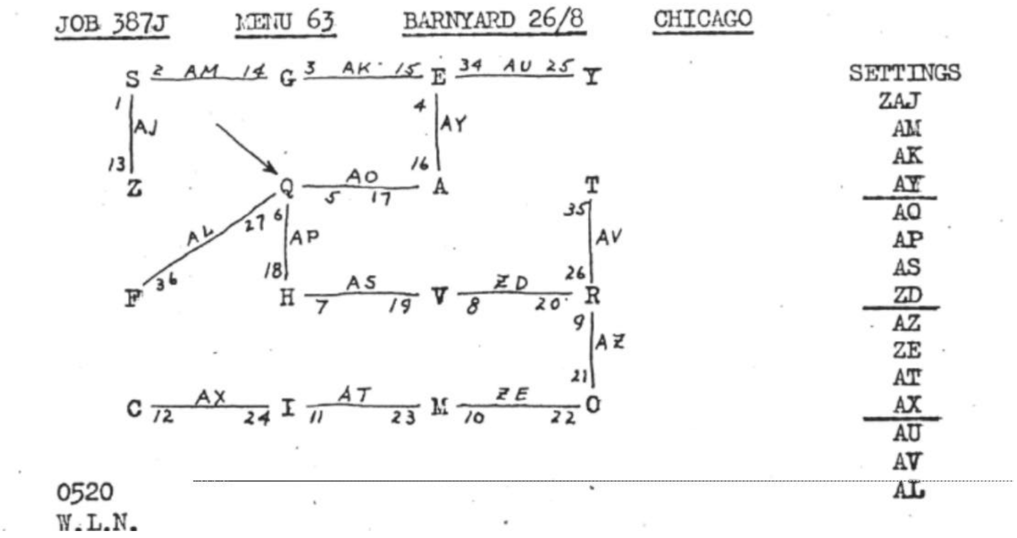


Fig. 12. Typical Menu.

For instruction in plugging this menu see the representation of the jack panel in the rear of the bombe (Fig. 13) On the next page.

There are 7 steps to be followed in plugging up a bombe as follows.

(1) Obtain menu.

(2) Number-up menu to reduce number of commons used.

(2a) plug commoning plug into enigma jacks

(3) Plug enigmas to commons.

(4) Patch commons to diagonal board, also patch input.

(5) Count the letters plugged on the diagonal board and compare this count with the menu.

(6) Count the number of plugs in the commons. Never should be less than 3. Compare this result between banks.

(7) Compare commoning jack positions in enigmas between banks.

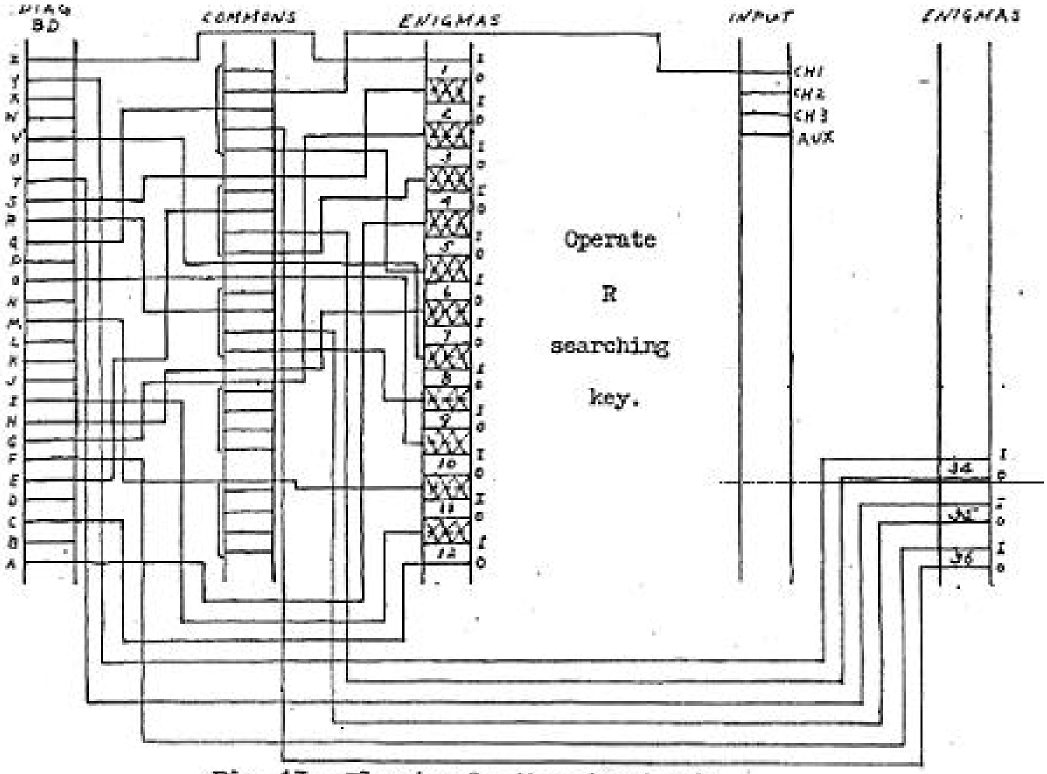


Fig. 13. Plugging for Menu in Fig.12.

Another sample menu is

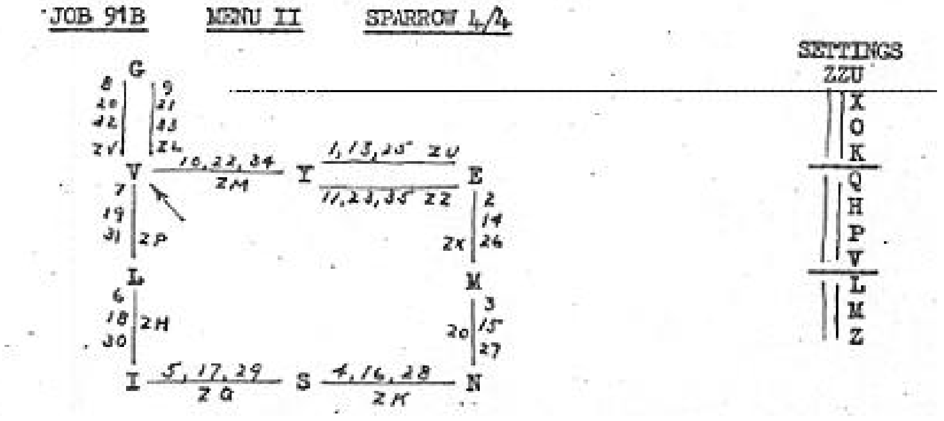


Fig. 14. Sample Menu

It is plugged as follows.

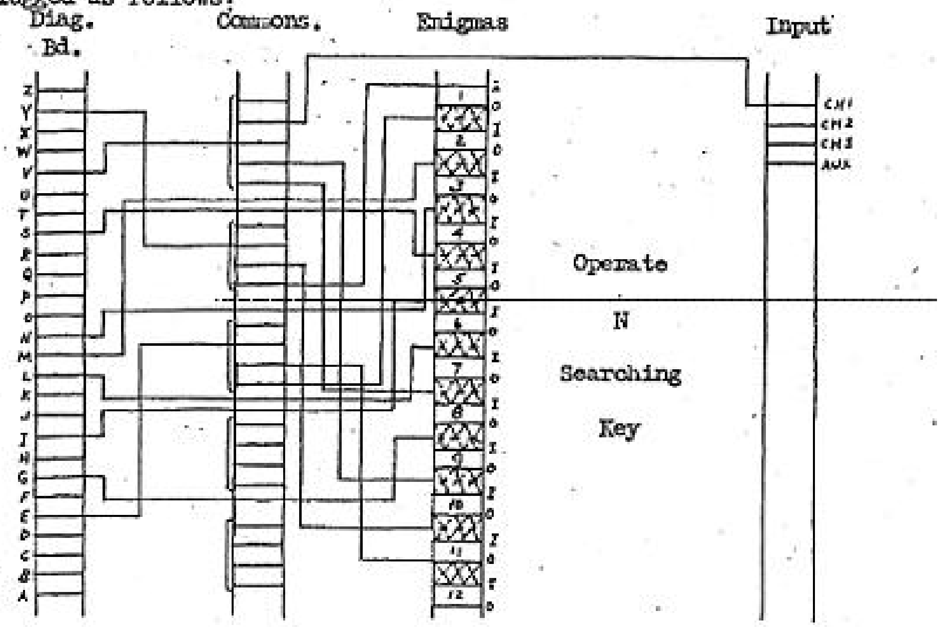
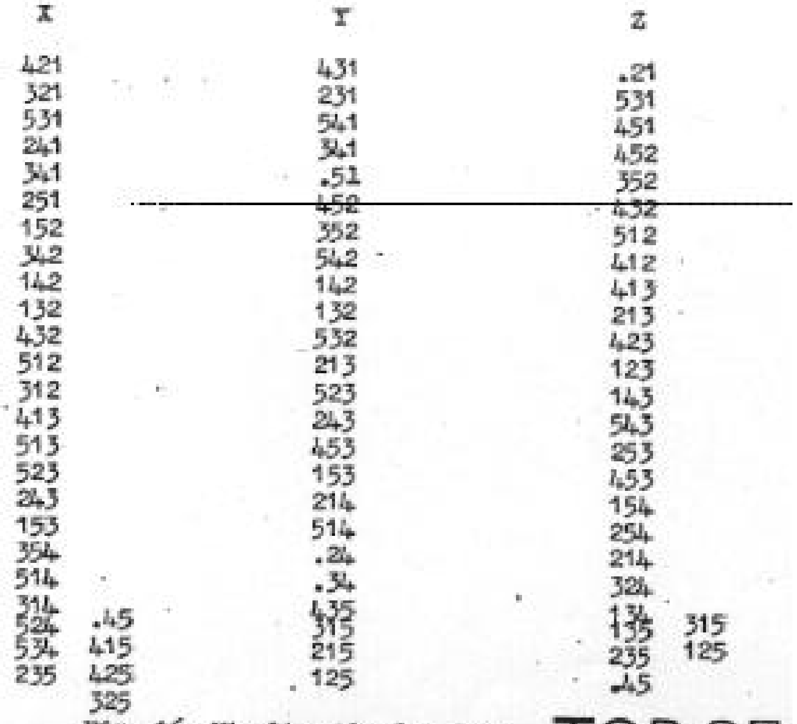


Fig. 15. Plugging for Menu in Fig.14.

Various arrangements Of wheel orders are specified to be run on the bombe. It nay be specified that all 60 wheel orders be run. (abbr. 60. w/os) Sometimes it is specified that we run the left (right) hand side of the w/o sheet only.(abbr. L.H.S. br R.H.S.) It may be required that we use only the nigel Y w/os on the left had
side of the w/o sheet. The Nigelian wheel orders are listed below. They are referred to as Nigel X,Y,or Z.

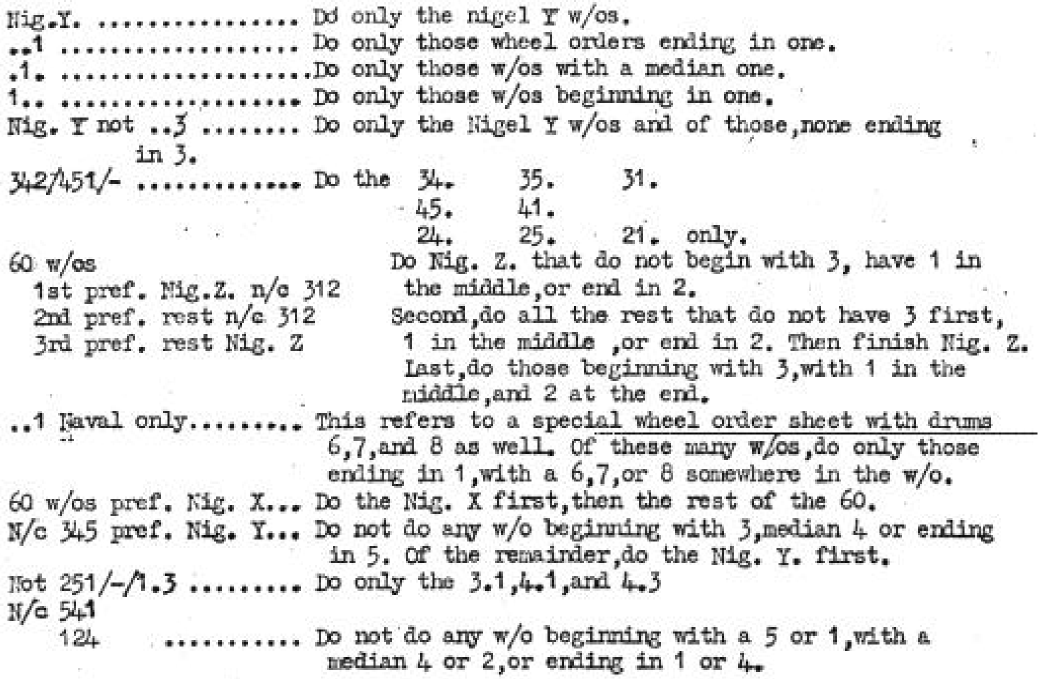


X		Y	Z	
421		431	.21	
321		231	531	
531		541	451	
241		341	452	
341		.51	352	
251		452	432	
152		352	512	
342		542	412	
142		142	413	
132		132	213	
432		532	423	
512		213	123	
312		523	143	
413		243	543	
513		453	253	
523		153	453	
243		214	154	
153		514	254	
354		.24	214	
514		.34	324	
314		435	134	
524	.45	315	135	315
534	415	215	235	125
235	425	125	.45	
	325			

Fig. 16. Nigelian Wheel Orders

TOP SE

It is often specified that non-crashing wheel orders be used. It is the practise of enemy encoders not to use crashing wheel orders on successive days. For instance if wheel order 523 has been used on the first of the month, the wheel order for the second of the month must not include a 5 for the first wheel, a 2 for the second wheel, or a 3 for the third wheel. For example 415 would be a non crashing wheel order which could be used on the second of the month. When all w/os n/c are requested there will be 32 w/os to run. The abbreviated request will read n/c 321 which means that you will run all w/os not beginning with a 3, or with a median 2, or a final 1. N/c. 321 & 452 indicates that all w/os will be run that do not begin with a 3 or 4, or with a median 2 or 5, or a final 1 or 2. Other W/os an preferences would be as follows.



