

The Abwehr Enigma G312 in the BP museum A case of mistaken identity?

During the preparation of material for a forthcoming special exhibition display at Bletchley Park relating to the wartime activities of Ian Fleming, GCHQ made available the appendix from a still classified wartime report that provided details about the wiring of the rotors and reflectors of several different versions of the Enigma machine. Some of these had been used operationally by the German Intelligence Service during the war and presumably were broken by ISK (Intelligence Services Knox) at BP. One of these machines known as 'KK' had been captured in October 1942 by a group of commandos under the operational control of Fleming, and it was first thought that this was probably the machine that in later years been entrusted by CGHQ to the Bletchley Park Trust to exhibit in the museum. It was hoped that this could be proved so that a new and interesting link would have been established between Ian Fleming and the work of BP.

Alas these initial hopes were subsequently dashed after investigations had shown that the wiring of the rotors in the G312 machine in the Museum was different from those of the rotors in any of the versions of the Abwehr machines listed in the appendix. Consequently the conclusion can be made that during the war BP probably did not receive any of the messages enciphered on the G312 machine and it was not one of the variants of the Abwehr Enigma that were successfully broken at the time.

Comparing the rotors used in different machines:

The task of comparing the electrical characteristics of rotors one with another is not as straightforward as might be supposed. Even if two rotors are wired to the same basic pattern but with different orientations (i.e. the wiring in one rotor is rotated with respect to the wiring in the other) their similarity is not immediately obvious. BP devised procedures that enabled each rotor to be associated with a unique set of characteristics so that comparisons between rotors (and reflectors) could be easily made.

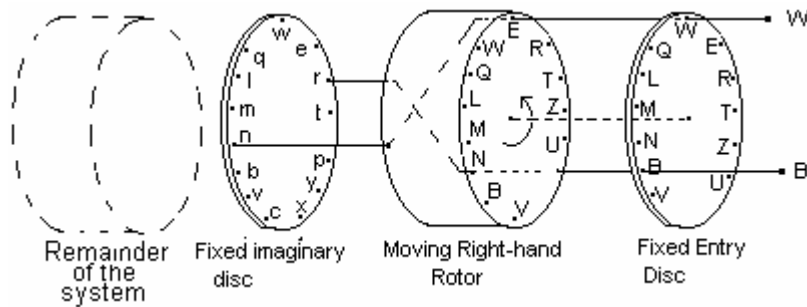
These procedures required the construction of at least a part of what was known as the '**Rod square**' for each rotor, and the following notes provide an explanation of the nature of a rod square and how it was subsequently used to provide the unique characteristics of the rotor that were required.

Constructing a rod square

A rod square is a table that provides all of the information about the electrical connections between two sets of twenty-six fixed contacts placed one on either side of a given rotor, for each of the twenty-six different rotational orientations of the rotor.

The versions of the Enigma machine that were not equipped with a plug-board had entry discs on which the terminals connected to the keys on the keyboard were ordered in the sequence:- QWERTZUIOASDFGHJKPYXCVBNML, in a clockwise sense when viewed from the right-hand side of the machine. This was in contrast to the Army and Naval Enigma machines for which the sequence was in alphabetic order (i.e. ABCD...XYZ). These notes are related to machines with 'QWERTZU' entry discs and so include all the ISK machines.

The basic idea used in the construction of a rod square is illustrated in the following diagram, in which an imaginary fixed disc with twenty-six electrical contacts is shown on the left hand side of the rotor occupying the right-hand position in the Enigma machine, with the remaining parts of the rotor/reflector system on the left of this imaginary disc.



For any given position of the right-hand rotor each of the 26 letter electrical contacts on the entry disc will be directly connected to an individual contact on the fixed imaginary disc, and if the internal wiring of the rotor is known, then these can be determined. Since the rotor can be set to twenty-six different positions, the complete set of results can be shown in the form of a 26 x 26 tabulation, forming the 'rod square' table for the rotor.

