‘BUTTONING UP’

(A method for recovering the wiring of the rotors used in a non-stecker Enigma)

A description of the code-breaking technique known as ‘Rodding’, currently available on the Bletchley Park website, shows how the ‘*rod square*’ tables for the Enigma rotors were used to make the required sets of rods. However before a particular table could be constructed it was first necessary to determine the complete sequence of letters in the left-hand column of the table, known as the ‘1st upright’. From this upright it was then possible to construct the entire table, and also find the internal wiring of the corresponding rotor.

Clearly the establishment of a procedure for finding the 1st upright was of fundamental importance, and in the following notes an account is given of the one originally devised by the veteran code-breaker ‘Dilly’ Knox. These include an illustrative example to demonstrate the effectiveness of the procedure, which involved a process referred to by Knox as ‘*buttoning up*’.

In order to understand what is to follow, it is essential to have read pages 1 to 4 from the notes on ‘Rodding’ given elsewhere on this website.

During the Spanish Civil War the Italian Navy made some use of the commercial Enigma machine but with differently wired rotors, and it was in 1937 that Knox recovered the internal wiring of these. The so called ‘Railway’ Enigma has the same basic structure as the machine used by the Italians, and as a computer emulation of it happens to be available, it has been used instead of the Italian machine, to generate the cipher messages used in these notes.

Both of these versions of the Enigma machine (which did not have plug-boards), had an entry disc on which the electrical contacts were connected to the keyboard in the sequence:- **QWERTZUIOASDFGHJKPYXCVBNML** (in a clockwise sense when viewed from the right-hand side of the machine). As a logical consequence of this, the letters in all the diagonals (from top right to bottom left) of the rod squares, form cyclic sequences of letters in the order shown above.
As described elsewhere, a set of rods was based on the strips formed by dividing the corresponding rod square into its twenty-six individual horizontal rows.

The basis of the method that Knox employed to find the 1st upright from a rod square depended upon the property of the diagonals in the rod squares described above, and on the way in which the rods were to be used to decipher messages. Initially of course the details of both the rod squares and the individual rods would not have been known.

The ‘rod square’ table for Rotor I from the ‘Railway’ Enigma is shown below, and it will be observed that the letter sequences in the diagonals in the table (top right-bottom left) do conform to the cyclic ‘QWERTZU…’ sequences previously described.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
q	C	U	L	H	I	V	Y	R	P	S	D	M	T	K	W	G	B	J	B	F	X	N	O	Q	M	A
w	I	Q	J	O	B	X	T	Y	D	F	L	Z	P	E	H	N	K	N	G	C	M	A	W	L	S	V
e	W	K	A	N	C	Z	X	F	G	Q	U	Y	R	J	M	P	M	H	V	L	S	E	Q	D	B	O
r	P	S	M	V	U	C	G	H	W	I	X	T	K	L	Y	L	J	B	Q	D	R	W	F	N	A	E
t	D	L	B	I	V	H	J	E	O	C	Z	P	Q	X	Q	K	N	W	F	T	E	G	M	S	R	Y
z	Q	N	O	B	J	K	R	A	V	U	Y	W	C	W	P	M	E	G	Z	R	H	L	D	T	X	F
u	M	A	N	K	P	T	S	B	I	X	E	V	E	Y	L	R	H	U	T	J	Q	F	Z	C	G	W
i	S	M	P	Y	Z	D	N	O	C	R	B	R	X	Q	T	J	I	Z	K	W	G	U	V	H	E	L
o	L	Y	X	U	F	M	A	V	T	N	T	C	W	Z	K	O	U	P	E	H	I	B	J	R	Q	D
a	X	C	I	G	L	S	B	Z	M	Z	V	E	U	P	A	I	Y	R	J	O	N	K	T	W	F	Q
s	V	O	H	Q	D	N	U	L	U	B	R	I	Y	S	O	X	T	K	A	M	P	Z	E	G	W	C
d	A	J	W	F	M	I	Q	I	N	T	O	X	D	A	C	Z	P	S	L	Y	U	R	H	E	V	B
f	K	E	G	L	O	W	O	M	Z	A	C	F	S	V	U	Y	D	Q	X	I	T	J	R	B	N	S
g	R	H	Q	A	E	A	L	U	S	V	G	D	B	I	X	F	W	C	O	Z	K	T	N	M	D	P
h	J	W	S	R	S	Q	I	D	B	H	F	N	O	C	G	E	V	A	U	P	Z	M	L	F	Y	T
j	E	D	T	D	W	O	F	N	J	G	M	A	V	H	R	B	S	I	Y	U	L	Q	G	X	Z	K
k	F	Z	F	E	A	G	M	K	H	L	S	B	J	T	N	D	O	X	I	Q	W	H	C	U	P	R
p	U	G	R	S	H	L	P	J	Q	D	N	K	Z	M	F	A	C	O	W	E	J	V	I	Y	T	G
y	H	T	D	J	Q	Y	K	W	F	M	P	U	L	G	S	V	A	E	R	K	B	O	X	Z	H	I
x	Z	F	K	W	X	P	E	G	L	Y	I	Q	H	D	B	S	R	T	P	N	A	C	U	J	O	J
c	G	P	E	C	Y	R	H	Q	X	O	W	J	F	N	D	T	Z	Y	M	S	V	I	K	A	K	U
v	Y	R	V	X	T	J	W	C	A	E	K	G	M	F	Z	U	X	L	D	B	O	P	S	P	I	H
b	T	B	C	Z	K	E	V	S	R	P	H	L	G	U	I	C	Q	F	N	A	Y	D	Y	O	J	X
n	N	V	U	P	R	B	D	T	Y	J	Q	H	I	O	V	W	G	M	S	X	F	X	A	K	C	Z
m	B	I	Y	T	N	F	Z	X	K	W	J	O	A	B	E	H	L	D	C	G	C	S	P	V	U	M
l	O	X	Z	M	G	U	C	P	E	K	A	S	N	R	J	Q	F	V	H	V	D	Y	B	I	L	N