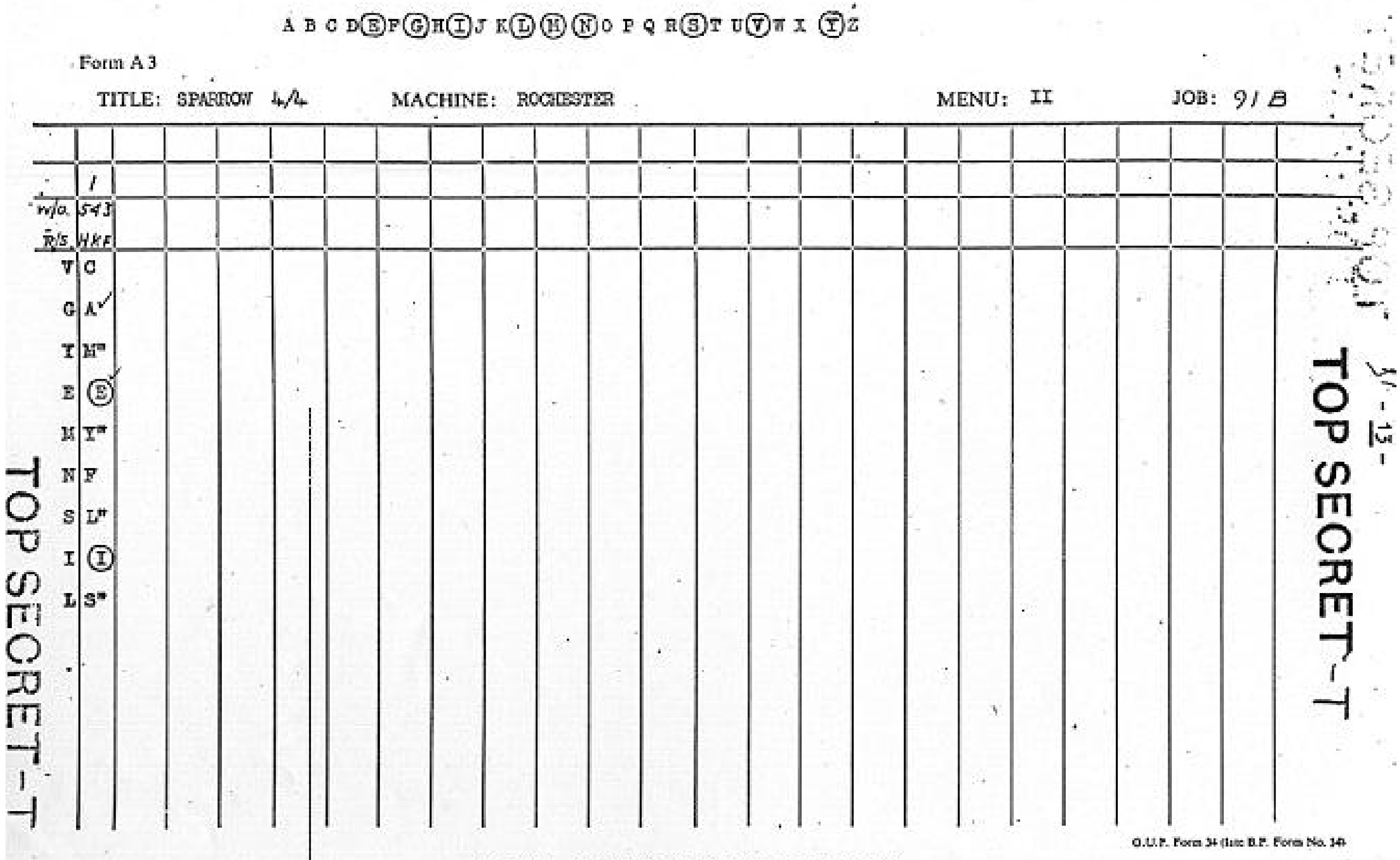
Nig.Y. .... Dd only the nigel Y w/os.
..1 .... Do only those wheel orders ending in one.
.1. ....Do only those w/os with a median one.
1.. .... Do only those w/os beginning in one.
Nig. Y not ..3 .... Do only the Nigel Y w/os and of those,none ending
in 3.
342/451/- .... Do the 34. 35. 31.
45. 41.
24. 25. 21. only.
60 w/os
1st pref. Nig.Z. n/c 312
2nd pref. rest n/c 312
3rd pref. rest Nig. Z
Do Nig. Z. that do not begin with 3, have 1 in the middle,or end in 2.
Second,do all the rest that do not have 3 first, 1 in the middle ,or end in 2. Then finish Nig. Z.
Last,do those beginning with 3,with 1 in the middle,and 2 at the end.
..1 Naval only......... This refers to a special wheel order sheet with drums 6,7,and 8 as well. Of these many w/os,do only those ending in 1,with a 6,7,or 8 somewhere in the w/o.
60 w/os pref. Nig. X... Do the Nig. X first,then the rest of the 60.
N/c 345 pref. Nig. Y... Do not do any w/o beginning with 3,median 4 or ending in 5. Of the remainder,do the Nig. Y. first.
Not 251/-/1.3 .... Do only the 3.1,4.1,and 4.3
N/c 541
124 .... Do not do any w/o beginning with a 5 or 1,with a median 4 or 2,or ending in 1 or 4.

CHECKING BOMBE STOPS.

Each stop obtained from the bombe is verified on a checking machine. This machine has 4 enigma wheels, keys and lamps and is the equivalent of the enigma machine minus the stecker board. When a stop is obtained from the bombe, the operator supplies the following data to the checker, -Stop No., wheel order, Ringstellung setting, and Stecker of input letter. The checker prepares a checking sheet as shown in figure 17, filling in the details called for at the top of the sheet. He writes the alphabet across the top of the sheet and circles the letters on the main chain. A tadpole (wavy line) is drawn below the letters on the subsidiary chain. The letters of the menu are written down in the narrow column at the left of the sheet, starting with the input letter and following consecutively around the menu so as to check through closures first.

There are 3 squares at the top of each column on the checking sheet. When a stop is received, write down the serial number in the second square, wheel order and letters of the stop in the bottom square, and the relay letter opposite the input letter. The top square is left blank until after the stop is checked. The extreme left hand drum should have the Ringstellung (revolving disc) set with Z at the spot on the drum and the drum is set so that the pointer points to B. This setting makes the wiring of the drum The equivalent of the current enemy uncle walter. Set up the letters of the stop on the other three drums by the desired letter on the revolving disc to the spot on the drum. Set the letters of the stop from left to right on the three drums. Revolve the three drums so that

TOP SECRET-T



A B C D Ⓔ F Ⓖ H Ⓘ J K Ⓛ Ⓜ Ⓝ O P Q R Ⓢ T U Ⓥ W X Ⓨ Z

Form A 3

TITLE: SPARROW 4/4 MACHINE: ROCHESTER MENU: II JOB: 91 B

	/																							
w/o.	543																							
R̄/S.	HKF																							
V	C																							
G	A✓																							
T	M"																							
E	Ⓔ✓																							
M	Y"																							
N	F																							
S	L"																							
I	Ⓘ																							
L	S"																							

G.U.P. Form 34 (late B.P. Form No. 14)

TOP SECRET-T

Fig. 17. Check Sheet For Menu in Fig. 14.

the pointers are set for the first link to be checked. Depress the key corresponding to the relay letter (stecker of the input letter) and observe the lighting a lamp corresponding to the stecker of the letter at the other end of the link. Follow round until all links on the menu have been checked.

Definitions Used In Checking

Closure Made (Indicate with /) Occurs when the same stecker letter is obtained over 2 different links between 2 letters. (Female)

Confirmation (Indicate with ") occurs when stecker for one letter on the menu is another letter on the menu an vice versa.

Contradiction occurs when a confirmation does not occur between 2 litters on the menu.

Legal Contradiction (Indicate with *)exists when 2 letters on the menu are steckered to the same letter off the menu.

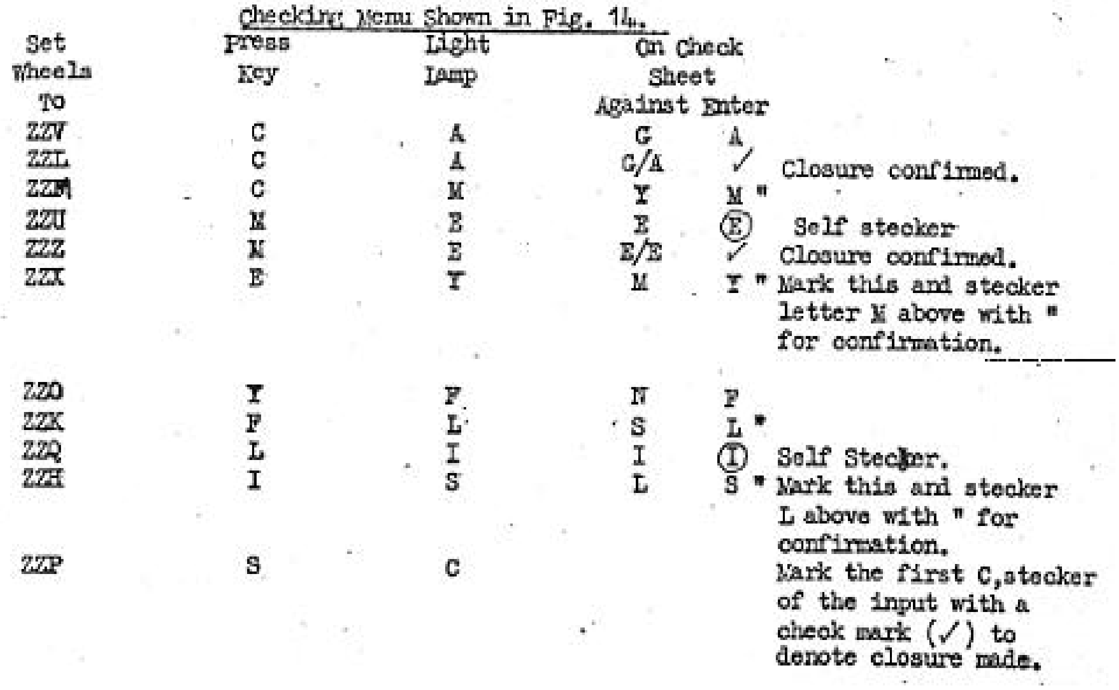
Illegal contradiction (Indicate with x) exists when 1 letter on the menu is steckered to another letter on the menu, but not vice versa.

Good Stop (Indicate with /) any stop without illegal contradictions.

Bad Stop (Indicate with x) any stop with illegal contradictions or fails a closure (all letters obtained art off the menu).

Hut 6 Stop (Indicate with mc/) any stop without any contradictions or with one legal, provided one of the letters involved is on an outlying link or on a phantom. For a single input menu with auxiliary, if a double entry into the auxiliary from the main chain is obtained, this counts as a legal contradiction.

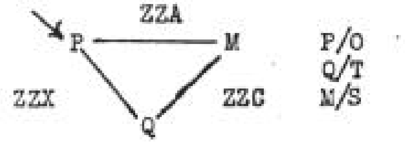
If the 2 letters on the subsidiary give a confirmation when returning to the main chain this stop is sent to Hut 6. If either one or both of the letters on the main menu providing the entry art on outlying links the stop is sent to Hut 6.



Checking Menu Shown in Fig. 14.

Set Wheels To	Press Key	Light Lamp	On Check Sheet Against	Enter	
ZZV	C	A	G	A	
ZZL	C	A	G/A	✓	Closure confirmed.
ZZM	C	M	Y	M "	
ZZU	M	E	E	Ⓔ	Self stecker
ZZZ	M	E	E/E	✓	Closure confirmed.
ZZX	E	Y	M	Y "	Mark this and stecker letter M above with " for confirmation.
ZZO	Y	F	N	F	
ZZK	F	L	S	L "	
ZZQ	L	I	I	Ⓘ	Self Stecker.
ZZH	I	S	L	S "	Mark this and stecker L above with " for confirmation.
ZZP	S	C			Mark the first C,stecker of the input with a check mark (✓) to denote closure made.

The checker must go round every closure to ascertain that the stecker returns to the original letter. Thus:



When starting with P/O, getting Q/T, M/S, we must be able to set ZZA, press S and light up 0. Having completed the closure the last letter, S in this case, should be marked with a check mark to indicate that you have made this closure.

Check all steckers against alphabet at the tope of the sheet and mark confirmation and self steckers, as follows:

A/P "
P/A "
S/(S)

All entries onto subsidiary chain must be checked. When checking subsidiary chain all entries back onto the main chain must result in a confirmation, otherwise there is an illegal contradiction and the stop is wrong. Check over steckers and mark legal contradictions as follows:

R/W*
T/W

Summarize the total number of self steckers, legal contradictions, and confirmations for the stop and write the total in the stecker column. Thus:

2 *
1 "
(2)

CHECK STOPS

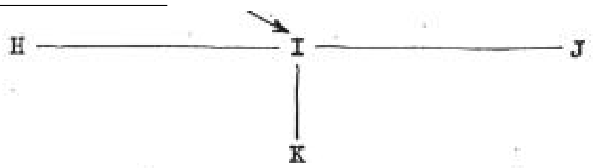
In order to maintain a continuous check on the performance of the bombe and its operator, check stops are taken on all wheel orders where a good stop does not occur. This is done by opening a link through removing the fast drum. Always try to open a "female" or the smallest closure. If, however, there is no closure, an outlying link can be taken off. In any case the link being broken must be one or more links removed from the input.

The stop slip which the operator gives the checker will bear the notation that a link was removed to obtain the stop, shown as minus the link setting, that is (-ZZA). All other links on the menu are checked in the normal manner. The notation (-ZZA) is placed in the same square with the wheel order and letters of the stop. If the link removed is an outlying link, an illegal contradiction must be obtained from the stecker of the letter at the end of the removed link. If the link removed breaks a closure, the checker must check across the link removed and prove that it fails the closure as it should. If these results are not obtained the check stop is wrong. When checking across a link that was removed to break a closure write down the resulting incorrect stecker in the upper left corner of the square and put the correct stecker in the lower right corner of the square.

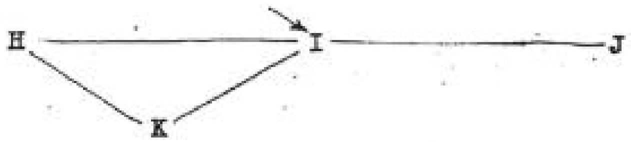
	CHECKING
To be sent in if half of legal contradiction is on out-lying link.	To be sent in for further investigation.

Procedure:
(1) Place on the machine the w/o of stop to be tested.
(2) Rotate drum discs until letters of the stop are opposite the dots on the drums.
(3) Decide which is the easiest way to test around the menu, starting with the input.
(4) Turn drums to the first setting and depress the relay(couple of the input).
(5) Resultant light indicates the couple of the next letter on the menu.
(6) Continue the process around the menu, rotating the drums to the next setting and depressing the previous couple to get the couple of the following letter on the menu.

SINGLE INPUT, SINGLE RELAY.

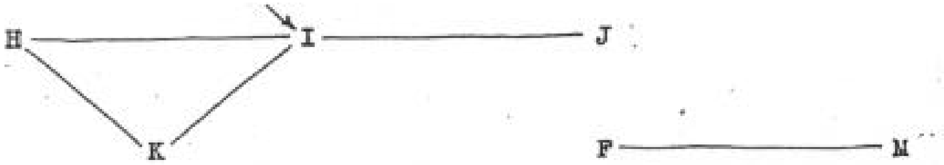


TYPES OF CONTRADICTION AND CONFIRMATIONS WHEN TESTING.	COUPLES	STANDARD M/C'S	JUMBOS	REMARKS.
2 letters on the chain coupled to a third letter off the chain.	I|P J|T H|L K|L	legal contradiction.	stop.	correct from M/C point of view, If legal contradiction is on out-lying link, could be correct stop.
2 letters on the chain coupled to a third letter on the chain	I|P J|T H|J K|J	illegal contradiction, M/C should not have stopped.		a fault on the M/C. Inform Technician.
1 letter on the chain coupled to another letter on the chain which does not give a confirmation.	I|P J|T H|K K|R	illegal contradiction, M/C should not have stopped.		a fault on the M/C Inform Technician.
1 letter on the chain coupled to another letter on the chain which gives a confirmation.	I|P J|T H|K K|H	confirmation.	stop.	could be correct stop.