For example the above diagram shows that for a particular orientation of the rotor contact r on the imaginary disc is connected to contact B on the entry disc forming the pair (r, B) and that another such pair of contacts is (n, W). The complete rod square would contain in effect a total of 26 x 26 such pairs.

Constructing the rod square from a given tabulation of the wiring of the rotor:

As an example the wiring of 'Rotor I' used in the Enigma machine known at BP as the 'Railway Enigma' is shown in the following table (wiring from left to right) for the ring-setting 'Z', (i.e. for the rotor orientation defined by this ring-setting with the letter 'Z' on the rotor set to position Z on the Enigma machine.)

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

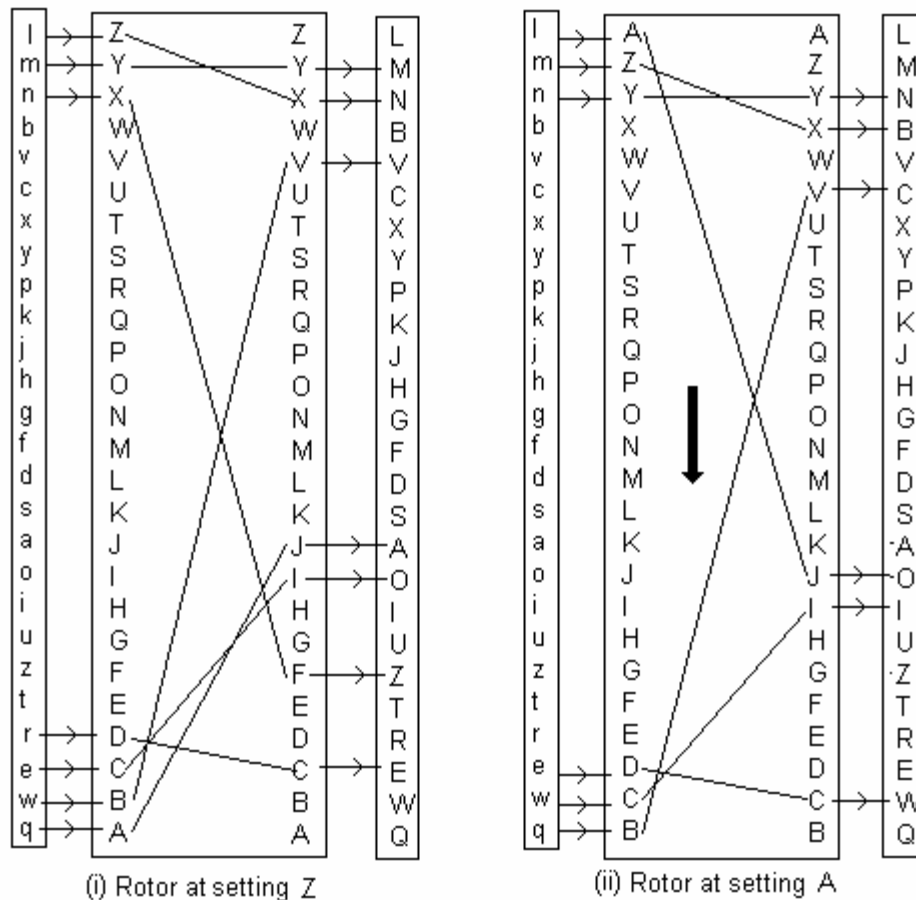
The following pair of diagrams show some of the connections between the imaginary disc on the left, through the rotor wiring to the input disc on the right, for the two rotor settings 'Z' and 'A' (with the same ring-setting 'Z').

In diagram (i) the rotor is in the initial setting 'Z' so that for example, terminal 'q' on the imaginary disc is in electrical contact with terminal 'A' on the left hand side of the rotor. The diagram shows the sequence of connections $q \rightarrow A \rightarrow J \rightarrow A$, so that contact 'q' on the imaginary disc is electrically connected to contact 'A' on the entry disc.