Rod square for Rotor I

Two of the rods formed by individual rows from this table are shown below side by side, and above them a short sequence of letters from a message in cipher (it is supposed that the rods are correctly aligned with the cipher and are paired through the machine as described in the notes on 'Rodding' given elsewhere on this website).

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

The four letters from the message that have been deciphered by the rods are:- W, O, B and A. Note that two adjacent letters in the cipher message (A and N) happen to be the same as a pair of adjacent letters on the upper rod, and this leads to the corresponding pair of adjacent letters O and B on the lower one. A pair of adjacent letters on the same rod was referred to by Knox as a '*beetle*', so that the letter pair AN is one example of a beetle and the letter pair OB is another.

If in a cipher message two successive letters form a beetle in the correct rod position, the corresponding deciphered letters will form a beetle on another rod.

In their original fixed locations in the rod square it is unlikely that the two rods will be in adjacent rows, and usually they will be separated from each other by an unknown number of other rows, as is the case for the pair of rods in the example. These are shown in their true locations in the following diagram, which only illustrates the relevant part of the rod square.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
q																										
w																										
e	W	K	A	N	C	Z	X	F	G	Q	U	Y	R	J	M	P	M	H	V	L	S	E	Q	D	B	O
r																										
t																										
z	Q	N	O	B	J	K	R	A	V	U	Y	W	C	W	P	M	E	G	Z	R	H	L	D	T	X	F
u																										
i																										

The two corresponding rows from the rod square (beetles outlined)

The diagonals in this rod square will have the invariant property previously described, namely that the letters in each diagonal always conform to the cyclic sequence based on the letter order of the terminals on the entry disc. For the version of Enigma machine being used here, as already noted the letters in each diagonal reading from top right to bottom left are in the cyclic sequence:-

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

Using this information it is possible to insert additional letters into the cells of the diagonals, to the left and below each of the beetles shown in the following diagram, which conform to this cyclic sequence. (Some additional empty rows have been introduced into the diagram in order to avoid overlaps between these additional letters.)

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

This provides a useful starting point for an explanation of the procedure used to recover the letter sequence forming the 1st upright in a rod square.

Consider the above diagram from a point of view in which there is no prior knowledge about the structure of the upright, but it is known that the two 'Enigma alphabet' letter pairs (AO) and (NB) occur at the 3rd and 4th positions in the message. (i.e. A would encipher as O at the 3rd position, and N would encipher as B at the 4th position). The sequences of letters in the two 'descending;' diagonals from the two letters A and N are respectively ASD and NMLQ, and likewise the two 'descending' diagonals from the pair of letters O and B are respectively OAS and BNML. It will be observed that as a consequence of these sequences, the 1st upright contains the two pairs of adjacent letters DQ and SL.