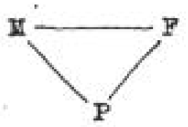
TYPES OF CONTRADICTION AND CONFIRMATIONS WHEN TESTING.	COUPLES	STANDARD M/C'S	JUMBOS	REMARKS.
When going round a closure the couple of the letter started at is the same when it is returned to.	I|P H|T K|S I|P J|K	imperative.	stop or story.	might be the right stop.

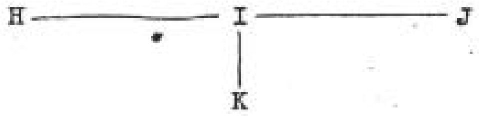
When going round a closure the couple of the letter started at is not the same when it is returned to.	I|P H|T K|S I|N J|R	illegal contradiction machine should not stop		a fault on the M/c. Inform Technician.



To get on to a subsidiary chain a letter on the main chain must be coupled to a letter on the subsidiary chain but not returning to the main chain by a couple of any other letter of the subsidiary chain unless it confirms,	I|N H|L J|T K|F --- F|K M|S	remissible	story printed. of all letters on both chains if there is no legal contradiction on the other letters	Could be the right stop.
2 letters on the main chain coupled to 2 different letters on the subsidiary if chain which give a confir-'nation when returning to the main chain	I|N H|F J|S K|N ------ F|H|H M|K|K	confirmation	story printed of all letters on both chains if there is no legal contradiction on the other letters.	could be the right stop.
2 letters on the chain chain coupled to 2 different letters on the subsidiary chain which give a contradiction through the subsidiary chain.	I|N H|F J|S K|M ----- F|J|R M|Q|K	legal contradiction	stop	correct from M/C point of view. If either want chain letter or subsidiary chain letter concerned on an outlying link, stop is sent in.
2 letters on the main chain coupled to one letter on the subsidiary chain.	I|N H|L J|F K|F ----- F|J|K M|S|W	legal contradiction	stop	as above.
After getting on to the subsidiary chain, one letter on the subsidiary chain is coupled to one letter on the main chain which does not confirm.	I|N H|L J|F K|F ---- F|K M|I	illegal contradiction (unless there are two relays up on the main chain). Machine should not have stopped		a fault on the M/C. Inform Technician.

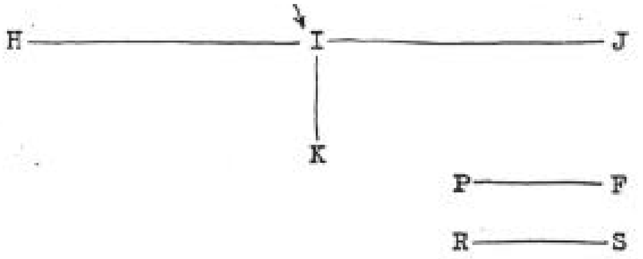
After getting on to the subsidiary chain, a contradiction occurs on the subsidiary chain	I|N H|L J|S K|F ------ F|K|M M|F|S	legal contradiction	stop	correct from M/C point of view. F must be tested with M and another couple will be found for M which must not contradict on the main chain. If main chain letter or any subsidiary chain letter concerned is on outlying link, stop is sent in.





If on getting on to subsidiary chain, stop does not go round closure of subsidiary chain.	I|N H|H J|J K|F ---- F|K P|P M|W P|T	permissible but not completely checked.	stop only	correct from M/C point of view if on completing checking no contradiction is found with letters of main chain. If main chain letter concerned is outlying link,stop is sent in.

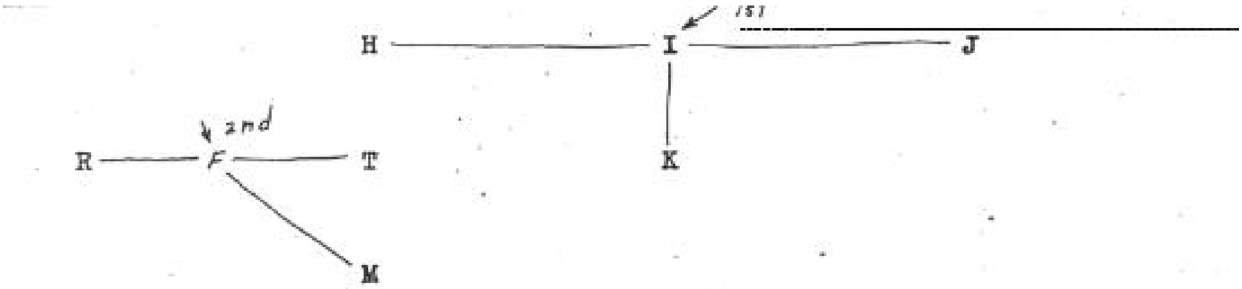
SINGLE INPUT,SINGLE RELAY WITH MORE THAN ONE SUBSIDIARY CHAIN



After getting on to the subsidiary chain,one letter on the same chain is coupled to a letter on another subsidiary chain.	I|A J|B H|L K|P ---- P|K|R|F F|R|S|G	permissible	One complete story for all letters.	Could be the right stop,because F-R it must then be assumed that R/F and the couple for S found.
After getting on to the subsidiary chain 1 letter on the same chain is coupled to a letter on another subsidiary chain, a letter on this chain is then coupled back to the first subsidiary chain.	I|A J|B H|L K|P ---- P|K|S F|R|G ----- R|F S|P	legal contradiction	stop	correct from M/C point of view. Only sent in if any letter concerned is the end letter of any outlying link.

```
After getting on to the        I|A   illegal contradiction,   a fault on the
subsidiary chain one           J|B  machine should not      machine. Inform
letter on the same chain       H|L  have stopped.           Technician.
is coupled to a letter on      K|P
another subsidiary chain,    ----
a letter on this chain is     P|K
then coupled back to a         F|R
letter on the main chain.      ----
which does not confirm.        R|F
                               S|J
                                                                          .
```

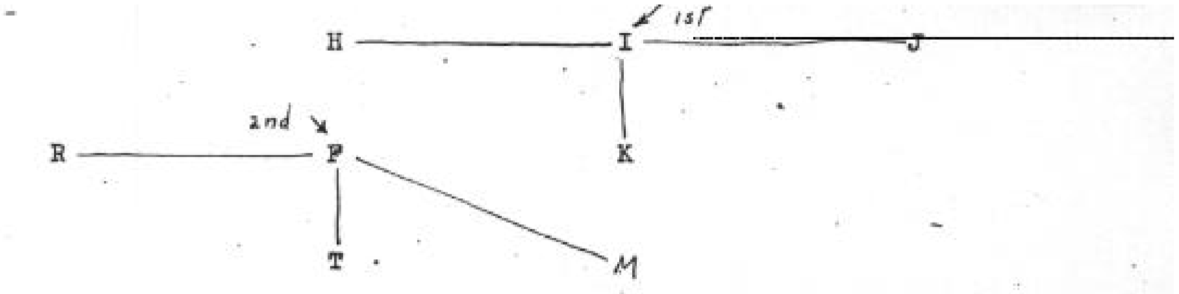
DOUBLE INPUT. SINGLE RELAY ON EACH CHAIN



```
With a double input job each   I|A||F|E permissible  1 couple  could be
chain has an input and each    J|S||M|Z               for each  correct stop.
input has a relay,therefore    H|L||T|X               chain
each chain is checked as       K|Y||R|D               printed
though it were a separate
chain.
                                                                          .
```

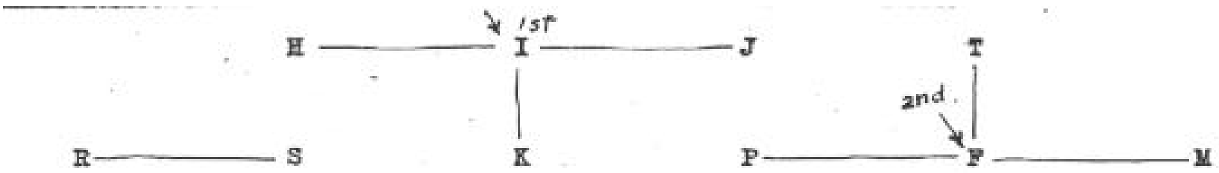
```
1 letter on one chain          I|A||F|E  confirma-   one story could be
is coupled to one on           J|S||M|Z  tion         for all   correct stop.
the other chain and            H|L||T|X               letters
gives a confirmation.          K|R||R|K               printed
                                                      (unless
                                                      there is
                                                      a legal
                                                      contradiction)
                                                                          .
```

```
1 letter on each chain         I|A||F|E  legal        one story  correct from
is coupled to the same         J|S||M|Z  contra-      for each   M/C point of
letter off both chains.        H|L||T|X  diction     chain     view.If legal
                               K|C||R|C               printed   contradiction
                                                                 is on outlying
                                                                 link, could be
                                                                 correct, stop
                                                                          .
```



<table>
<tr><td>1 letter on one chain is coupled to one letter on the other chain which is coupled back to another letter on the first chain</td><td>I|A||F|E
J|S||M|Z
H|L||T|X
K|R||R|J</td><td>illegal contradiction. M/C should not have stopped.</td><td>fault on the M/C. Inform Technician.</td></tr>
<tr><td>1 letter on one chain is coupled to one letter on the other chain ,which is coupled to another letter on the same chain.</td><td>I|A||F|E
J|S||M|Z
H|L||T|X
K|R||R|F</td><td>illegal contradiction. M/c should not have stopped.</td><td>a fault on the M/C. Inform Technician.</td></tr>
<tr><td>1 letter on one chain is coupled to one letter on the other chain ,which is coupled to a letter off both chains.</td><td>I|A||F|E
J|S||M|Z
H|L||T|X
K|R||R|C</td><td>illegal contradiction. M/C should not have stopped.</td><td>a fault on the M/C. Inform Technician.</td></tr>
</table>

DOUBLE INPUT, SINGLE RELAY ON EACH CHAIN, WITH SUBSIDIARY CHAIN.



<table>
<tr><td>@After getting on to the subsidiary chain from the main chain, one letter on the subsidiary chain is coupled to one letter on the auxiliary chain which confirms,</td><td>I|A||F|Y
J|B||P|D
H|L||T|X
K|R||M|U

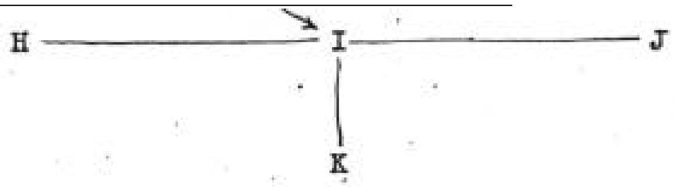
R|K||R|K
S|F||S|F</td><td>confirmation.</td><td>story printed (unless there is a legal contradiction on the other letters.</td><td>could be the right stop.</td></tr>
<tr><td>@After getting on to the subsidiary chain from the main chain,one letter on the subsidiary chain is coupled to one letter on the auxiliary chain which does not confirm.</td><td>I|A||F|S
J|B||P|D
H|L||T|Q
K|R||M|U

R|K
S|F</td><td>illegal contradiction, M/C should not have stopped.</td><td></td><td>a fault on the M/C Inform the Technician.</td></tr>
<tr><td>@After getting on to the subsidiary chain from the main chain,one letter on the auxiliary chain is coupled to a letter on the subsidiary chain which does not confirm.</td><td>I|A||F|D
J|B||P|S
H|L||T|Q
K|R||M|U

R|K||R|C
S|Y||S|P</td><td>Permissible</td><td>2 stories printed (unless there is a legal contradiction on the other letters).</td><td>correct from M/C point of view. If the main chain letter concerned is on out-lying link the stop is sent in.</td></tr>
</table>

@ In all examples "Main" and "Auxiliary" chain can be reversed and conditions still apply.

SINGLE INPUT, DOUBLE RELAY. SEE ALSO BOXING STOPS.

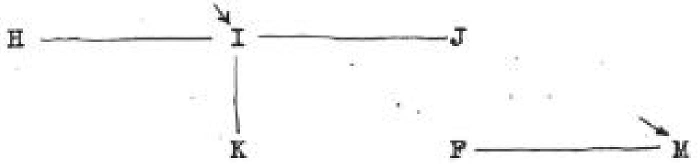


```
When going round a chain       I|P|N   permis-  2 storys   one relay could
each relay has to be           J|S|R   sible.   possible.  be the right stop.
tested. This gives two         H|L|P
different couples for          K|S|S
each letter of the menu.
                                                                                .
```

```
When going round a chain       I|P|N   Impossible. Wrong checking.
one letter cannot be           J|T|R
coupled to the same letter     H|L|F
each time.                     K|S|S
                                                                                .
```

```
on the first relay one
letter on the chain is         I|K||I|A  illegal contra-   a fault on M/C on
coupled to another letter      H|L||H|H  diction on first  first relay. Inform
on the chain,which does        K|S||K|D  relay but second  Technician. Second
not confirm on either          J|T||J|R  relay is correct. relay could be
relay.                                                      right stop.
                                                                                .
```

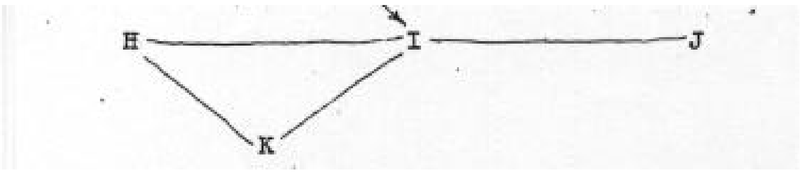
DOUBLE INPUT. SINGLE RELAY ON MAIN CHAIN. DOUBLE RELAY ON AUXILIARY CHAIN.



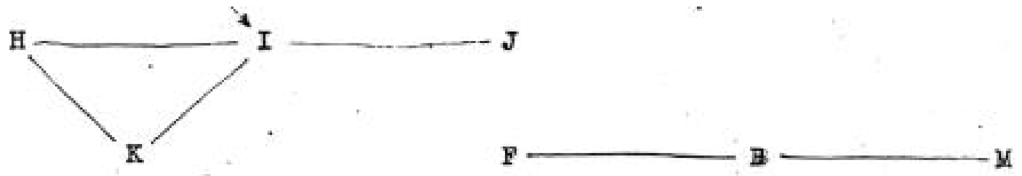
```
1 letter on the main           I|P   confir-  stop or story
chain is coupled to one        J|S   mation.  possible.
letter on the auxiliary        H|L             Second story
chain. zither of the           K|F             also possible
auxiliary chain relays         ------          on auxiliary
may confirm.                   M|T|B           chain.
                               F|N|K
                                                                                .
```

```
1 letter on the main           I|P   illegal contradiction.   a fault on the
chain is coupled to            J|S   M/C should not have      M/C. Inform
one letter on the              H|L   stopped.                 Technician.
auxiliary chain which          K|F
is not confirmed.              --------
                               M|T|B
                               F|N|Y
                                                                                .
```

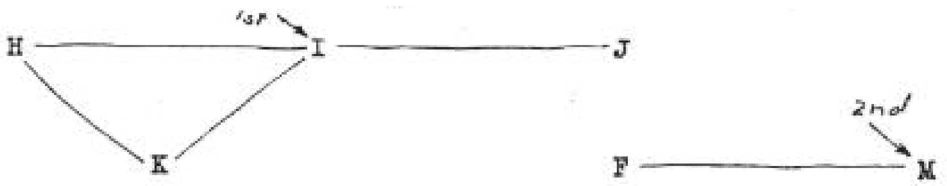
BOXING STOPS.