In diagram (ii) where the rotor shown at setting 'A', it has moved on by one position in the direction indicated by the arrow, so that the letters on the rotor are all displaced by one place from their corresponding positions in diagram (i) when the rotor was at the setting 'Z'

Contact 'q' on the imaginary disc is now in direct contact with terminal 'B' on the left hand side of the rotor. The diagram shows the sequence of connections $q \rightarrow B \rightarrow V \rightarrow C$, so that the contact 'q' on the imaginary disc is now electrically connected to contact 'C' on the entry disc.

In order to find all of the connections for each rotor position by means of the table of the rotor wiring given earlier it is necessary to take into account these displacements.



In general if the displacement is represented by the symbol T , then when the rotor is at the setting 'A', $T = "+1"$. (In fact T is the permutation in which all the letters are advanced by one position)

For this particular setting consider another example, say contact 'e' on the entry disc.

Diagram (ii) shows that contact 'e' on the imaginary disc is connected through the rotor to contact 'W' on the entry disc.

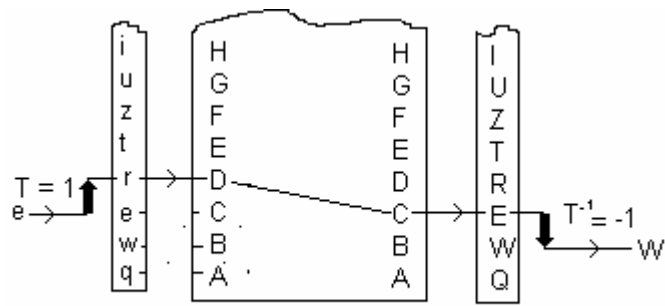
This result can also be derived from diagram (i):-

First it is necessary to carry out the transformation $T (= "+1")$, that will result in letter e being replaced by letter r (i.e by advancing one position on the 'qwertzio..' scale).

In diagram (i) letter r is adjacent to letter 'D' on the left hand side of the rotor, and the corresponding letter on the right-hand side of the rotor is seen to be 'C' which is adjacent to letter E on the entry disc

Finally the inverse transformation ($T^{-1} (= "-1")$) must be carried out so that the contact letter 'E' is changed to 'W' (i.e by moving back by one position on the right hand 'QWERTZIO..' scale).

This procedure is illustrated in the diagram below:-



(i) Rotor at position Z

This can be generalized to deal with any required displacement in the following way:-

Let α the required letter on the imaginary disc.

Let β the corresponding letter on the input disc

Let P be the permutation due to the rotor wiring.

Then (reading from right to left) the above procedure can be represented by the permutation equation :- $\beta = (T^{-1} \cdot P \cdot T) \alpha$ and so all of the entries in the 1st column (column 'A') of the rod square are given by the composite permutation:- $T^{-1} \cdot P \cdot T$

Likewise the entries in the 2nd column (column 'B') are given by the composite permutation:- $T^{-2} \cdot P \cdot T^2$

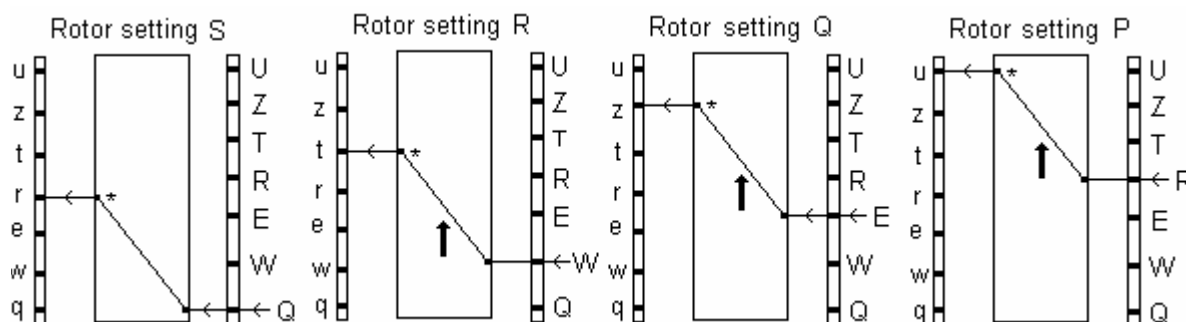
This symbolism can be extended to represent the composite permutation for any column of the rod square and this can be used as the basis for a computer program for determining the complete rod square, given a tabulation of the wiring for one particular orientation of the rotor.

