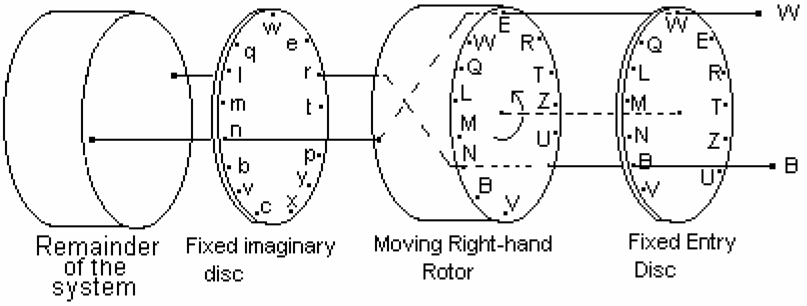
‘RODDING’

This technique (invented by ‘Dilly’ Knox in 1937) was used to break messages that had been enciphered on Enigma machines that did not have a plug board. The first commercial version of Enigma was of this type and a few countries adopted it for use by their armed services, after equipping it with different sets of rotors. The Italian Navy used the machine during the Spanish Civil War, and continued to do so in a limited way after their entry into the Second World War in June 1940. In March 1941 ‘rodding’ was used to break some important Italian messages, which lead to the dramatic and successful action in the Mediterranean, known as the Battle of Matapan. A new exhibition at Bletchley Park gives an account of these events and includes some detailed information showing how the first success was achieved. The following notes explain the basic principles of the technique by means of an illustrative example.

Like most of the methods used at BP, ‘rodding’ required a crib with which to begin, however this technique did not provide a complete sequence of characters from the plain text, but to only a very fragmented one, and considerable linguistic skill was required to fill in the gaps, not unlike that required for solving crossword puzzles. Every correct inference made about the content of a message obtained in this way could then be used as an extension of the crib, and this would enable the process to be continued.

The versions of the Enigma machine without a plug-board, had entry discs on which the letter terminals followed the sequence:- QWERTZUIOASDFGHJKPYXCVBNML in a clockwise sense when viewed from the right-hand side, in contrast to the standard service Enigma machines for which the sequence was:- ABCD…XYZ.

The basic idea used in ‘rodding’ can be explained by means of a diagram, in which an imaginary fixed disc with twenty-six electrical contacts is shown between the right-hand rotor of the Enigma machine and the remaining components of the rotor/reflector system on the left.



Consider the contacts on the input disc, and suppose that the effect of the RH rotor is to connect contact ‘W’ to the contact ‘n’ on the imaginary disc. Likewise suppose that the effect of the RH rotor is to connect contact ‘B’ to the contact ‘r’ on the imaginary disc. If the letter W happens to be enciphered as B on the Enigma, then the pair of contacts ‘n’ and ‘r’ on the imaginary disc must be electrically connected through the remaining part of the Enigma system. For each position of the RH rotor there will be 13 of these pairs of contacts on the imaginary disc, all of them being ‘mutually disjoint’, i.e. no two pairs have a common contact.
For any given position of the R.H. rotor, the 26 letters on the entry disc will be directly connected to an individual contact on the fixed imaginary disc, and if the internal wiring of the R.H. rotor is known, then these can be determined. Since the rotor can be set to 26 different positions, the complete set of results can be presented in the form of a 26x 26 tabulation, known as the ‘rod square’ table for the rotor.

The rod square table for ‘Rotor I’ used with the 3-rotor, ‘QWERTZU’ version of the machine (without a plug board), known as the ‘Railway’ Enigma, is shown below. The lower case letters in the column at the left represent the contacts on the imaginary disc, and the numbers in the top row represent the twenty-six possible positions of the rotor. The table gives the connections between the imaginary disc contacts and the entry disc contacts for all positions of the rotor. (For this table the rotor ring-setting used was 'Z '. Then the 1st column in the table corresponds to the rotor position 'A', the 2nd to position 'B' etc.) For example the table shows that contact 't' on the imaginary disc is connected to contact 'C' on the entry disc when the rotor is at its 10th position.

Rotor positions

Contacts on the Imaginary disc

	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

It will be observed that the letters in all the diagonals running from top right to bottom left in the table, follow the order of the cyclic sequence of the letters on the entry disc: i.e. QWERTZU…….BNML . This phenomena can be explained by considering a particular case:-
The table shows that at the 15th position of the rotor, contact Z on the entry disc is directly connected to the contact 'v' on the imaginary disc. Suppose that the RH rotor rotates forwards (i.e. anti-clockwise when viewed from the right-hand side) by one position at a time to give the sequence of positions 15, 16, 17, 18, 19, 20, 21, ….etc., while the contact selected on the fixed entry disc is changed "backwards" (i.e. also anti-clockwise) by one position at a time giving the corresponding sequence of contacts:- Z, T, R, E, W, Q, L, M, N…..