When going round a closure on a double relay stop,the couple of the letter started at can return to the second couple	I|P||I|A H|L||H|Q K|S||K|F I|A||I|P J|T||J|R	boxing. M/C stops but does not print.	correct from M/C point of view,but could not be right stop.
When going round a closure on a double relay stop,the couple of the letter started at does not return to the same letter with either of the two relays.	I|P||I|A H|L||H|Q K|S||K|F I|N||I|S J|T||J|R	illegal contradiction. Machine should not stop.	a fault on the M/C. Inform Technician.
On the first relay one letter on the chain is coupled to another letter on the chain, which confirms on the other relay.	I|K||I|A H|L||H|Q K|S||K|I J|T||J|R	boxing. M/C stops but does not print.	correct from M/C point of view ,but could not be the right stop.



After getting on to the subsidiary chain by K being coupled to F,it is found that M returned to K. This is correct if on the 2nd time round K is coupled to M.	I|N||I|P H|L||H|X K|F||K|M J|S||J|C -----~-- F|K||F|K B|T||B|T M|K||M|K	boxing. M/C stops but does not print.	correct from M/C point of view,but could not be right stop.
After getting on to the subsidiary chain by K being coupled to F,it is founi that M returned to K,but on the 2nd time round K is not coupled to M.	I|N||I|N H|L||H|X J|S||J|C K|F||K|A -------- F|K B|P M|K	illegal contradiction. M/C should not stop.	a fault on, the M/C. Inform Technician.



2 letters on the main chann are coupled to 2 letters on the auxiliary chain which on testing giye a confirmation on one letter only the 1st time round on the auxiliary chain and on the other letter the 2nd time round.	I|M H|L J|W K|F -~-- M|0||M|I F|K||F|X	boxing. stop.	corrtct from M/C point of view,but could not be the right stop.

2 letters on the main chain are coupled to 2 letters on The auxiliary chain, which gives a confirmation on 1 letter but a contradiction on the other letter on either relay.	I M H L J W K F --------- M 0 M Y F K F X	illegal contradiction. M/C should not stop	a fault on the M/C Inform Technician .
2 letters on the main chain are coupled to 1 letter on The auxiliary chain which gives a confirmation on 1 letter and let time round and on the other the 2nd time round.	I F H L J X K F ------- M Y M W F I F K	stop.	correct from M/C point of view, but could be the right stop if either main chain letters were on out-lying link. .
2 letters on the main chain are coupled to one letter on the auxiliary chain which does not give a confirmation on both letters on the auxiliary chain.	I F H L J X K F ------- M Y M F F I F T	illegal contradiction. M/C should not stop.	a fault on the M/C. Inform Technician. .

TYPES OF MENUS.

In the general description of setting up a menu on a bombe,the single input menu has been used as an example. There are several other types of menus, a description of which follows.

Double Input - On sane menus the crib produces several letters which are not connected to the main menu by links and yet their menu is too strong to be run as
a subsidiary to the main menu. In such a case both menus are plugged to the same diagonal board and a double input used. The following is a sample of such a menu:

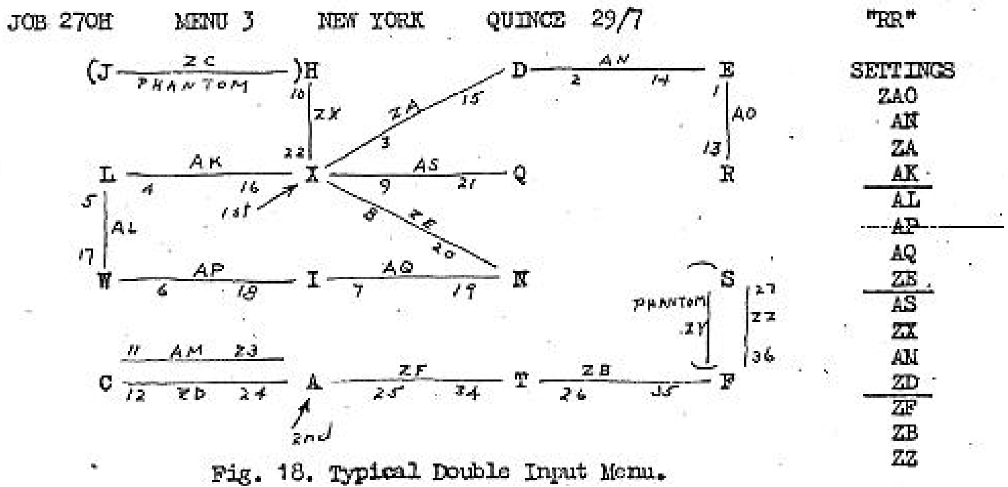


Fig. 18. Typical Double Input Menu.

This menu is numbered and plugged the same as for a single input except that the second input patch is connected to Chain 2 or Auxiliary as the case may be.

These menus can only be put on the bombe twice since there are only 4 chain circuits with associated inputs. In the older type machines a double input plug board must be substituted for the single input. This changes the association of wiring and the contacts of the sensing relays so that the bombe will not stop unless there is an open circuit on both parts of the menu. In the newer type machines the "double input" switch operated. One letter (stecker) per chain must be read at each stop. On the older type machines the letter for the auxiliary chain cannot be read on the indicator and must be found by feeling the sensing relays for that chain. On the new type machines this is read on the chain 2 portion of the indicator. The search keys used for double input menus must be arranged to cross search,that is the search key for the main menu has the same letter designation as the input letter for the auxiliary chain and vice versa. This practise has been adopted to give the best distribution of
current due to the association of the two search points through the diagonal board. If this is not done you have more than one point on each row of the diagonal board where you are applying potential and may obscure the one o.c. point you are seeking.

5 Points of Difference in Plugging and Operating Double Input.

(1) Both menus plugged to the same diagonal board.

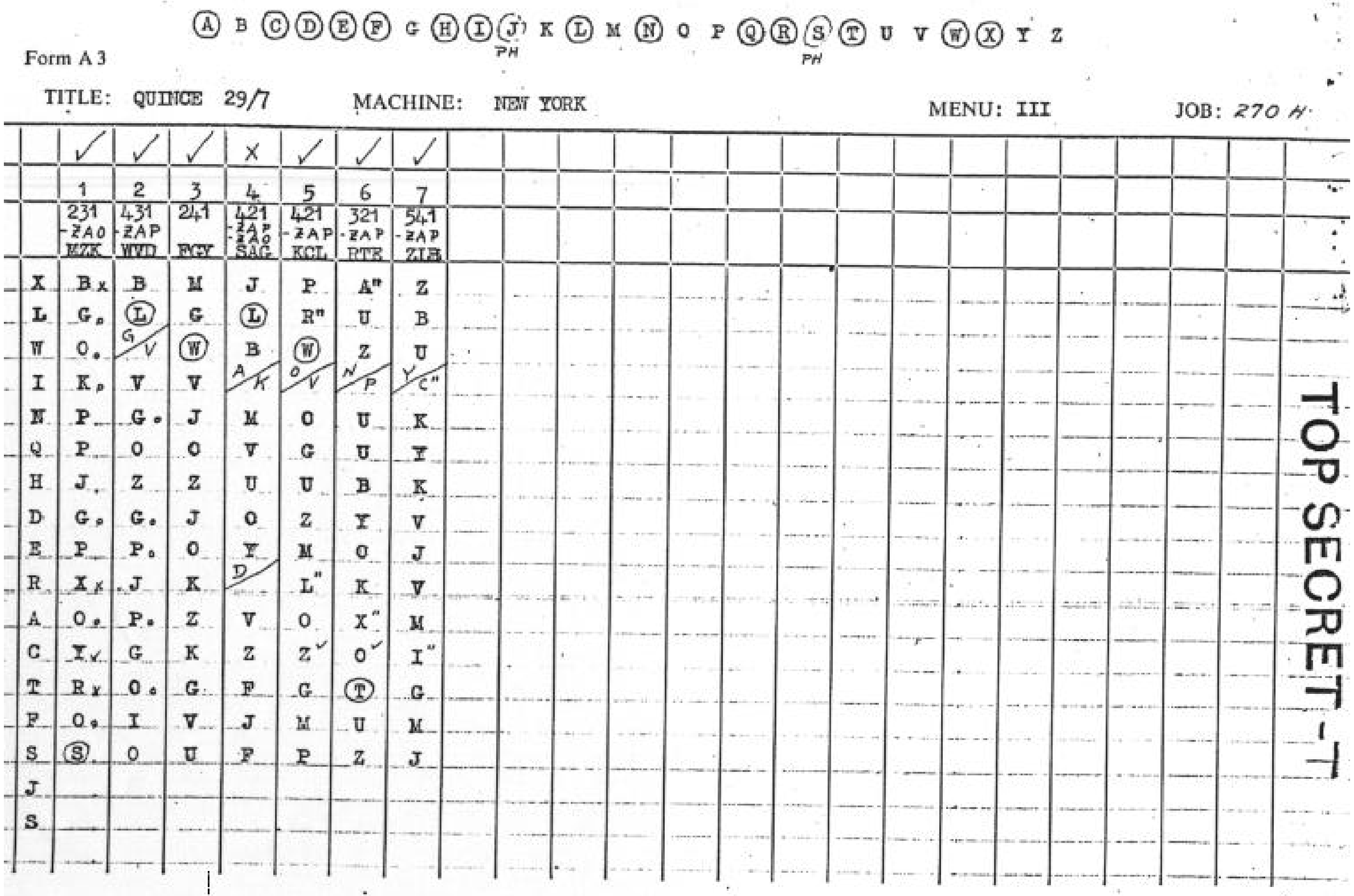
(2) Before starting be sure D.I.plugboard has been substituted for S.I. board in old machines ,-D.1. key thrown on new machines,

(3) Be sure to "cross-search."

(4) Have technician find Auxiliary chain relay (indication) on old machine.

(3) Record at least 2 relays per stop.

The checking of double input menus is somewhat different. In this case you are supplied with two stecker letters ,one for the input of each menu. Each menu is checked through independently. After deriving all stecker letters,the two menus are evaluated as one to determine the type of stop. It may be found in checking a female link that you have a boxing stop,-you derive 4 stecker letters in going round the closure and have to go round twice to obtain a closure. This is not a good stop since on the enigma machine one letter can only have one stecker.



Ⓐ B Ⓒ Ⓓ Ⓔ Ⓕ G Ⓗ Ⓘ Ⓙ K Ⓛ M Ⓝ O P Ⓠ Ⓡ Ⓢ Ⓣ U V Ⓦ Ⓧ Y Z
PH PH

Form A 3

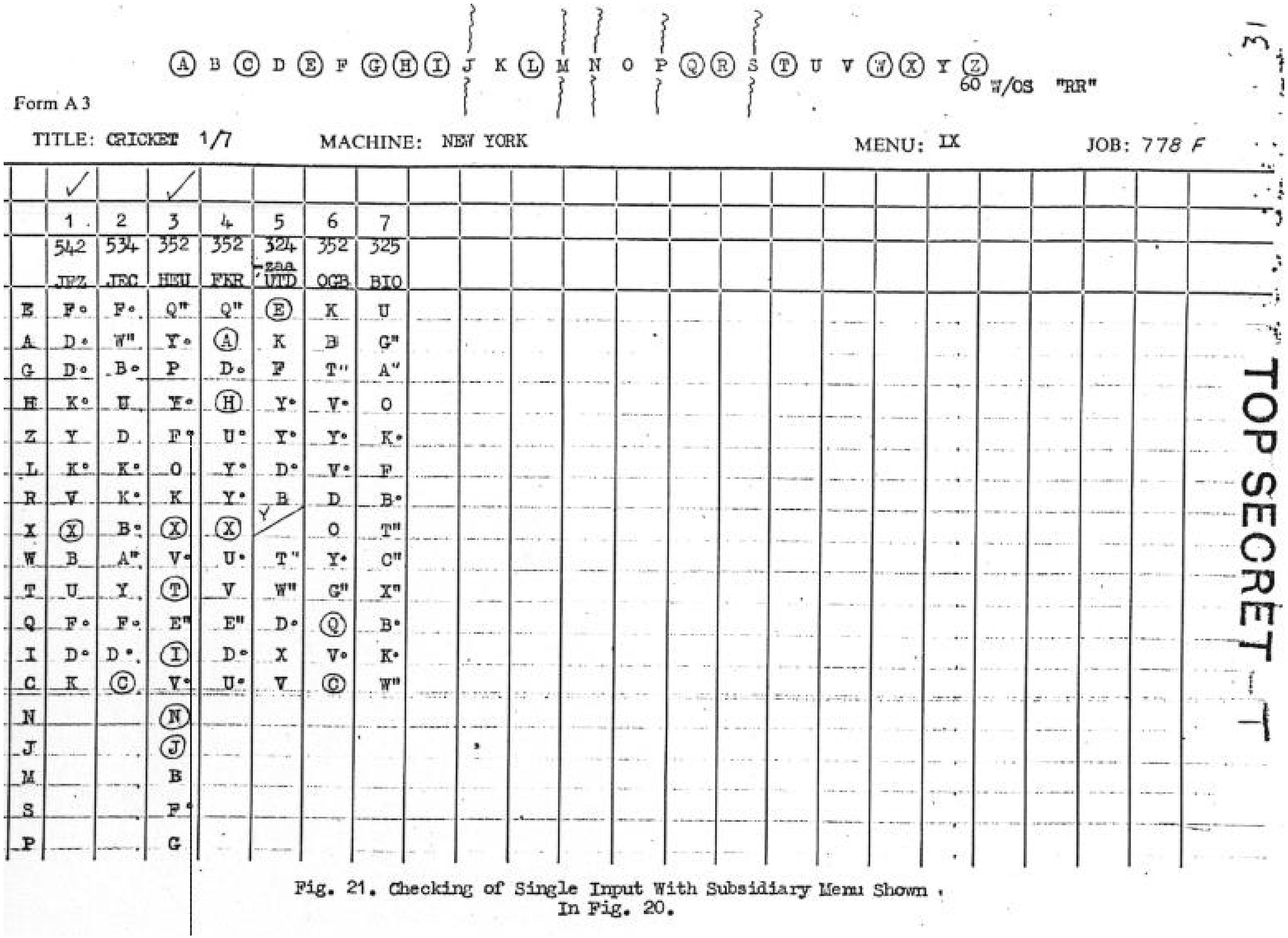
TITLE: QUINCE 29/7 MACHINE: NEW YORK MENU: III JOB: 270 H

TOP SECRET -T

		✓	✓	✓	X	✓	✓	✓
		1	2	3	4	5	6	7
		231 -ZAO MZK	431 -ZAP WVD	241 FGY	421 -ZAP -ZAO SAG	421 -ZAP KCL	321 -ZAP RTE	541 -ZAP ZIB
	X	Bx	B	M	J	P	A"	Z
	L	G.	Ⓛ	G	Ⓛ	R"	U	B
	W	O.	G / V	Ⓦ	B	Ⓦ	Z	U
	I	K,	V	V	A / K	O / V	N / P	Y / C"
	N	P	G.	J	M	O	U	K
	Q	P	O	O	V	G	U	Y
	H	J.	Z	Z	U	U	B	K
	D	G.	G.	J	O	Z	Y	V
	E	P	P.	O	Y	M	O	J
	R	Xx	J	K	D /	L"	K	V
	A	O.	P.	Z	V	O	X"	M
	C	Y✓	G	K	Z	Z✓	O✓	I"
	T	Rx	O.	G	F	G	Ⓣ	G
	F	O.	I	V	J	M	U	M
	S	Ⓢ	O	U	F	P	Z	J
	J							
	S							

Fig. 19. Checking of Double Input Menu Shown in Fig.18.