The rod square for rotor 1 in the Railway Enigma

	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
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

The ‘Diagonals’ in a rod square:

The given example of a rod square shows that at the rotor setting ‘S’, contact ‘r’ on the imaginary disc is electrically connected to contact ‘Q’ on the entry disc. If the rotor then moves successively ‘backwards’ (in a clockwise direction when viewed from the right) one place at a time from setting ‘S’ to give the sequence of settings: S, R,Q, P,) while the contact on the fixed entry disc is also successively changed in a clockwise direction from ‘Q’ to give the sequence of contacts ‘Q, W, E, R T....’, then the combination of these two actions will on each occasion cause the electrical signal from the contact on the entry disc to be conveyed to the same electrical contact on the right-hand face of the rotor and consequently to the same contact on its left-hand face (marked * in the diagrams). As the rotor advances successively by one position at a time, this particular contact will move in a clockwise direction relative to the fixed contacts on the imaginary disc, giving the sequence of contacts r, t, z, u... on the disc. This process is illustrated in the following diagrams.



These explain why, beginning at the cell (r, S), the sequence of letters ‘Q W E R....’ appears in the right to left diagonal of the rod square. They also provide insight into why all of the diagonals (top right to bottom left) in the complete rod square are made up from the sequence of letters:- 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

Deriving the rotor characteristics from the rod square:

It is possible to decide whether two rotors have basically the same wiring by comparing their rod squares to see if they each contain a column with identical entries. However when the work is to be done by hand the construction of a complete rod square is a time consuming task. There is an alternative way of finding a suitable rotor characteristic that can be directly used to compare one rotor with another that only requires that a small part (just three of the columns) of each rod squares to be determined.

Consider the first three columns of the rod square shown above, where for the convenience of presentation, these are shown horizontally:-

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

Beginning with letter ‘C’ in the 1st ‘column’ the corresponding letter in the 2nd column is ‘U’; then taking letter ‘U’ in the 1st column, the corresponding letter in the 2nd column is ‘G’.

By continuing this process and recording the sequence of letters obtained the outcome will be the closed cycle of letters:- (C U G P S M A J W K E D L Y R H T B I Q N V O X)

By starting again with a letter in the 1st column not appearing in this cycle (F say) a second closed cycle (F Z) will be obtained. In this case just two closed cycles of lengths 24 and 2 are obtained. These cycles are related to the permutation that will transform the letters in the 1st column into the corresponding letters in the 2nd column.

Using the same procedure with the 2nd and 3rd columns leads to the cycles that are related to the permutation that will transform the letters in the 2nd column into the corresponding letters in the 3rd column:- (U L B C I Y X Z F K A N O H Q J W S M P E G R V) and (D T).

Although this pair of cycles contains different sequences of letters, the numbers of letters involved are the same in each pair. The same numerical results will be obtained using any pair of adjacent columns from the rod square so that in all cases the derived cycle lengths will be the same. Thus these cycle lengths are independent of the ring-settings and are a fundamental characteristic of the rotor wiring. In order to provide a theoretical justification for this consider as a particular example the first three rows of any rod square.

Let **X** represent the permutation between the 1st and 2nd columns in the rod square and let **Y** represent the permutation between the 2nd and 3rd columns of the rod square.