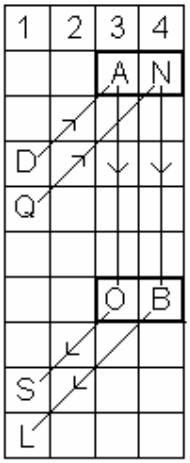
Alternatively from another point of view if it is assumed that the 1st upright contains the letter pair DQ, then the existence of the two alphabet letter pairs (AO) and (NB) jointly leads to the conclusion that the 1st upright will also contain the letter pair SL.

This conclusion can also be established by the use of the following procedure:-
The two letters 'A' and 'O' at the 3rd position are replaced by the corresponding two letters (D and S) at the 1st position in their 'descending' diagonals.

Likewise the two letters 'N' and 'B' at the 4th position are replaced by the corresponding letters (Q and L) at the 1st position in their 'descending' diagonals.

In this way the two Enigma letter pairs (AO) and (NB) are replaced by two new letter pairs (DS) and (QL). (This is the process that was originally referred to by Dilly Knox as '*buttoning up*'.)
The new letter pairs (DS) and (QL) lead directly to the two deductions:-
D→ S and Q→ L, which when considered jointly, give the same result as before (i.e. that if the 1st upright contains the letter pair DQ, it must also contain the letter pair SL.)

This procedure is illustrated in the following diagram and tables:-



Enigma letter pairs occurring at the designated positions

1	2	3	4
		A O	N B

corresponding pairs of 'buttoned up' of letters in the 1st column

1	2	3	4
		DS	QL

The final conclusion can be obtained directly from the table containing the pairs of 'buttoned up' letters, without any reference to the diagram. In general, once such a table has been constructed from a number of Enigma letter pairs, it can be used to derive the deductions for adjacent letter pairs in the 1st upright without any further reference to the sequences of letters in the diagonals.

The process of buttoning up is carried out by using the diagonal sequence:-
Q W E R T Z U I O A S D F G H J K P Y X C V B N M L
For example suppose that letter 'X' from an Enigma pair occurs at the 6th position, then beginning at 'X' in the above sequence then a displacement of five positions down the diagonal (from right to left) will lead to 'M', the corresponding 'buttoned up' letter at the 1st position.
If instead the given letter from an Enigma pair happened to be 'N' then a displacement of five positions down the diagonal will lead to the 'buttoned up' letter 'E' (a consequence of the cyclic nature of the diagonal sequence).

In order to apply this process usefully, it is first necessary to discover a number of Enigma alphabet letter pairs for about six consecutive positions of the Enigma rotors. (An analysis by Alan Turing showed that roughly around 100 Enigma alphabet letter pairs are required.) All of the letters in the alphabet pairs are then 'buttoned up' and by means of them, an initial assumption about the identity of one pair of adjacent letters on the 1st upright can be used to make logical conclusions about other adjacent letter pairs, which in turn can then be used as the basis for further similar conclusions.
If the initial assumption happens to be false, then this will soon become evident, as logical contradictions will arise between some of the outcomes.

These ideas lead to a procedure in which a sequence of possible initial assumptions are tested one by one, until a correct assumption is found that does not lead in any inconsistent conclusions and indeed is very likely generate some confirmatory (repeated) ones.

Success in the task of identifying Enigma alphabet letter pairs depends upon finding cribs for the intercepted cipher messages. The precise pre-war circumstances that enabled Knox and his colleagues to obtain a sufficient number of these letter pairs are not known, but it is believed that during the Spanish Civil War the Italian Navy sometimes transmitted signals that had been enciphered with the same Enigma configuration. Provided that a sufficient number of these had been intercepted and identified, they would have provided a set of messages 'in depth' enabling the task in hand to be successfully completed.

Given such a set of messages in depth, and starting with one or two cribs based on likely words, it is possible to find cribs for the others by using the reciprocal rule imposed on Enigma encipherments, and also applying some of the skills of a solver of crosswords. Once this task has been completed, then from the resulting Enigma alphabet letter pairs, the 1st upright in the rod square table can be found, this in turn leading to the wiring of the corresponding rotor.

The following contrived list of clear texts and enciphered texts will be used as a basis for a practical illustrative example of the task of finding the 1st upright in a rod square. (A number of these were composed by someone with real wartime experience of this type of work, and are reminders of episodes from the past that were in some way related to cryptology.)