TOP SECRET



Ⓐ B Ⓒ D Ⓔ F Ⓖ Ⓗ Ⓘ J K Ⓛ M N O P Ⓠ Ⓡ S Ⓣ U V Ⓦ Ⓧ Y Ⓩ 60 W/OS "RR"

Form A 3

TITLE: CRICKET 1/7 MACHINE: NEW YORK MENU: IX JOB: 778 F

	✓		✓				
	1	2	3	4	5	6	7
	542 JWZ	534 JEC	352 HEU	352 FKR	324 zaa UTD	352 OGB	325 BIO
E	F°	F°	Q"	Q"	Ⓔ	K	U
A	D°	W"	Y°	Ⓐ	K	B	G"
G	D°	B°	P	D°	F	T"	A"
H	K°	U	Y°	Ⓗ	Y°	V°	O
Z	Y	D	F°	U°	Y°	Y°	K°
L	K°	K°	O	Y°	D°	V°	F
R	V	K°	K	Y°	B Y	D	B°
X	Ⓧ	B°	Ⓧ	Ⓧ		O	T"
W	B	A"	V°	U°	T"	Y°	C"
T	U	Y	Ⓣ	V	W"	G"	X"
Q	F°	F°	E"	E"	D°	Ⓠ	B°
I	D°	D°	Ⓘ	D°	X	V°	K°
C	K	Ⓒ	V°	U°	V	Ⓒ	W"
N			Ⓝ				
J			Ⓙ				
M			B				
S			F°				
P			G				

Fig. 21. Checking of Single Input With Subsidiary Menu Shown In Fig. 20.

Single Input With Subsidiary. Frequently the main menu is not strong enough to hold the number of stops per wheel order down to a reasonable figure. When this happens a subsidiary menu is added. The following is an example.

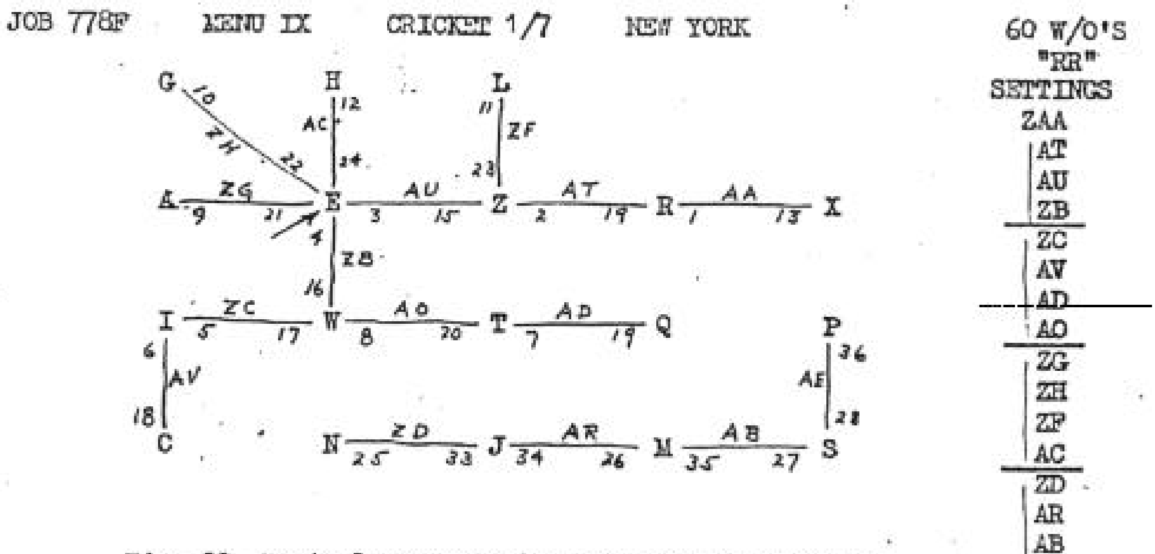


Fig. 20. Typical Menu,Single Input With Subsidiary.

The bombe is set up for this type menu in the same way as for a regular single input menu. The probable searching key would be M. When checking this type menu apply the stecker letter from the bombe in the normal manner to the letters of the main chain. From these you may or may not get on to the subsidiary chain. If you do, and work out its steckers, these must be evaluated together with the main chain.

Double Input With Subsidiary . - The procedure for this type of menu is very similar to that for Single Input With Subsidiary. The following menu is a sample:

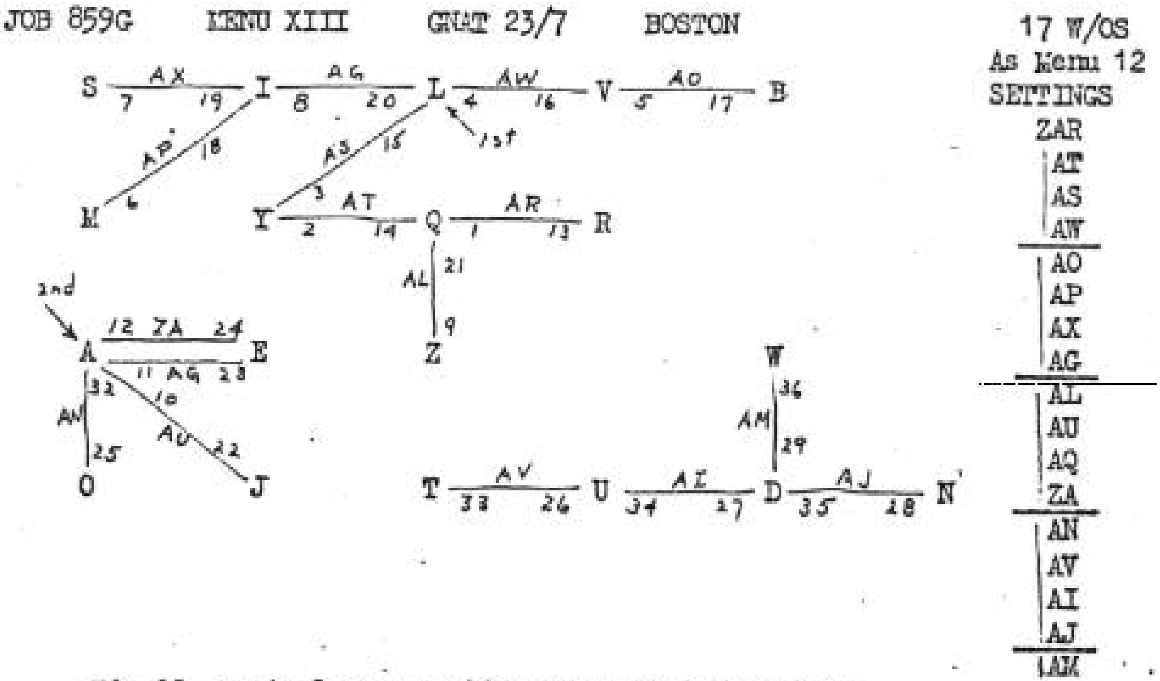
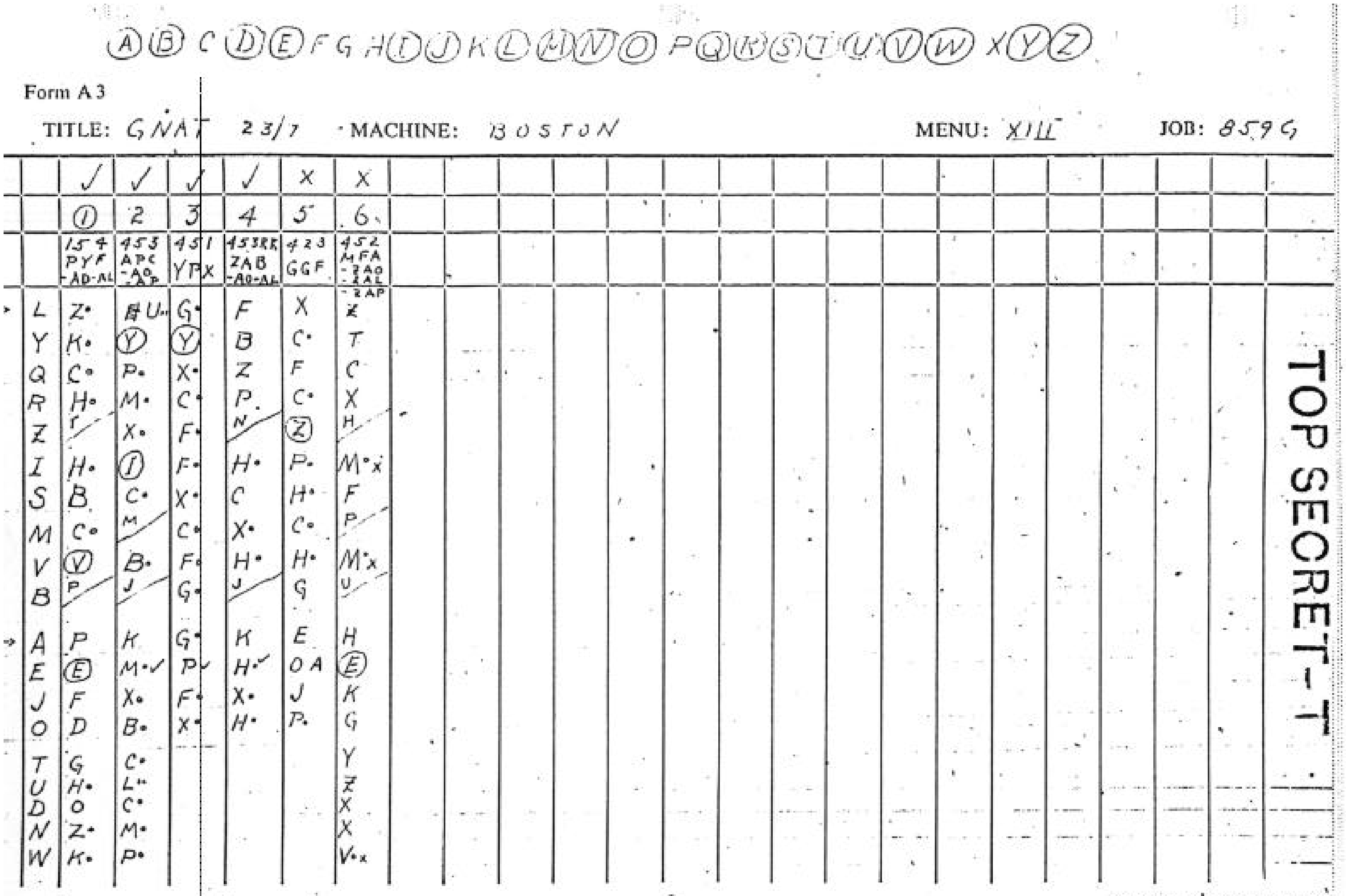


Fig.22. Typical Menu,Double Input With Subsidiary.

For the checking of this menu, see fig.23.



Ⓐ Ⓑ C Ⓓ Ⓔ F G H Ⓘ Ⓙ K Ⓛ Ⓜ Ⓝ Ⓞ P Ⓠ Ⓡ Ⓢ Ⓣ Ⓤ Ⓥ Ⓦ X Ⓨ Ⓩ

Form A3

TITLE: GNAT 23/7 MACHINE: BOSTON MENU: XIII JOB: 859G

TOP SECRET-T

	✓	✓	✓	✓	X	X
	Ⓘ	2	3	4	5	6
	154 PYF -AD-AL	453 APC -AO -AP	451 YPX	453RR ZAB -AO-AL	423 GGF	452 MFA -ZAO -ZAL -ZAP
L	Z•	~~B~~U•	G•	F	X	X
Y	K•	Ⓨ	Ⓨ	B	C•	T
Q	C•	P•	X•	Z	F	C
R	H• r	M•	C•	P. N	C•	X H
Z		X•	F•		Ⓩ	
I	H•	Ⓘ	F•	H•	P•	M•x
S	B	C• M	X•	C	H•	F P
M	C•		C•	X•	C•	
V	Ⓥ P	B• J	F•	H• J	H•	M•x U
B			G•		G	
A	P	K	G•	K	E	H
E	Ⓔ	M•✓	P✓	H•✓	O A	Ⓔ
J	F	X•	F•	X•	J	K
O	D	B•	X•	H•	P•	G
T	G	C•				Y
U	H•	L••				Z
D	O	C•				X
N	Z•	M•				X
W	K•	P•				V•x

*O.U.P. Form 34 (late B.P. Form No. 14

Fig. 23. Checking of Double Input With Subsidiary Menu Shown in Fig.22.