As shown earlier the columns of the rod square can also be represented as permutations.

Let the 1st column be represented by the permutations **Q**, so that $Q = T^{-1}.P.T$

Let the 2nd column be represented by the permutation **R**, so that $R = T^2.P.T^2$

Let the 3rd column be represented by the permutation **S**, so that $S = T^3.P.T^3$

Since **X** is the permutation that transforms the 1st column into the 2nd column, $R = X.Q$

Likewise since **Y** is the permutation transforming the 2nd column into the 3rd column, $S = Y.R$

After substituting the expressions given above for **Q**, **R** and **S**, the following pair of equations are obtained:- $T^2.P.T^2 = X.T^{-1}.P.T$ and $T^3.P.T^3 = Y.T^2.P.T^2$

Then by simplifying these equations the following two expressions for the permutations **X** and **Y** can be derived:- $X = T^{-1}.(Q.P^{-1}).T$ and $Y = T^2.(Q.P^{-1}).T^2$

If the term $Q.P^{-1}$ is replaced by the symbol **M** then $X = T^{-1}.M.T$ and $Y = T^2.M.T^2$

There is an important theorem from permutation theory (first used by Marian Rejewski in a completely different context) stating that:-

'Permutations of the form M and $U^{-1}.M.U$ will have the same cycle characteristics.'

The two expressions $T^{-1}.M.T$ and $T^2.M.T^2$ are both of the same form (If this assertion seems questionable then consider the further substitution:- $V = T^2$ which will transform $T^2.M.T^2$ to the form $V^{-1}.M.V$) Thus the permutation cycle characteristics obtained in the way described will have the same as the cycle characteristics as permutation **M** ($= Q.P^{-1}$). This is a fixed permutation for a given rotor, independent of the ring-settings, and so can be used as an invariant characteristic of the rotor wiring when comparing one rotor with another.

The lengths of these cycles (2, 24) can be used as a way of representing the characteristics of the rotor, and this particular pair of cycles is referred to as the '**Type I** characteristic of the rotor. Similarly the permutation that transforms the 1st column of letter to those in the 3rd column in the rod square can be used to derive the '**Type II** characteristic:-

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

Thus the Type II characteristic is;- 1, 2, 5, 18.

If both the Type I and Type II characteristics are listed together the result is a distinctive description of the rotor that is independent of the orientation of the wiring core.

For 'Railway Enigma 'Rotor 1' this characteristic is:- 2, 24 / 1, 2, 5, 18. and so far as is known this is unique to this particular rotor as no other rotor that were used operationally during the war had the same set of cycle characteristics.

Finding the characteristics for a reflector:

Although in the standard 3-rotor machine the reflector does not move in some other versions of the machine it can be adjusted to different positions manually or in the case of the Abwehr machine it moves automatically. It is possible to construct a theoretical rod square for any reflector, and from the columns of the square to derive the cycle characteristics for the given rotor. However the method using pairs of columns as previously described is not satisfactory. The reason for this is that the wiring of any reflector is entirely reciprocal (i.e. If A → G then G → A etc) and a consequence of this is that the cycles generated by this method always occur in pairs of equal length; consequently the characteristics obtained are not sufficiently discriminatory.

The reciprocal property of any reflector means that the cells in the rod square occur in pairs that also have the property of reciprocity so that for example if one of the cells in a particular column in the rod square say in row 's' happens to contain the letter 'G' then in the same column the cell in row 'g' will contain the letter 'S'; this twofold symmetry is the reason why the cycles occur in pairs of equal length.