1	**E**	**N**	**E**	**M**	**Y**	**X**	**S**	**I**	**G**	**H**	**T**	**E**	**D**				13	**S**	**E**	**N**	**D**	**X**	**A**	**D**	**D**	**R**	**E**	**S**	**S**	**X**		
	U	X	Q	B	E	J	Y	O	Z	W	P	H	X					A	K	L	S	K	R	B	X	L	F	X	W	D		
2	**P**	**E**	**R**	**S**	**O**	**N**	**A**	**L**	**X**	F	**O**	**R**					14	**N**	**O**	**T**	**H**	**I**	**N**	**G**	**X**	**T**	**O**	**X**	**R**	**E**	**P**	
	F	K	T	D	C	H	K	E	S	E	B	X						X	L	R	K	P	H	M	D	F	V	S	X	T	O	
3	**I**	**N**	**F**	**O**	**R**	**M**	**A**	**T**	**I**	**O**	**N**	**X**					15	**M**	**E**	**R**	**R**	**Y**	**X**	**C**	**H**	**R**	**I**	**S**	**T**	**M**	**A**	**S**
	Y	X	M	X	L	Y	K	Z	P	V	M	R						C	K	T	T	E	J	R	K	L	L	X	B	P	Q	R
4	**R**	**E**	**C**	**E**	**I**	**V**	**E**	**D**	**X**	**Y**	**O**	**U**	**R**				16	**F**	**O**	**R**	**X**	**C**	**A**	**P**	**T**	**A**	**I**	**N**	**X**			
	G	K	K	V	P	T	V	X	S	P	B	C	S					P	L	T	O	O	R	F	Z	D	L	M	R			
5	**I**	**M**	**M**	**E**	**D**	**I**	**A**	**T**	**E**	**X**	**F**	**O**	**R**				17	**B**	**L**	**E**	**T**	**C**	**H**	**L**	**E**	**Y**	**X**	**P**	**A**	**R**	**K**	
	Y	J	F	V	V	D	K	Z	V	S	J	N	S					J	O	Q	R	O	N	H	L	M	S	T	K	S	Y	
6	**A**	**C**	**T**	**I**	**O**	**N**	**X**	**T**	**H**	**I**	**S**	**X**	**D**				18	**H**	**E**	**A**	**V**	**Y**	**X**	**A**	**T**	**T**	**A**	**C**	**K**			
	S	V	R	Q	C	H	O	Z	W	L	X	R	X					L	K	G	E	E	J	K	Z	F	Q	U	A			
7	**P**	**L**	**E**	**A**	**S**	**E**	**X**	**S**	**E**	**N**	**D**						19	**D**	**I**	**S**	**P**	**A**	**T**	**C**	**H**	**X**	**N**	**O**	**W**			
	F	O	Q	C	N	P	O	G	V	M	E							V	W	Y	G	U	V	R	K	S	M	B	S			
8	**R**	**E**	**P**	**O**	**R**	**T**	**X**	**N**	**O**	**W**							20	**O**	**P**	**E**	**R**	**A**	**T**	**I**	**O**	**N**	**X**					
	G	K	W	X	L	V	O	J	U	H								Q	H	Q	T	U	V	Z	I	C	S					
9	**A**	**C**	**K**	**N**	**O**	**W**	**L**	**E**	**D**	**G**	**E**	**X**					21	**W**	**A**	**R**	**X**	**O**	**F**	**F**	**I**	**C**	**E**					
	S	V	C	L	C	Z	H	L	A	D	D	R						K	U	T	O	C	Q	P	O	N	F					
10	**T**	**O**	**D**	**A**	**Y**	**X**	**I**	**S**									22	**A**	**D**	**V**	**A**	**N**	**C**	**E**	**X**							
	Z	L	X	C	E	J	Z	G										S	G	J	C	S	G	V	D							
11	**F**	**R**	**O**	**M**	**X**	**A**	**D**	**M**	**I**	**R**	**A**	**L**	**T**	**Y**																	
	P	Q	Z	B	K	R	B	F	P	T	Y	Q	E	K																	
12	**F**	**R**	**O**	**M**	**X**	**W**	**A**	**R**	**X**	**O**	**F**	**F**	**I**	**C**	**E**																
	P	Q	Z	B	K	Z	K	B	S	V	J	Y	U	B	M																

In order to obtain a set of cipher messages in depth, all the clear text sequences shown in the above list were enciphered on the Railway Enigma emulation, using the same key:- Rotor order:- 3,2,1, ring settings ZZZZ, message settings:- FLCZ.