C.S.K.O. (Consecutive Stecker Knock Out). - It has been observed that some enemy encoders have a rule not to use consecutive letters for steckers,e.g. they would not use either A or C is a stecker for B. In breaking such traffic, stops which include such consecutive steckers can be thrown out. This is done automatically by the use of the CSKO jack which causes the bombe to reject such stops and continue testing. The CSKO jack is located in the column of COMMONS jacks just below the INPUT COMMONS and is painted red. To make the feature effective a short circuiting plug is inserted in the CSKO jack. This is the last plug put into the bombe when setting it up and is the first to come out when stripping. It's circuit is as follows:

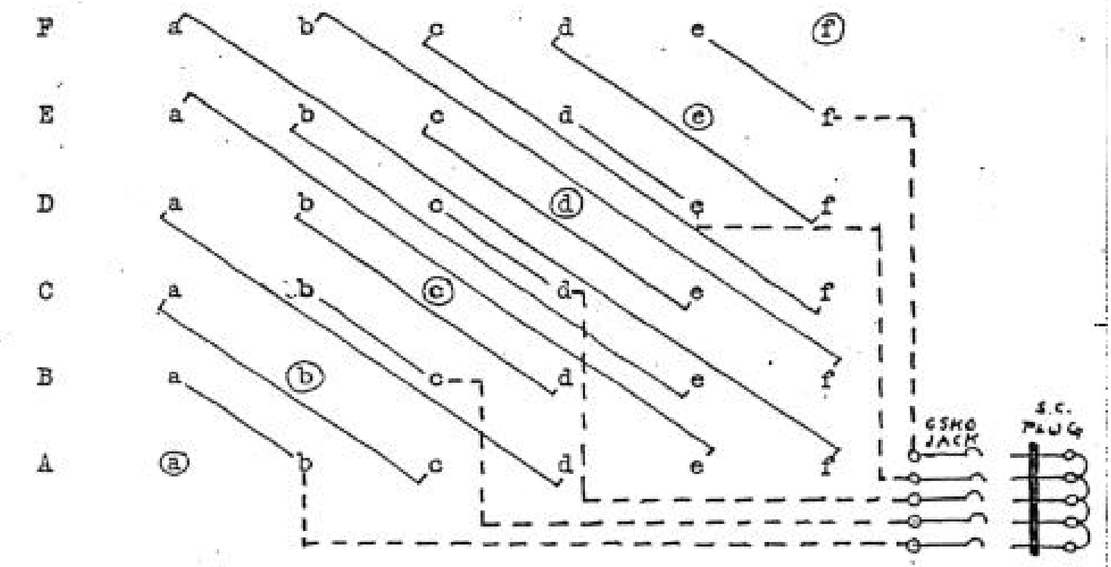


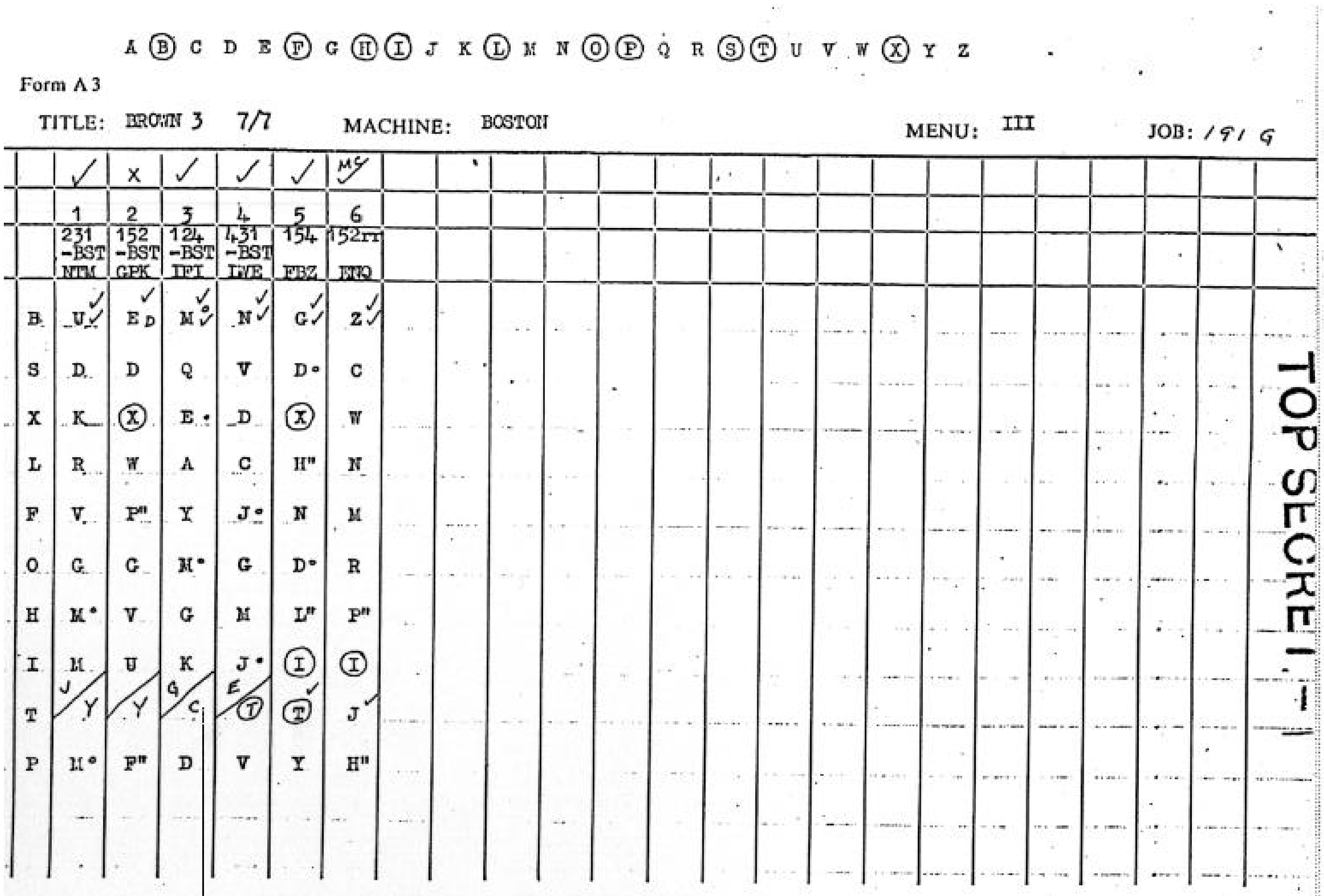
Fig. 24. Partial Circuit of CSKO Jack.

The condition for a stop is that one point on each row of the diagonal board has no current flowing through it. Let us assume we get a stop and find, by checking, the following steckers:

MENU	STECKER
F	E"
E	F"
D	B"
C	(C)
B	D"
A	(A)

We do not want the bombe to stop under this condition,as E is a consecutive stecker for F and vice versa, This will be accomplished through the CSKO jack which ties e on F and f on E to 2 points on each horizontal row. Since 25 points on each row will have current on them (only 1 point per row will not), this jack feeds current to c on F and f on E and rejects the stop.

Cilly Settings. -Certain enemy operators show a tendency to use stereotyped settings for the indicators at the beginning of their messages. They sometimes use the last position of the previous message as one of the indicators for this purpose. This practise gives the person breaking the message an insight into the probable settings for different links. The following is a typical menu taking advantage of this tendency:



TOP SECRET.

A Ⓑ C D E Ⓕ G Ⓗ Ⓘ J K Ⓛ M N Ⓞ Ⓟ Q R Ⓢ Ⓣ U V W Ⓧ Y Z

Form A 3

TITLE: BROWN 3 7/7 MACHINE: BOSTON MENU: III JOB: 191 G

	✓	X	✓	✓	✓	MS ✓
	1	2	3	4	5	6
	231 -BST NTM	152 -BST GPK	124 -BST IFI	431 -BST LWE	154 FBZ	152rr ENQ
B	U ✓✓	✓ E D	M ° ✓✓	N ✓✓	G ✓✓	Z ✓✓
S	D	D	Q	V	D°	C
X	K	Ⓧ	E •	D	Ⓧ	W
L	R	W	A	C	H"	N
F	V	P"	Y	J°	N	M
O	G	C	M•	G	D°	R
H	M•	V	G	M	L"	P"
I	M	U	K	J•	Ⓘ	Ⓘ
T	J / Y	/ Y	G / C	E / Ⓣ	Ⓣ ✓	J ✓
P	M°	F"	D	V	Y	H"

Fig. 26. Checking of Cilly Setting Menu Shown in Fig.25

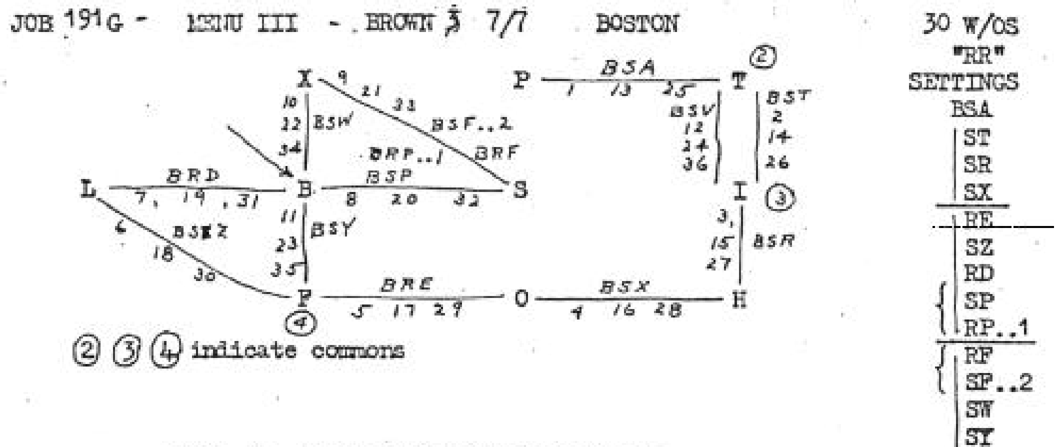
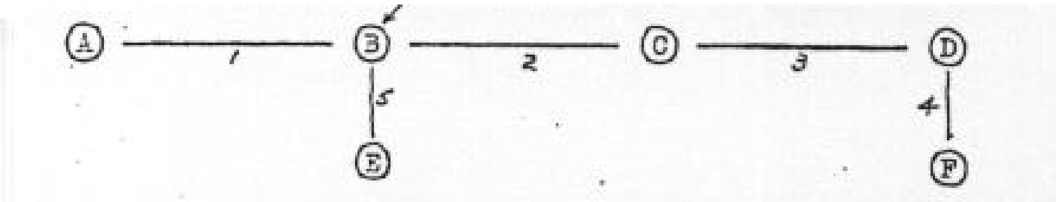


Fig. 25. Typical Menu,Cilly Settings.

The operator is instructed by this menu to use BSP as the setting of the drums on link BS for all wheel orders except those ending in 1, in which case he is to use the setting BRP. Similarly for the link SX BRF shall be used as the setting for all wheel orders except those ending in 2, in which case BSF is to be used. The checker must observe these same instructions. Samples of the checking of the above menu will be found in fig.26. In this message it is probable that the enemy operator did not change his indicators after each 250 letters of the message. Therefore the wheel settings are based on the reference point for the beginning of the message. Hence,BSA,BST,&.

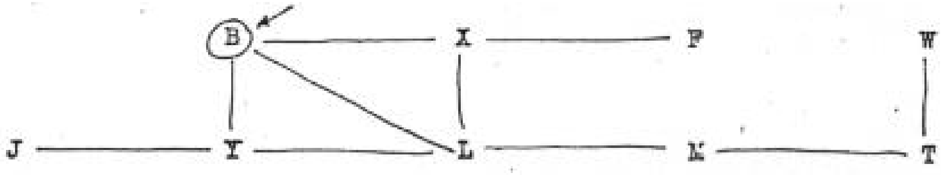
Phantom Links. - When the crib includes a letter and link which would make the menu too strong (give less than one stop per wheel order,and require the removal of more than one link to get a check stop) it is customary to include the letter and link in the menu but indicate it as a phantom. This is done by enclosing the link and letter in parentheses and marking it "phantom", in this fashion >E(-ZC/PH- L) |When a phantom is included in the menu it is disregarded by the bombe operator but is used in checking. In checking the letters of phantom links are placed at the bottom of the column of menu letters. To the left of each phantom letter is put the abbreviation PH. Legal contradictions involving the stecker of the phantom link letter are treated the same as legals on outlying links in the analysis of the stop.
The checker, should he get a HUT 6 stop, then checks the phantom to see whether it gives a legal contradiction. If it does and if the stop already included a legal contradiction, the stop becomes a bad stop. If the stop did not already include a legal contradiction ,and the phantom contributes only one legal contradiction, it is still considered a HUT 6 stop. However an illegal contradiction is also allowable on the phantom link,and provided it is the only contradiction on the stop it should be sent to HUT 6. It is customary to use from i to 3 phantoms.

Self Steckered Menus. - When a key is being used a second day it is only necessary to determine the wheel order and ringstellung for the second day. This is done by making a menu out of the known self steckered letters. The following would be a typical menu.



The circles around the letters means that they are self-steckered,and only stops where these letters are steckered to themselves are wanted. It can easily be seen that one such letter will decrease the number of stops by 25-1 because normally the machine will stop when it is steckered to any of the 26 but if we are only interested in one of the 26, the chances of it being that one is 25-i. By suppressing the others we arrive at the same condition we would have if we added a closure. The possible number of stops per wheel order is 26x26x26x26. Therefore with four self steckers we could run a menu which would average only 1 stop per wheel order. The searching point is usually put at some letter off the menu. The menu is plugged by the use of EEL plugs. An EEL plug is one in which the wires from the plug contacts are brought out to a plug board mounted on the plug and used with a "daisy chain". A "daisy chain" is a cord with 25 single conductor plugs connected to each other to permit short circuiting 25 of the letters. The plug is always inserted with the metal plate on the bottom and under that condition the plug board is designated A/B C/D --- Y/Z. In plugging the above menu,the inner end of enigma 1 would be patched to the first "common" jacks. An EEL plug with A left open is plugged into these common jacks. The plugging is similar for all other letters except that a different letter is left open on the EEL plug. On a completely self steckered menu you do not need a diagonal board. The bombe runs until it reaches a wheel order and ringstellung where all the above letters are self steckered. To make a check stop pull out the EEL plug furthest away from the input.

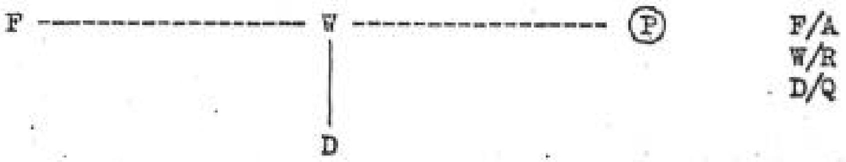
If there is a menu with one self stecker only, choose that as the input provided it is not a straggler. This gives a quick check that the correct relay is coming up. For example, if ,as below, the input is at B, only the B relay should appear on a stop.



A bombe stops when there is an open circuit on the input and, under normal conditions, one to three relays come up. If, with the input at B as indicated , relay F comes up there is an open circuit at F and current on the remaining positions. But we do not want to stop at F for this menu. So we short circuit all other letters except B which puts current on F and rejects the stop. For this example we plug the bombe normally and then in the common to which B is connected plug an EEL plug with the B point isolated,

Where a self steckered letter is used, commons must be employed except in extreme cases, such as in the first example where the EEL plugs can be plugged directly into the enigmas at A,C,D,E and F, using a common only at B(the input). The menu then becomes a Dummy Letter Menu in which contradictions are not permissible and each letter must be self steckered.

Prohibitive or Mandatory Steckered Menus. - This type of menu is similar to the self steckered menu except that some of the letters are specified to be coupled to letters other than themselves. For instance:



In this case EEL plugs are used for all the letters and arranged to couple the letters as indicated. The EEL plug at F will have A isolated , that at W will have R open and that at D will have Q isolated. P, of course is self steckered and it's EEL plug will have P open.