The combination of these two actions will, on each occasion, cause the electrical signal to be conveyed to the same contact on the right-hand face of the RH rotor, and hence to a particular contact on its left-hand face.

As this rotor is advancing by one position each time, this particular left-hand contact will move backwards (anti-clockwise) relative to the fixed contact points on the imaginary disc, giving the sequence of contact points v, c, x, y, p, k, j ... on it.

This behaviour is illustrated in the following diagram, and confirms that the patterns in the diagonals in the rod square table consist of letter sequences running top right to bottom left, in the same order as those for the contacts on RH side of the entry disc, i.e. QWERTZU……… .

Rotor positions

Contact points on the Imaginary disc

	15	16	17	18	19	20	21
j							**L**
k						**Q**	
p					**W**		
y				**E**			
x			**R**				
c		**T**					
v	**Z**						

The Rods:- A set of twenty-six rods is made up from the individual rows of a rod-square table. Originally three sets would have been needed, one for each of the three rotors used in the machine. These sets were colour coded to avoid confusion.

Two examples are shown with a pair of rods (for 'rotor I') aligned side by side:-

	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
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

The 1st rod shows that for the succession of R.H. rotor positions:- 1, 2, 3, 4, 5, 6,…..26, the corresponding sequence of contacts on the entry disc:- C, U, L, H, I, V, Y, R , …M, A are all connected to contact "q" on the imaginary disc. Likewise the 2nd rod shows that for the same succession of rotor positions the corresponding sequence of contacts on the entry disc:- M, A, N, K, P, T, S, B, …G, W are all connected to contact 'u'.

Suppose that the letter 'V' from a cipher message is known to represent the plain-text letter 'T', and that this occurs when the R.H. rotor is at its 6th position. Then it follows as a consequence of the reciprocal relationship between the two letters 'V' and 'T', (each being the encipherment of the other), that the two terminals 'q' and 'u' on the imaginary disc must be electrically connected together through the remaining components of the Enigma machine. The letters 'q' and 'u' are known as the 'rod coupling' letters, and the diagram shows the pair of rods 'q' and 'u' coupled together side by side with the pair of letters (V T) at position 6.
Now suppose that the third letter of the cipher message happens to be 'B' (appearing at the 8th position on the second rod), then as a result of the same rod coupling it should be evident that the corresponding plain-text letter must be 'R'.
Thus by means of the rods one known letter of the plain text crib has enabled an additional letter to be deduced. The validity of this deduction is however dependent on two conditions:-

1. That the pair of rods is taken from the correct set for the R.H. rotor originally used.
2. That a middle rotor 'turn-over' (T.O.) has not occurred between the 6th and 8th positions in the cipher.

The application of this useful property of the rods can be extended. A general description of the procedure is hard to formulate, but an understanding can be obtained by means of an illustrative practical example:- A message was enciphered on the 'Railway' Enigma machine (which has an adjustable reflector) configured in the following way:- rotor order 3, 2, 1: ring settings 'ZZZZ': reflector setting 'F': rotor settings 'LCZ'. The cipher message obtained was as follows:-

MLXVK SCLDU HOHSV FKXKU SDVRP NGCYA T (31 characters)

A description follows showing how the process of 'rodding' can be used to recover the plain-text, given the accurate starting crib:- 'CODEX' (X was commonly used as a 'space' mark).

The procedure would originally have begun with the lengthy task of trying in turn each of the three possible rotors that might have occupied the R.H. location in the machine together with its possible initial position (there are up to 3 × 26 = 78 possible configurations to try.) Each could be tested by finding the corresponding set of pairs of rod couplings and checking them for inconsistencies (i.e. no two to contain a common letter). If, for a particular combination of rotor and initial position, no inconsistencies occurred in the set of rod couplings derived from the crib, then there was a good chance that it was the correct combination. (***Much time and effort would have been required to find the correct combination by this process of elimination.***)

In the demonstration example this protracted task (and another described later on), have been avoided (*dishonestly*!) by the prior knowledge of the Enigma configuration used. (In reality 'rodding' must have been an extremely tedious process, requiring great patience as well as skill.) The crib and cipher provide the following pairs of reciprocal characters (bigrams):-

(M C), (L O), (X D), (V E) and (K X)

The five corresponding pairs of rod couplings (shown at the top of page 5) for Rotor "I", starting its 1st position are:-

(u q), (t s), (o y), (r k), and (b x), and there are no inconsistencies between them.