From the above tabulation a number of Enigma alphabet letter pairs were obtained, and Table I (below) gives these letter pairs all from the first six positions in the messages.
(For example at the 2nd position, AU indicates that A is enciphered as U and U is enciphered as A)
Table II shows the corresponding letter pairs at the 1st position obtained by means of the 'buttoning up' process. (Note that the first column is the same in both tables.)

1	2	3	4	5	6
A S	A U	A G	A C	A U	A R
B J	C V	C K	B M	C O	C G
C M	D G	E Q	D S	D V	D I
D V	E K	F M	E V	E Y	E P
E U	I W	J V	H K	I P	F Q
F P	L O	L N	I Q	K X	H N
G R	M J	O Z	L N	L R	J X
H L	N X	P W	O X	N S	M Y
I Y	P H	R T	P G		V T
N X	Q R	S Y	R T		W Z
O Q	X N	XD			
T Z					
W K					

Table I

1	2	3	4	5	6
A S	S I	D J	F N	G S	H O
B J	V B	B Y	L W	M F	L Y
C M	F H	G V	H G	J L	K F
D V	R P	T E	Z M	U B	I B
E U	O E	H Q	P X	D V	P Z
F P	Q A	P N	S R	C N	X E
G R	L K	W L	E Q	R I	C M
H L	M C	S I	D B	W H	R N
I Y	Y J	X R	C K		Q A
N X	W T	Z U	U I		U S
O Q		F C			
T Z					
W K					

Table II

Table II will be used extensively in the following work and it is important to understand how the entries in it were derived from those in Table I.
As an example consider the letter pair (D V) in the 5th column of Table I. By means of the diagonal sequence:- **Q W E R T Z U I O A S D F G H J K P Y X C V B N M L** letter 'D' is replaced by letter 'J' (four places forward in the sequence). Likewise letter 'V' is replaced by letter 'L' (again four places forward). Note that the resulting letter pair (J L) appears in the 5th row of table II.

By means of the information in this table, the somewhat lengthy process of constructing the 1st upright in the rod square for the right-hand rotor can begin.
Without any prior knowledge about this upright, the strategy used will be to carry out a search for a correct letter pair contained in it. The choice will be made systematically from the list of possibilities:- A/B, A/C, A/D, …..etc, so that if the hypothesis 'A/B' (i.e. A is above and adjacent to B) is found to lead to inconsistencies then a fresh start will be made using the next hypothesis 'A/C' and so on. The correct hypothesis related to letter A will be readily identified as it will be the only one not leading to any inconsistent conclusions.

From the initial hypothesis A/B and the information contained in Table II, the following conclusions can be made:-

Letter pair (AS) in the 1st column indicates that A→ S and the letter pair (VB) in the 2nd column indicates that B → V. Jointly these show that A/B → S/V.
As the letter pair (AS) occurred in the 1st column of the table, this result can be expressed more precisely as:- AB---1---SV.

Likewise in the 2nd column letter pair (QA) indicates that A→ Q and in the 3rd column letter pair (BY) indicates that B → Y. Jointly these show that A/B → Q/Y.
As the letter pair QA occurred in the 2nd column of the table this result is expressed more precisely as:- AB---2---QY.

Notes: (i) The two pairs of 'buttoned up' letters are always selected from adjacent columns in Table II. This is because the procedure, as explained earlier, is based upon the use of pairs of adjacent letters (beetles) in the messages and cribs.
(ii) As only one of the given sets of Enigma alphabets is complete, sometimes an appropriate ' buttoned up' letter pair will not be present in Table II.
In these circumstances no new conclusion can be made.

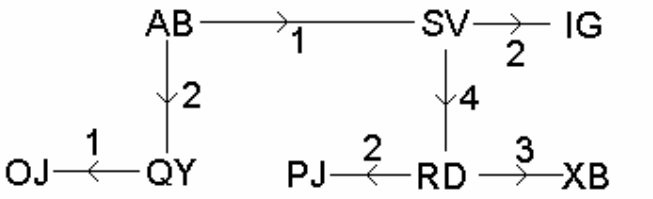
The result S/V obtained above also leads to further conclusions:-
Letter pair (SI) (2nd column) indicates that S→ I and letter pair (GV) (3rd column) indicates that V→ G. Jointly these show that S/V → I/G or SV---2---IG.
Letter pair (SR) (4th column) indicates that S → R and letter pair (DV) (5th column) indicates that V→ D. Jointly these show that S/V → R/D or SV---4--- RD.