The following diagram gives some of the entries in the first two columns A and B of the rod square for a particular reflector where again for convenience the columns have been printed horizontally.

	q	w	e	r	t	<i>z</i>	u	<i>l</i>	<i>o</i>	a	s	d	f	g	h	j	k	p	y	x	c	v	b	m	n	l
A						<i>O</i>			Z				<i>Y</i>				L		F							<i>K</i>
B						<i>K</i>			F				<i>O</i>				Z		L							<i>Y</i>

These entries in the 'columns' in the rod square are reciprocal, so that for example column 'A' row 'o' contains the entry 'Z' and row 'z' contains the entry 'O'

The six entries in the two adjacent columns (shown in heavy type) imply the existence of the following closed cycle:-

$$Z \rightarrow F (F) \rightarrow L \rightarrow (Z) , \text{ i.e. the cycle } (Z F L) \text{ of length } 3$$

As a consequence of the reciprocal nature of the table these six entries imply the presence of another six entries (shown in italic type), and these form the basis for another corresponding cycle :- *O* → *K* (*K*) → *Y* → *O* i.e. the cycle (*O K Y*) also of length 3

Hence the occurrence of this pair of cycles both of length 3 is a consequence of the existence of six pairs of cells in columns 'A' and 'B' of the rod square with reciprocal entries.

Since all of the entries in the cells in each column of the rod square of a reflector will occur in reciprocal pairs then it follows that all the cycles generated will occur in pairs of equal length.

In order to overcome this technical difficulty another procedure was devised to generate cycles that would not invariably occur in pairs of equal length but were still independent of the orientation of the reflector, so that the cycles generated were the same for all columns of the rod square.

This new procedure requires only any one column from the rod square together with the initial 'qwertyu...' reference column.

An example is shown below in which again for sake of convenience the two columns 'A' and 'B' are printed horizontally. Consider first 'column A'; the letter 'w' in the first row has the substitution letter 'S' in the second row and so the first letter in one cycle is taken to be the letter 'S'.

The letter in the first row that is one position to the left of letter 's' is letter 'a' and this letter has the substitution letter 'G', and this is taken as the second letter in the cycle.

The letter in the first row that is one position to the left of letter 'g' is letter 'f' which has the substitution letter 'Y', and this is taken as the third letter in the cycle, and so on..

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

Working systematically in this way the following 10 letter pairs are obtained:-

(w,S), (a, G), (f, Y), (p, U), (z, O), (i, N), (b, C), (x, Q), (l, K), (j, E)

leading to the cycle:- (S G Y U O N C Q K E) of length 10.

It is necessary to demonstrate that the same cycle characteristic can be derived from another column of the rod square and for this purpose ten corresponding letters in column 'B' of the rod square are also shown in heavy type. Then as a consequence of the reciprocal properties of the reflector, these entries in the cells of column 'B' from the rod square imply the additional ten entries:- (h, W), (q, A), (o, F), (d, P), (k, Z), (t, I), (u, B), (v, X), (y, L), (m, J).

These particular 10 letter pairs are identical to those that will be obtained by directly applying the process previously described to the given entries in 'column B'.

These lead to the cycle:- (W A F P Z I B X L J) of length 10 which matches with the corresponding cycle of this length that has been derived from 'column A'.

Thus the two columns 'A' and 'B' from the rod square will lead to matching pairs of cycles of the same length, by extension implying that the same cycle characteristics will be generated from the entries in any column of the rod square.

Returning to the other entries in 'column A', the process described will lead to the second cycle:- (X F R J V B H A Z M I P L T D W) of length 16. Any column of the rod square will provide a corresponding cycle of this length.

A very similar process was also used that involved the displacement of the letters by 'two positions to the left' to derive a class II characteristic for reflectors. A similar analysis to the one given will show that the class II characteristics so obtained were also the same of all the columns of the rod square.

The procedures described above were used to find the characteristics of the rotor/reflector wiring for the five different types of machines described in the recently released appendix referred to at the beginning of these notes. These were known by the following names:- "Group II", "South American", "South American II", "K.K." and "S.D. Commercial"

In addition another machine known in certain U.S. documents as an "Argentinean Abwehr machine G260" has also been included. Originally this work would have been done by hand but with the number of rotor and reflectors involved the task was not an inviting one, and short computer programs were written that enabled the results to be obtained more readily.