S.S.S (Single Self Steckered) Menus. Single Self steckered menus are those in which the correct stop is expected to have at least one self couple. Some of the bombes have been equipped with a special SSS socket installed on the diagonal board, the contacts of which connect consecutively to the self steckered points on the diagonal board. These bombes may then be plugged in such a way that they will stop only if there is one or more self steckers on the menu, The bombes so equipped are indicated on the IC OPS board. There are two methods of plugging
this type menu;

Method I. (For all ordinary menus having 3 or more links on the input).
The menu is plugged normally except: -

(a) the input is connected to a separate common other than the normal input common,
(b) the special SSS jack is connected to the same common,
(c) an EEL plug is inserted in the same common with all the letters off the menu plus the input letter plugged(short circuited.)
(d) searching is done at any letter off the menu.
(e) the relays that fall will indicate those letters which are self coupled.
@ (f) these are the letters from which checking will have to be started

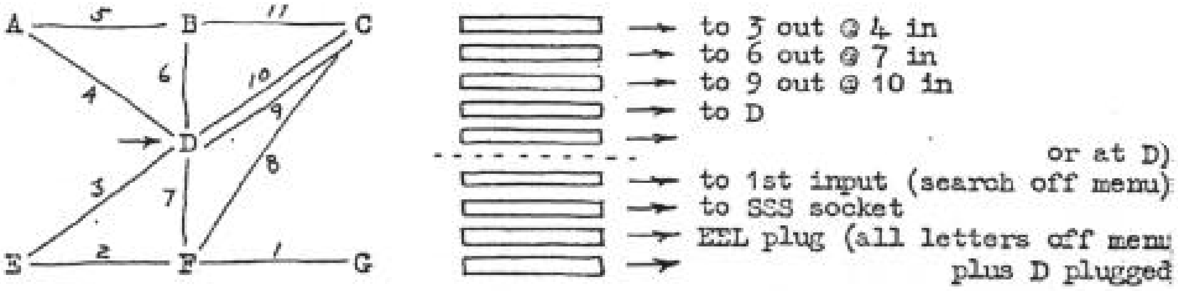


Fig. 27. Method I,Plugging Single Self Steckered Menus.

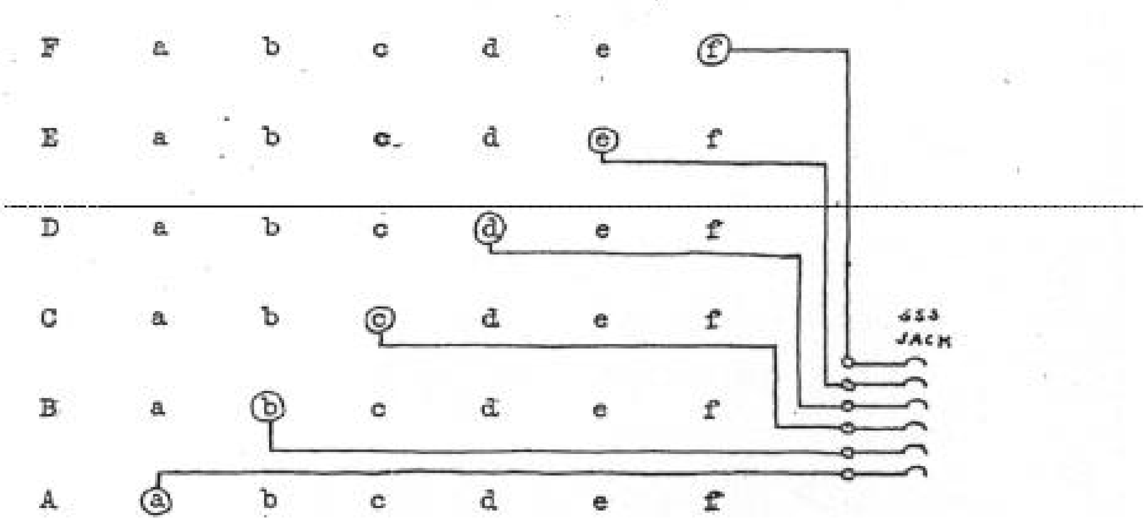


Fig. 28. Circuit of SSS(Single Self Steckered) Jack.

Method II. (For weak menus)
The menu is plugged normally except: -

(a) the SSS jack is connected to the set of commons below the normal input common.
(b) insert an EEL plug in the top jack of these commons with all letters off the menu connected together with a "daisy chain" leaving the unused plugs hanging.

Handwritten note at @: plugging arranged so that current from input reaches spider via SSS jack and all letters off menu are excluded by daisy chain plugging and same daisy chain is used to supply current to the search point

(c) the input is connected to the same common (Note: There is no enigma plugged to this common.)

(d) insert a 2nd EEL plug into the bottom jack of the input common (i.e. at D on example) The end plug Of the trailing daisy chain from the 1st EEL plug is connected to the normal searching position on the 2nd plug, NOT THE INPUT LETTER, and any searching switch of a letter off the menu is operated. The current is therefore put into the enigmas in the usual way but returns to the input through the self couple positions on the diagonal board. As soon as a straight is called with a self-couple on it the current does not return from that position and the differential relay concerned operates. THUS THE RELAY CALLED WILL BE THE SELF COUPLE OF LETTER ON THE MENU, and the stop will have to be checked from that point.

It will not be the coupling of the input letter.

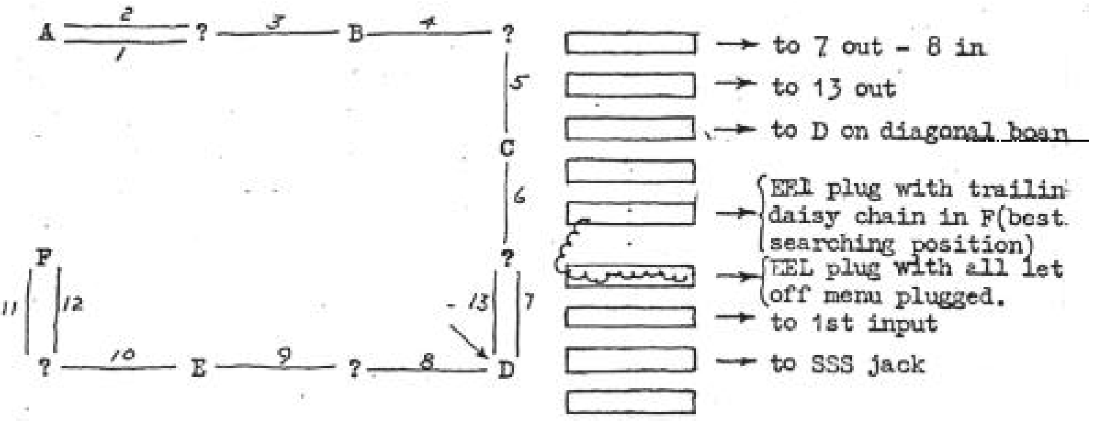

A
2
1
?
3
B
4
?
5
C
6
?
F
11
12
- 13
7
?
10
E
9
?
8
D
to 7 out - 8 in
to 13 out
to D on diagonal boan
EEl plug with trailin daisy chain in F(best searching position)
EEL plug with all let off menu plugged.
to 1st input
to SSS jack

Fig. 29. Method II, Plugging Single Self Steckered Menus.

Method III. (For double input menus)

The menu is plugged normally except: -

(a) plugging for the first input is as described above.

(b) SSS jack is plugged to a common which is plugged to second input.

(c) an EEL plug with all the letters off the menu plugged together is inserted in this common.

(d) any letter off the menu is used for the searching position on the 2nd input.

(e) use the double input board.

(f) when a stop occurs, the relays indicated for the first input will be the couples of the input letter, and those indicated on the second will be the self couples.

(g) this method should always be used when there is an auxiliary chain and the first input should be on the strongest chain.

Summary.

A stop may occur without a self-couple, if the relay on the 1st chain is the same as the searching letter. Under this condition the other 25 relays will show and all the relays on the menu will show on the 2nd input. If 25 relays show on the 1st input and not all those on the menu show on the 2nd, those missing will be self-couples.

When only one input is used and the searching letter is self-coupled,all relays on the menu except those self-coupled will come down.

It is possible for as many relays to be indicated as there are self-couples.

Dummy Letter Menus. - This type of menu is used when it is desired to put the menu on the bombe four times. The menu must consist of at least four closures and not more than nine letters. It is plugged up 3 times normally as a single input menu. For the 4th time no diagonal board is used. The 4th chain does not cut out illegal contradictions since it does not use a diagonal board. A stop is considered good if it has one contradiction either legal or illegal . Assume the following menu:

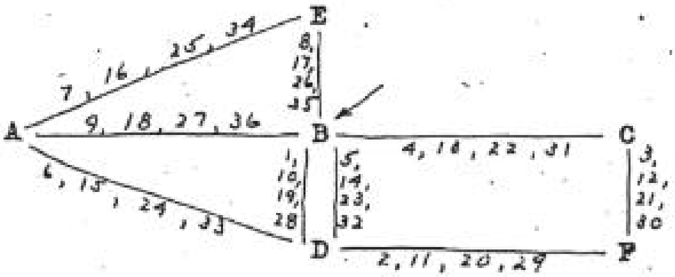


Fig. 30. Typical Dummy Letter Menu.

The menu is plugged as follows:

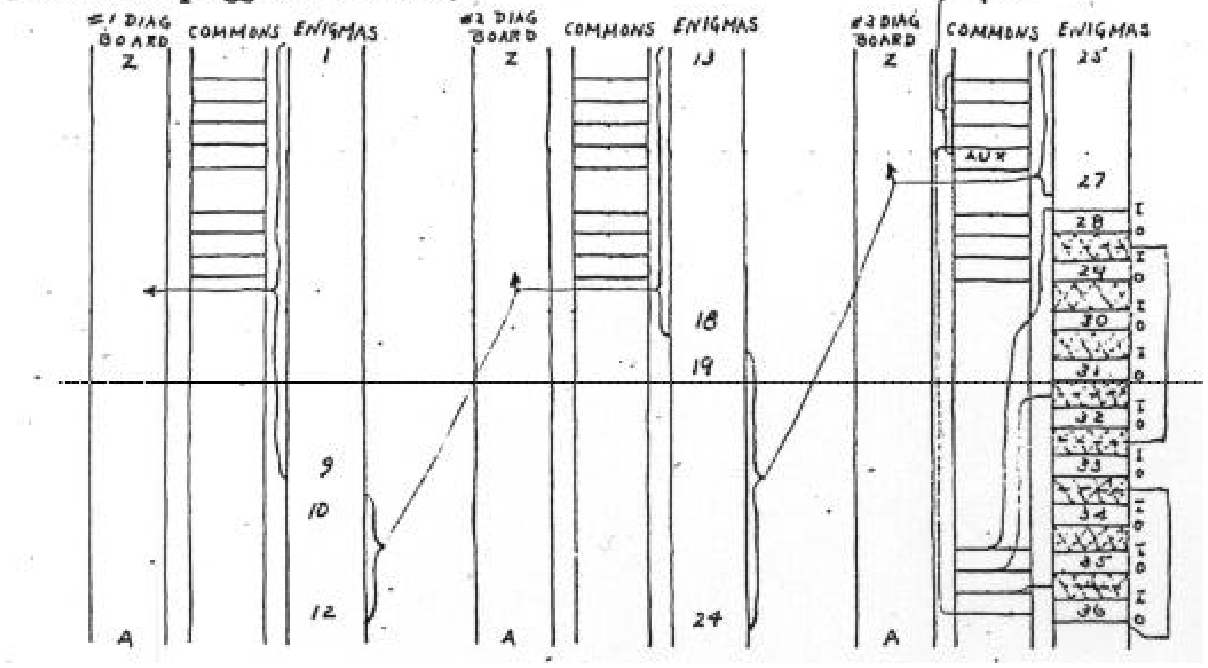


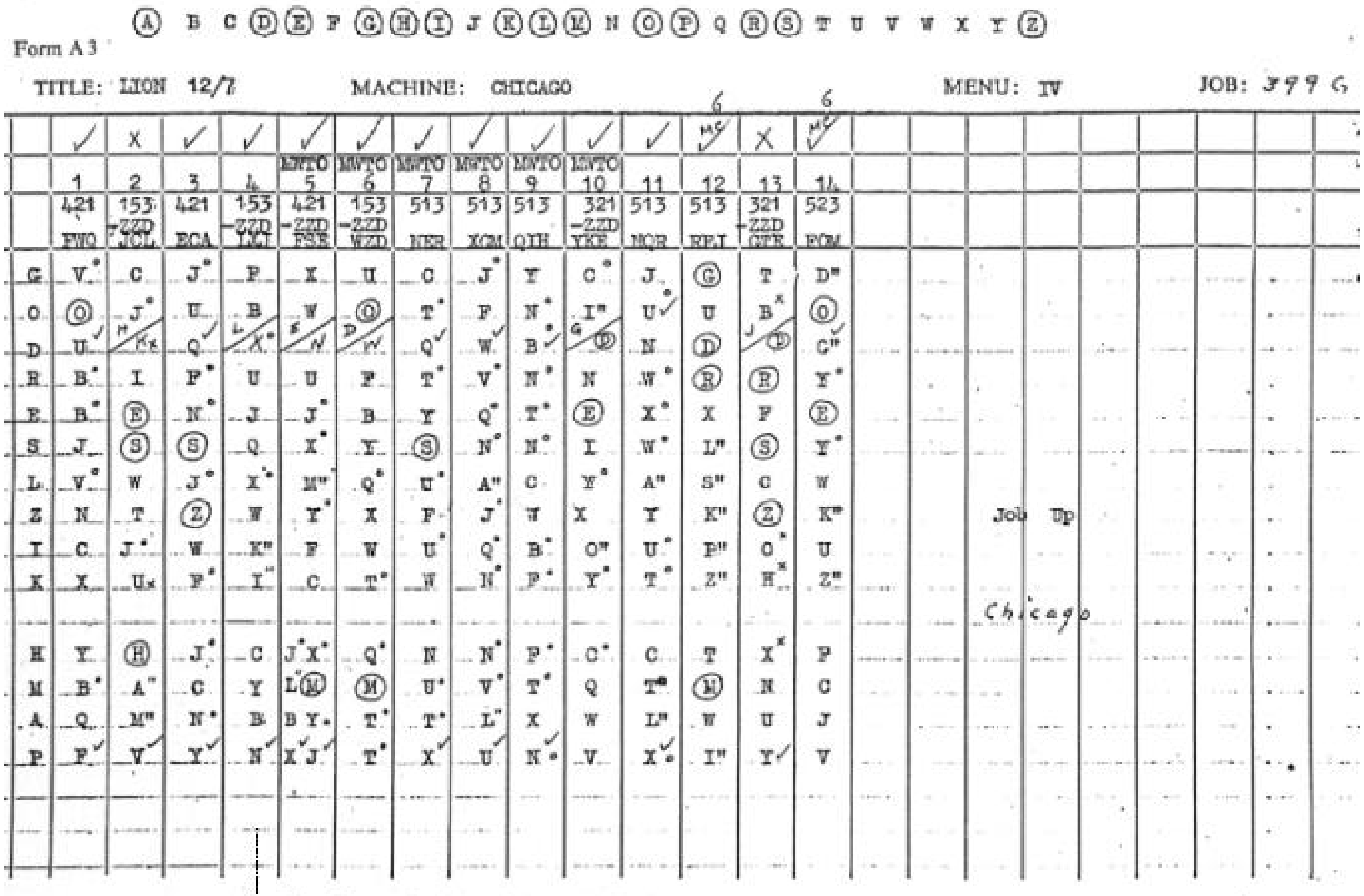
Fig. 31. Plugging for Dummy Letter Menu in Fig.30.

There is no diagonal board available for the 4th chain - hence all patching is made as if all letters were query letters and commoning plug-jacks are patched together directly to avoid the use of cords and common jacks.