Starting with the result Q/Y obtained above:-
Letter pair (OQ) (1st column) indicates that Q→ O, and letter pair (YJ) (2nd column) indicates that Y→ J. Jointly these show that Q/Y → O/J or QY---1---OJ

Starting with the result R/D obtained above:-
Letter pair (GR) (1st column) indicates that R→ G. However letter 'D' does not appear in the letter pairs from the 2nd column of the table and consequently no conclusion for this letter can be made, and the process cannot be completed.

However the occurrence of the letter pair (RP) (2nd column) and the letter pair (DJ) (3rd column) jointly show that R/D → P/J or RD---2---PJ.

In addition the letter pair (XR) (3rd column) and the letter pair (DB) (4th column) jointly show that R/D → X/B or RD---3 ---XB.
These results are shown in the following diagram:-

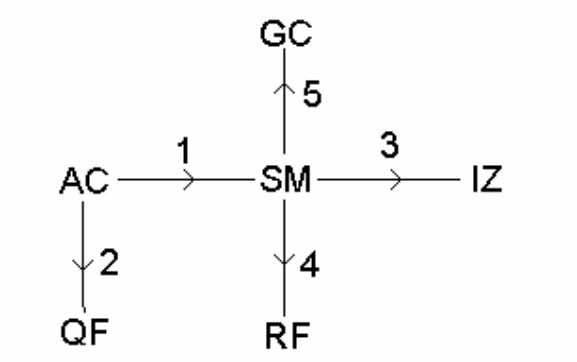


The two conclusions O/J and P/J are inconsistent and the conclusion X/B is inconsistent with the initial assumption A/B, which consequently must be false.

The procedure must now be repeated with the next initial assumption 'A/C', and the details of this are shown (in a somewhat more abbreviated form) below:-
(AS) 1st column, and (MC) 2nd column:- A/C → S/M or AC---1---SM.
(QA) 2nd column, and (FC) 3rd column:- A/C → Q/F or AC---2---QF.

Starting again with S/M:-
(SI) 3rd column, and (ZM) 4th column:- S/M → I/Z or SM---3---IZ
(SR) 4th column, and (MF) 5th column:- S/M → R/F or SM---4---RF
(GS) 5th column, and (CM) 6th column:- S/M → G/C or SM---5---GC

These results are shown in the following diagram.



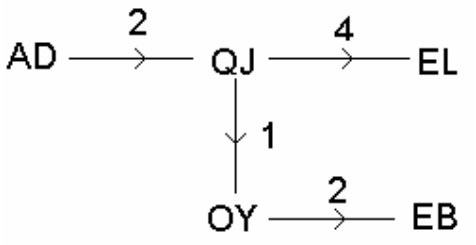
One of the conclusions reached is G/C, which conflicts with the initial assumption A/C, so that the assumption A/C is false.

Starting with the initial assumption 'A/D':-
(QA) 2nd column, (DJ) 3rd column:- A/D → Q/J or AD---2---QJ

Starting again with Q/J:-
(OQ) 1st column, and (YJ) 2nd column:- Q/J → O/Y or QJ---1---OY
(EQ) 4th column, and (JL) 5th column:- Q/J → E/L or QJ---4---EL

Starting again with O/Y:-
(OE) 2nd column, and (BY) 3rd column:- O/Y → E/B or OY---2---EB

These results are shown in the following diagram.



The conclusions E/L and E/B are clearly inconsistent and hence the assumption A/D is false.

This procedure must be repeated to systematically test in turn the initial assumptions A/E, A/F … etc.

When the assumption A/K is tested, the results are strikingly different. A large number of conclusions are obtained which do not logically conflict with one another, and some do indeed provide confirmation of others that have already been found. Some of these conclusions are shown below and are followed by a diagram showing the rather complex way in which they are related to each other. (In order to reduce as far as possible the length of the work, all of the confirmations have been omitted except for one that has been shown as an illustrative example.)