The characteristics for the G312 machine currently in the museum were derived from the details of the wiring published in the journal *'Cryptologia'* (January 2000) in an article by David Hamer, an internationally recognised authority on Enigma machines. The following table gives the 'Class I' and 'Class II' characteristics of the wheels and reflectors:-

Machine Type	Rotor 1 (Red)	Rotor 2 (Blue)	Rotor 3 (Green)	Reflector
"G 312"	3, 23 / 4, 22	6, 20 / 2, 24	2, 24 / 2, 2, 6, 16	10,16 / 1, 5, 20
"K.K"	2, 24 / 2, 2, 9, 13	2, 3, 7, 14 / 10,16	2, 2, 4, 5, 6, 7 / 8,18	1,3,5,17 / 1, 2, 3, 4,16
"South American"	10, 16 / 7, 19	4, 22 / 2, 24	8,18 / 3, 3, 6, 14	10,16 / 1, 5, 20
"South American (II)"	9, 17 / 2, 24	2,6,7,11 / 2, 5,6,13	2,6,7,11 / 4,22	1, 1, 2, 22 / 1, 6, 19
"G260"	9,17 / 2, 24	2,6,7,11 / 2,5,6,13	2,6,7,11 / 4,22	1, 2, 2, 22 / 1, 6, 19
"SD commercial"	8, 18 / 2, 24	7,19 / 6,20	1,4,9,12 / 2,3,5,16	1, 1, 2, 22 / 1, 6, 19
"Group II"	2, 24 / 11, 15	2,2,3,19 / 4,5,8,9	8,18 / 1,2,8,15	1,5, 5,15 / 1,1,2, 6,16

(The computer program confirmed the characteristics of the wheels and the reflector of the G312 machine at BP given in David Hamer's published paper.)

Observations:

- (i) From the table it is apparent that "South American II" and G260 are two descriptions of the same machine.
- (ii) This machine used the same reflector as the "SD commercial" variant.
- (iii) The G 312 machine at BP has the same reflector as the "South American" machine.

Final Comments:

It had originally been hoped that the G312 Abwehr machine at currently at BP was in fact the "K. K" machine captured in Algeria in 1942. However the evidence provided by comparing the rotor/reflector systems shows this not to be so.

The discovery of different machines with common reflectors is of great interest and confirms new evidence obtained by Frode Weierud (Geneva) that a large number of Abwehr type machines were manufactured in 1940 with serial numbers G304 - 403 but that these were not wired until they were required for operational use.

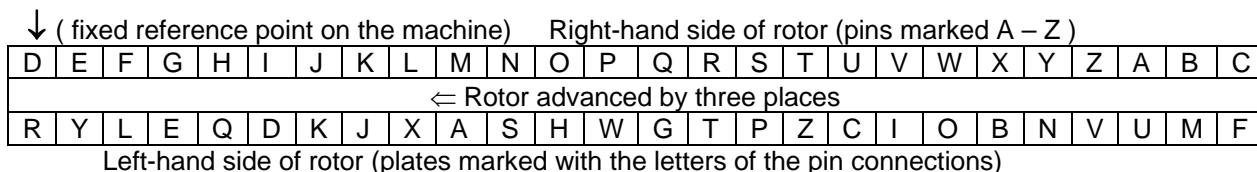
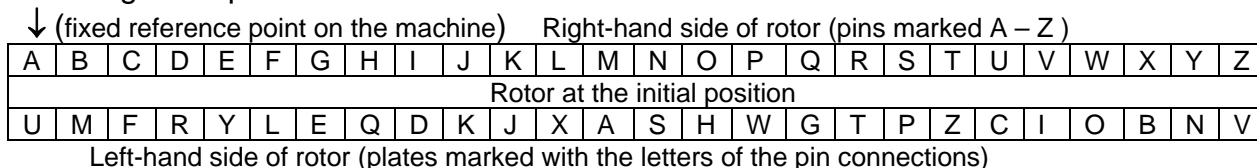
Thus it seems very probable there were a number of mechanically identical machines being used but with different electrical wiring. Currently the role of G312 during the war is unknown, but it has been established that it was not the "KK" machine that was used for a brief period by the German Armistice commission in North Africa as had originally been thought possible.