When a relay appears on the third alphabet it may be a stop on either the 3rd or 4th input. In order to determine to which bank it belongs turn off the carry and the 4th chain. If the relay returns the stop must be on the 3rd bank. When sending stops to the checker on the dummy bank, the operator must label each stop D.L. , because since the menu is not plugged to the diagonal board, all the stops with illegal contradictions will be correct (providing the stop goes round all the closures). Although illegal contradictions are permitted on the dummy bank, the right stop cannot contain legals or illegals.

Query Letter Menus . - Sometimes the enemy operator encodes his wheel position twice as ART UXG ART ZET. Hence ART is the point at which to set the wheels and decode UXG to get the wheel setting for the message. UXG represents encodement at positions ZZA,ZZB,ZZC while ZFT represents encodement of the same indicator at

Handwritten Note: 10/NOV/44 (A recent notice from BP states that if a query letter menu marked SSO is being checked, only stops which have a different (unreadable) including those on (unreadable) links should be sent.)



A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Form A3

TITLE: LION 12/7 MACHINE: CHICAGO MENU: IV JOB: 3796

												6		6
	✓	X	✓	✓	✓	✓	✓	✓	✓	✓	✓	MC ✓	X	MC ✓
					MWTO	MWTO	MWTO	MWTO	MWTO	MWTO				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
	421	153	421	153	421	153	513	513	513	321	513	513	321	523
		-ZZD		-ZZD	-ZZD	-ZZD				-ZZD			+ZZD	
	FWO	JCL	ECA	LXI	FSE	WZD	NER	XCM	QIH	YKE	NQR	RPJ	GTR	POM
G	V	C	J	P	X	U	C	J	Y	C	J	G	T	D"
O	O	J	U	B	W	O	T	F	N	I"	U ✓	U	B×	O
D	U ✓	H / Kx	Q ✓	L / X	E / N	D / W ✓	Q ✓	W ✓	B ✓	G / D	N	D	J / D	C" ✓
R	B	I	P	U	U	F	T	V	N	N	W	R	R	Y
E	B	E	N	J	J	B	Y	Q	T	E	X	X	F	E
S	J	S	S	Q	X	Y	S	N	N	I	W	L"	S	Y
L	V	W	J	X	M"	Q	U	A"	C	Y	A"	S"	C	W
Z	N	T	Z	W	Y	X	F	J	W	X	Y	K"	Z	K"
I	C	J	W	K"	F	W	U	Q	B	O"	U	P"	O	U
K	X	Ux	F	I"	C	T	W	N	P	Y	T	Z"	H×	Z"
H	Y	H	J	C	J X	Q	N	N	P	C	C	T	X×	P
M	B	A"	C	Y	L"M	M	U	V	T	Q	T"	M	N	C
A	Q	M"	N	B	B Y	T	T	L"	X	W	L"	W	U	J
P	P ✓	V ✓	Y ✓	N ✓	X ✓ J ✓	T	X ✓	U ✓	N ✓	V	X ✓	I"	Y ✓	V

Job Up

Chicago

Fig. 34. Checking for Typical Middle Wheel Turnover Menu of Fig.33.

positions ZZD,ZZE and ZZF under these conditions it is known that the first letter of the indicator is coupled to both U and Z. On the menu this is shown U -- ? -- Z. A typical menu would look like this:

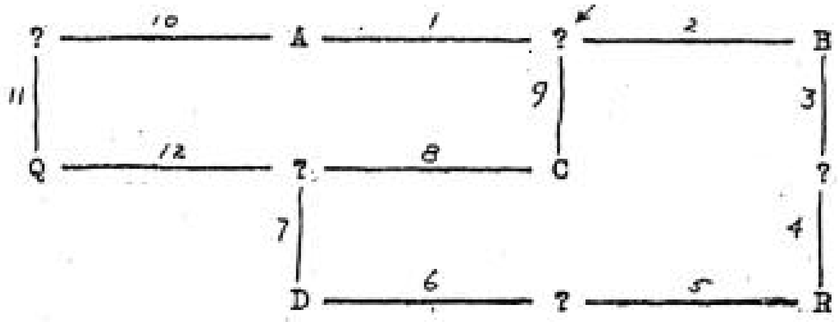
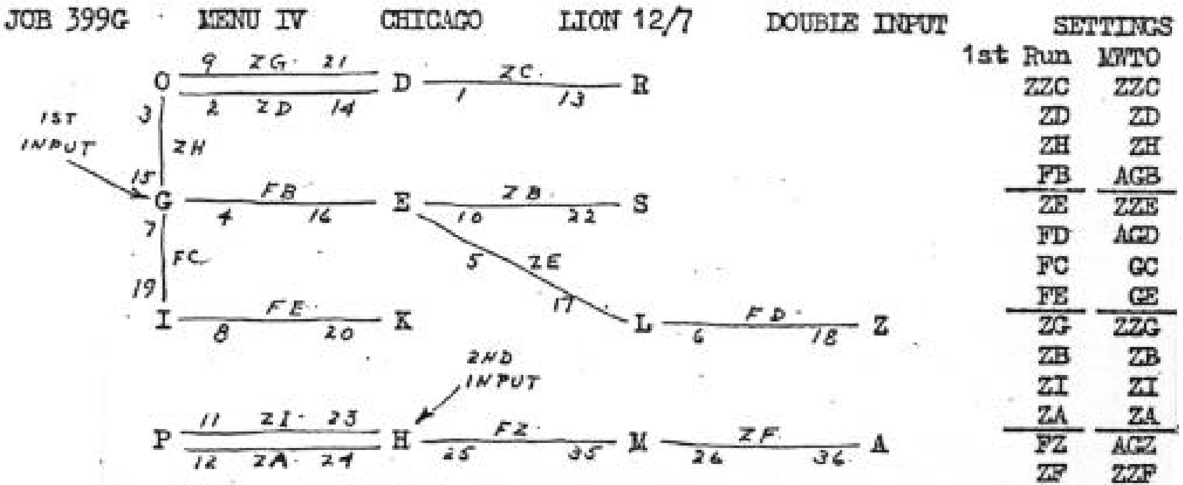


Fig. 32. Typical Query Letter Menu.

It is plugged by merely tying those ends of enigmas serving query letters (?) together with commoning plugs, not patching them to the diagonal board. On the check sheet the query letters are identified by numbering. The steckers for the query letters are set down in a separate column. When the stop is evaluated the query letter steckers are disregarded.

Middle Wheel Turnover Menus. - This type of menu is used for "top and tail" cribs in which cribs have been made of the heading and closing of a message. In such a case it is assumed that the middle wheel has turned over and moved the slowest wheel at least one position. The bombe operator is asked to run first at ZZ- settings and then make the same runs with these wheels advanced. The following is a sample of such a menu:



SETTINGS

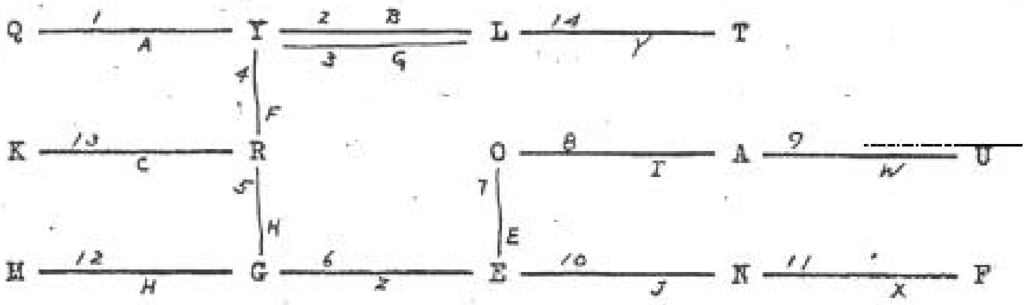
1st Run	MWTO
ZZC	ZZC
ZD	ZD
ZH	ZH
FB	AGB
ZE	ZZE
FD	AGD
FC	GC
FE	GE
ZG	ZZG
ZB	ZB
ZI	ZI
ZA	ZA
FZ	AGZ
ZF	ZZF

Fig. 33. Typical Middle Wheel Turnover Menu.

In this menu it is assumed that for settings ZF- the middle wheel turns one position and that its notch was effective and moved the slowest wheel one position. The resultant positions are AG-.

Hoppity Menus. A hoppity menu is an ordinary menu with definite changes during one run when the slow wheel reaches a designated letter,the center wheel shall be moved ahead one place of the indicated enigma. A typical hoppity menu follows:

DAFFODIL (AF)(ADM).



Changes.

N	M	L	K	J	I	H	F	E	D	C	B	A
12	10	8	5	3	4	7	13	2	1	6	14	11

Fig. 35. Typical Hoppity Menu.

Delayed Hoppity Menus. - This type of menu is used when the turnover point can't be determined by ordinary means. The menu is first run through with all settings normal. Then a run is made with the center wheel advanced one position on the enigma whose setting is nearest ZZZ. Successive runs are made advancing the center wheel of the enigma next further away from setting ZZZ. Stops are indicated on the stop slips as follows:

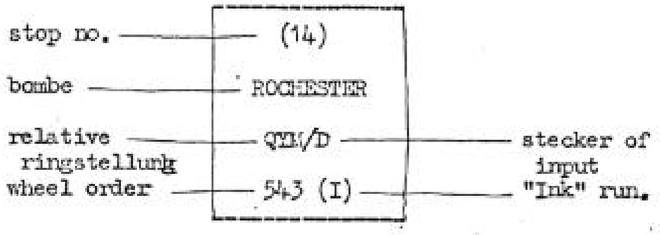
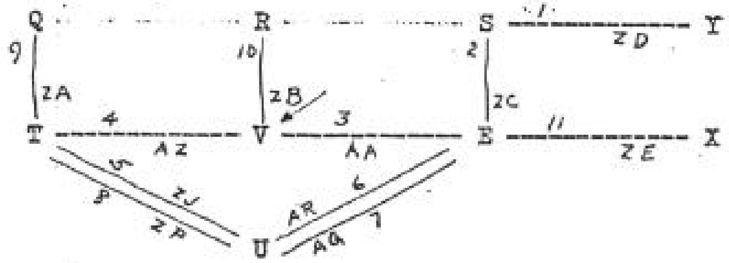


Fig. 36. Typical Delayed Hoppity Stop Slip.

A typical delayed hoppity menu is shown below:



[See Folder, Master Change Delayed Hoppities and Hoppies

Links in order of plugging	Links in order of change
ZZD	-4
ZC	-5
AA	-11
AZ	-8
ZJ	-2
AR	-9
AQ	-10
ZP	-1

ZZA	-7
ZB	-6
ZE	-3

Run no. 1 - All settings normal

" " 2 - ("O" run) advance middle wheel of enigma 8 one position from ZZP to ZAP.

" " 3 - ("I" run) advance middle wheel of enigma 5 one position from ZZJ to ZAJ. Leave enigma 8 in the ZAP setting.

Continue process until 12 runs are complet for this W/O

D Uncle Walter. - Several varieties of Uncle Walter have been used with the enigma machine. The A and B type were used during the Spanish Civil War. In the summer of 1940 the German Air Force started using the C Uncle Walter and then put it aside for the B. On 27 Dec 1944 we intercepted some clear text asking if the other station had their U/W Dora. A new unknown U/W would introduce 150 million,million possible combinations. However they did not change to the new D U/W on 1 January as expected. But Norway was using the D U/W with the same stecker board, wheel order and ringstellung as those using the B board. As a result on 2 January we found the wiring of Uncle Dick. On 11 January some Norway messages didn't decode, which led to the conclusion that Uncle Dick must be variable. Between 1 January and 1 March 7 different wirings of Uncle Dick were encountered. In all of them B was always paired with 0.

On 9 March the Russians captured the RED key, which forced the Germans to use Uncle B for the rest of the month. A new call sign book came out on 1 April. 3 different wirings of Uncle D were introduced on 9,21,30 April respectively. From the above experience it was assumed that Uncle Dick was pluggable.

By 1 May the Germans were changing the stecker 3 times a day. But they had to abandon this on 10 June because of so many operators errors. There were no changes during June and July. In July we captured A RED key sheet in Normandy which gave the U/W wiring for each 10 day period. This verified the fact that Uncle Dick was pluggable.

If the use of Uncle Dick is continued, new decoding equipment will have to be installed. Every 10 days it will be necessary to find another of 150,OOO,OOO,OOO,000 possible D wirings. It usually takes 5 of our mathematicians about 2 weeks of hibernation to get the solution. The Giant was developed for finding pluggable U/W's and takes 3 to 4 weeks to complete a menu. The second Scheme adopted to solve the problem was to use a 4 wheel machine with pluggable U/W. This took 16 days to complete a menu.

On 15 August the U.S. put out a 24-hour machine called DUENA. (DUENA - U.S. Navy, AUTO SCRIPTER - U.S.Army, Arlington)

The D U/W is coming into frequent use on our machines. The U/W wiring will be sent through from BP. Each wiring will be given a serial number. Menus are received with the serial number to be used. The following is the method of plugging the U/W extension to the bombe. There are three jack rails on the extension and reading from left to right they refer to Banks 3,2, and 1. The U/W wiring consists or 13 pairs of letters; for example

```
A  B  C  D   etc
Y  0  L  J
```

To plug this one end of a plug is inserted in "A" and the other end reversed and plugged in "Y". Another plug is placed in "B" while the other end is reversed and put in "O" and so on. All 3 banks are plugged in the same way.. Great care must be taken to insure that only one plug of the cord is upside down and that all contacts on the plugs are straight, since it takes longer to trace trouble on this than on ordinary patching.

In order to set up a checking machine for this type of menu there should be a STRAIGHT drum in the 4th wheel position. The plug at the side of machine must be removed. An EEL plug is inserted. This is plugged in the same way as the U/W. With the ESL plug held upside down the connections are then as follows;-

```
-------------------------
-------------------------    Metal strip.
A C E G I K M O Q S U W Y
B D F H J L N P R T V X Z
```

To plug up, use the plugs provided to connect the letter required in the same combination as on the bombe.

Hints. - When a board has been plugged, check that you have:

1. 13 plugs the right way and 13 upside down.
2. Check that all plugs are firmly in position.

Continuity and Short tests should be made before the job has been plugged. A quick way of finding open circuits is to plug a trolley to the enigma concerned. If a plug from the U/W is removed 2 lights should go out. If only one extinguishes this must be in the same circuit as the one already out.

"D U/W" with its serial number must be clearly shown on the Job and Checking Sheets and entered into Log Books. Operators should not strip D U/W.

Shorts on U/W Boards, - If, when short testing a machine which is using D boards, a short is indicated between two enigmas, it is more likely to be caused by two adjacent contacts touching on the U/W. Using the trolley in the orthodox manner it is difficult to isolate the fault but this can be overcome quite easily by a slight deviation. Having localized the fault to two enigmas, isolate them by removing the coupling jacks and proceed as follows:

Plug the top lead from the trolley to one end of the first enigma, and the bottom lead to one end of the second. The only possible continuity between the two enigmas is through The short and this will show by lighting one lamp on the trolley. If straight drums are put on the first enigma then the lamp will indicate the faulty letter on the U/W. By reversing the trolley input and putting the straight drums on the second enigma, the shorted letter on this enigma will be indicated. The plug of the letter in question can now be inspected on the U/W in the usual way.