Starting with the assumption A/K:-

(AS) 1st column, and (EK) 2nd column:- A/K→ S/L or AK---1---SL

Starting with S/L:-

(SI) 2nd column, and (WL) 3rd column:- S/L → I/W or SL---2---IW

(GS) 5th column, and (LY) 6th column:- S/L→ G/Y or SL---5---GY

Starting with I/W:-

(IY) 1st column, and (WT) 2nd column:- I/W→ Y/T or IW---1---YT

(UI) 4th column, and (WH) 5th column:- I/W → U/H or IW---4---UH

Starting with Y/T:-

(YJ) 2nd column, and (TE) 3rd column:- Y/T→J/E or YT---2---JE

Starting with U/H:-

(EU) 1st column and (FH) 3rd column:- U/H→ E/F or UH---1---EF.

(ZU) 3rd column, and (HG) 4th column:- U/H→ Z/G or UH---3---ZG

Starting with J/E:-

(BJ) 1st column, and (OE) 2nd column:- J/E→ B/O or JE---1---BO

(DJ) 3rd column, and (EQ) 4th column:- J/E→ D/Q or JE---3---DQ

(JL) 5th column, and (XE) 6th column:- J/E → L/X or JE---5---LX

Starting with E/F:-

(OE) 2nd column, and (FC) 3rd column:- E/F→ O/C or EF---2---OC

(EQ) 4th column, and (MF) 5th column:- E/F → Q/M or EF---4---QM

Starting with Z/G:-

(ZM) 4th column, 4 and (GS) 5th column:- Z/G→M/S or ZG---4---MS

Starting with B/O:-

(UB) 5th column, and (HO) 6th column:- B/O→ U/H or BO---5---UH

Starting with D/Q:-

(DV) 1st column, and (QA) 2nd column:- D/Q→ V/A or DQ---1---VA

Starting with M/S:-

(CM) 1st column, and (SI) 2nd column:- M/S→ C/I or MS---1---CI

(MF) 5th column, and (US) 6th column:- M/S→ F/U or MS---5---FU

Starting with C/I:-

(FC) 3rd column, and (UI) 4th column:- C/I→F/U or CI---3---FU

(Note: this is a confirmatory conclusion.)