A postscript

This additional note describes a simpler method for classifying rotors suggested by Keith Batey, a mathematician who during the war worked in Hut 6 and later with 'ISK', His method has the considerable advantage of being much simpler and easier to use.

Consider the following pair of diagrams showing the electrical connections between the 'pins' on the right-hand side of a particular rotor and the 'plates' on the left -hand side. The pins are

marked with the letters A - Z in alphabetic order while each plate is marked with the letter of the pin to which it is electrically connected. The rotor is shown in two different positions the second being three places in advance of the first:-



From the first diagram a table containing a sequence of twenty six numbers can be derived representing the ‘*alphabetic separation*’ of each pair of letters representing the plates. These values can be derived from the following table in which the numbers in the upper row are the alphabetic positions of the letters representing the plates on the left-hand side of the rotor:-

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

The ‘*alphabetic separation*’ between each pair of letters is derived in the following way:- Subtract the alphabetic position of the 1st letter from that of the 2nd letter; if the result is negative then add 26 to it.

So for example the ‘*alphabetic separation*’ between ‘U’ and ‘M’ = (13 – 21) + 26 = 18

Likewise the ‘*separation*’ between ‘M’ and ‘F’ = (6 – 13) + 26 = 19, and the separation between

‘F’ and ‘R’ = (18 – 6) = 12

In this way the following sequence of numbers are derived:-

18, 19, 12, 7, 13, 19, 12, 13, 7, 25, 14, 3, 18, 15, 15, 10, 13, 22, 10, 3, 6, 6, 13, 12, 8, 25

(Note: the last value in the sequence is the separation between the letters ‘V’ and ‘U’ :- (21 – 22) + 26 = 25)

If the same procedure were to be carried out on the plate letters in the second diagram it should be evident that although starting at a different position the same sequence would be obtained since all the plate numbers are the same and appear in the same cyclic order as in the first diagram.

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

Indeed for **any** position of the rotor the sequence of plate numbers will be the same, although each will begin at a different place. Hence the cyclic number sequence derived above is independent of the wiring orientation and so can be used to uniquely identify the wiring.

Bearing in mind that that the aim is to check whether a given wiring is the same as one on a given list of known wirings (which in practice will number rather less than 200) it will suffice to use four consecutive numbers from the sequence as a label to identify the wiring.

One way of deriving such a label is to use the smallest number in the sequence together with the three following numbers. If by chance the smallest number is not unique, then choose that which is followed by the smaller number, for example in the above sequence the resulting label is:- 3,6,6,13

For the purpose of listing the labels it is convenient to replace the numbers by the equivalent alphabetic letters, so that this label becomes:- C F F M

A matter that now has to be resolved is to estimate how likely it is that two different wirings will by chance have the same label. Each label consists of four positive whole numbers with values between 1 and 25 subject to the following condition:- The three numbers following the first one must each be greater than or equal to the first number. It can be shown that the total number of possible random labels = 105,625

Suppose that 200 essentially different known rotor wirings are to be compared with a random one, then the total number positions at which the label of the random rotor can be compared with the number sequences obtained from the 200 different rotors = 26 x 200.
Hence the probability of a label match occurring = $(26 \times 200)/105,625 = 0.05$

Another considerable advantage of this method is that it can be used to find the labels for reflectors as well as for rotors.

F.L.C

Frank Carter August 2008