(CK) 4th column, and (RI) 5th column:- C/I→ K/R or CI---4---KR

(CN) 5th column, and (IB) 6th column:- C/I→ N/B or CI---5---NB

Starting with F/U:-

(FH) 2nd column, and (ZU) 3rd column:- F/U→H/Z or FU---2---HZ

Starting with H/Z:-

(WH) 5th column, and (PZ) 6th column:- H/Z→ W/P or HZ---5---WP

Starting with N/B:-

(NX) 1st column, and (VB) 2nd column:- N/B→ X/V or NB---1----XV

(PN) 3rd column, and (DB) 4th column:- N/B→ P/D or NB---3---PD

Starting with G/Y:-

(GR) 1st column, and (YJ) 2nd column:- G/Y→ R/J or GY---1---RJ

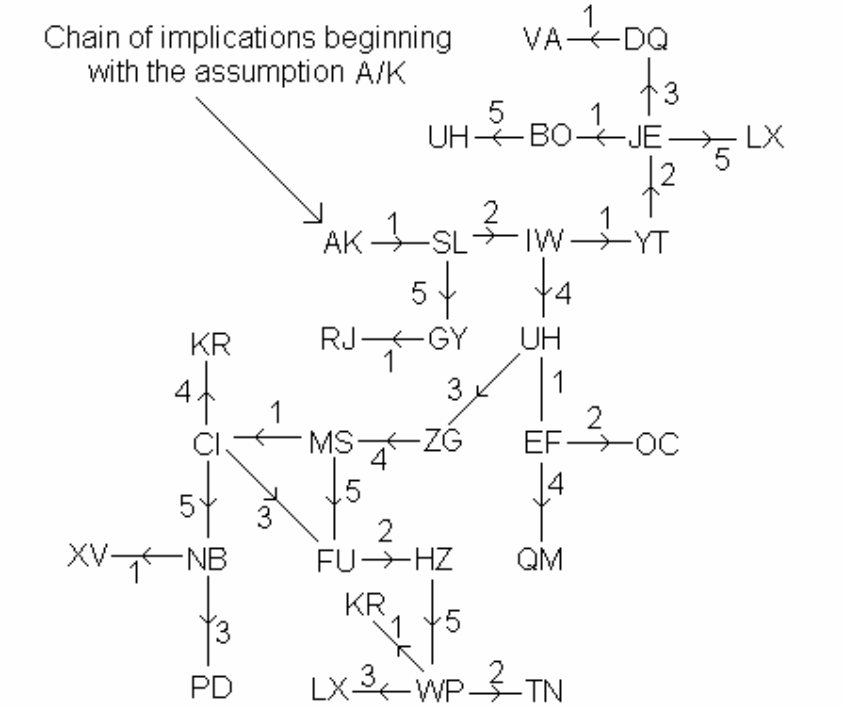
Starting with W/P:-

(WK) 1st column, and (RP) 2nd column:- W/P→K/R or WP---1---KR

(WT) 2nd column, and (PN) 3rd column:- W/P→ T/N or WP---2---TN

(WL) 3rd column, and (PX) 4th column:- W/P→L/X or WP---3---LX

This rather protracted procedure has now been carried far enough for it now to be possible to deduce the complete letter sequence in the 1st upright. The following diagram will be very helpful in this final stage of the work.



Conclusions obtained from the initial assumption 'A/K'

Combining the results:- The initial assumption that the letter pair A/K forms a fragment of the upright leads to a long chain of conclusions for other letter pairs on the upright, that is both consistent (and confirmatory) and these are shown in the final diagram below. When they are combined the result is a complete list of twenty-six ordered letters that form the required 1st upright.

Beginning with the letter pair AK, the above diagram can be used to list all the conclusions about the adjacent letter pairs existing in the 1st upright into an appropriate order:- AK, KR, RJ, JE, EF, FU, UH, HZ, ZG, GY, YT, TN, NB, BO, OC, CI, IW, WP, PD, DQ, QM, MS, SL, LX, XV, VA

Combining these then leads to the upright sequence:-

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

This is a cyclic sequence, that is closely related to the electrical connections between the contact 'pins' on the right-hand side of the rotor, and the 'plate' contacts (denoted by the sequence of letters:- q w e r t z u .. etc.) on an imaginary fixed reference disc on the left hand side of the rotor. The fact that letter 'A' appears at the beginning of the sequence is of no significance and this has only happened because the initial assumption 'A/K' was used to obtain all of the subsequent conclusions.

If it is assumed that, for the 1st position in each message, pin C on the rotor was connected to plate 'q' on the fixed reference disc (through the internal wiring of the

right-hand rotor), then the connections between these two sets of contacts will be as shown in the following table:-

q	w	e	r	t	z	u	i	o	a	s	d	f	g	h	j	k	p	y	x	c	v	b	n	m	l
C	I	W	P	D	Q	M	S	L	X	V	A	K	R	J	E	F	U	H	Z	G	Y	T	N	B	O

Reference to the rod square given earlier, confirms that this is corresponds to the 1st upright correct for Rotor 1 when set to ring setting 'Z' and rotor position 'A'.

A more practical version of this table can be constructed in the following way:-

Assign the numbers 1, 2, 3, 4, ….. 26 to the corresponding letters in the list:-
q, w, e, r, t, …….l, appearing in the 1st row and also to the corresponding capital letters in the 2nd row (e.g. both letters q and Q will be replaced by '1'; both letters w and W will be replaced by '2'). The table is will then be transformed to:-

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
21	8	2	18	12	1	25	11	26	20	22	10	17	4	16	3	13	7	15	6	14	19	5	24	23	9

This table shows the internal core wiring connections from the 26 contacts on the left hand face of the rotor to the corresponding contacts on the right-hand face.

A final version gives the same connections but now considered in the opposite direction, from the right-hand face of the rotor to the left-hand one:-

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
6	3	16	14	23	20	18	2	26	12	8	5	17	21	19	15	13	4	22	10	1	11	25	24	7	9

Concluding remarks:
It is believed that Dilly' Knox developed the technique of 'rodding' in 1936. In the following year he was first able to apply this method to 'live' messages, after he had determined the rod squares for the Enigma rotors then in use by the Italian Navy. This early work paid dividends later on, when in 1940/41 by means of 'rodding', some important Italian Naval signals yielded the intelligence that resulted in the dramatic British success at Matapan.
In 1941 Knox achieved perhaps his greatest success by breaking the 'Abwehr' Enigma, in which the 'buttoning up' procedure had again been usefully applied.

Frank Carter