A counter example:- It can be shown that the sequence of corresponding rod couplings for Rotor II starting at its 1st position begins: - (j x), (p c), (c q), (f n) and (j w) it is clear that this combination cannot be correct, as the rod couplings (p c) and (c q) demonstrate an inconsistency, (no single letter on the imaginary disc can be coupled to two different letters via the remaining part of the Enigma system).The couplings (j x) and (j w) are also inconsistent.

Supplementary note:

In an alternative approach, if the rods are used for a wrong combination of rotor and starting position, inconsistencies with the crib usually appear which will make this evident.
For example if Rotor I at starting position 2 is tried (i.e. with the 2nd letter on each rod aligned against the 1st letter of the cipher), the rod square table gives the rod couplings (i a) for the first bigram (M C), which gives no inconsistencies. For the second bigram (L O), the corresponding rod couplings are:- (q z) and these two rods are shown at the 2nd position in relation to the cipher message in the following diagram:-

		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	27	28	29	30
		M	L	X	V	K	S	C	L	D	U	H	O	H	S	V	F	K	X	K	U	S	D	V	R	P	N	G	C	Y	A
		C	O	D	E	X																									
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					
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	F	X					

An inconsistency is now apparent at the 5th place in the message. The rods indicate that the decipherment of letter 'K' is 'V' and not 'X' as given by the crib. Hence either the rotor/starting position combination is wrong or a T.O. has taken place before the 5th place in the message. Here, for the sake of brevity, it will be assumed that a T.O. has not occurred, when the correct combination would produce no inconsistencies.

Using the rods for Rotor I starting at its 1st position, the five pairs of coupled rods arising from the crib are shown. These rod pairs contain the bigrams obtained from the crib and cipher characters, but in addition, outside the range of the crib, there are some places where a letter on one of the rods matches a letter in the cipher, and at these places the letter on the other rod provides an additional character of the plain-text (assuming that no prior middle rotor T.O. has taken place) These pairs of letters are shown in the diagrams in bold type:-

			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	27	28	29	30	31
			M	**L**	**X**	**V**	**K**	**S**	**C**	**L**	**D**	**U**	**H**	**O**	**H**	**S**	**V**	**F**	**K**	**X**	**K**	**U**	**S**	**D**	**V**	**R**	**P**	**N**	**G**	**C**	**Y**	**A**	**T**
			C	**O**	**D**	**E**	**X**																										
		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					
		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					
		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					
		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					
		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					
		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					
		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					
		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					
		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					
		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	**O**	**D**	**E**	**X**			**E**			**I**		**G**	**X**				**B**				**C**		**Z**	**A**						

The eight-letter word ‘? ? E ? ? I ? G’ in the partially recovered plain-text between the two ‘space’ characters (X), very probably ends with ‘ING’, and taking into account the crib ‘CODE’, it is realistic to assume that this word is probably ‘BREAKING’. (This is an example of the type of linguistic assumption that had to be made.)

The probable extension of the plain-text arising from this assumption, leads to the following new bigrams and rod couplings shown below:-
At the 6th place (S B) gives rod couplings (a n), providing the bigram (A V) at the 15th place.
At the 7th place (C R) gives rod couplings (l z), confirming the bigram (U K) at the 10th place.
At the 9th place (D A) gives rod couplings (w v), providing the bigram (K X) at the 17th place.
At the 12th place (O N) gives rod couplings (m h), which provides no useful results.
The new pairs of rods giving additional information are shown below:-

	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	27	28	29	30	31
	M	**L**	**X**	**V**	**K**	**S**	**C**	**L**	**D**	**U**	**H**	**O**	**H**	**S**	**V**	**F**	**K**	**X**	**K**	**U**	**S**	**D**	**V**	**R**	**P**	**N**	**G**	**C**	**Y**	**A**	**T**
	C	**O**	**D**	**E**	**X**	**B**	**R**	**E**	**A**	**K**	**I**	**N**	**G**	**X**				**B**				**C**		**Z**	**A**						
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					
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					
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					
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	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					
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					
	C	**O**	**D**	**E**	**X**	**B**	**R**	**E**	**A**	**K**	**I**	**N**	**G**	**X**	**A**		**X**	**B**				**C**		**Z**	**A**						
	C	**O**	**D**	**E**	**X**	**B**	**R**	**E**	**A**	**K**	**I**	**N**	**G**	**X**	**A**		**X**	**B**				**C**		**Z**	**A**						

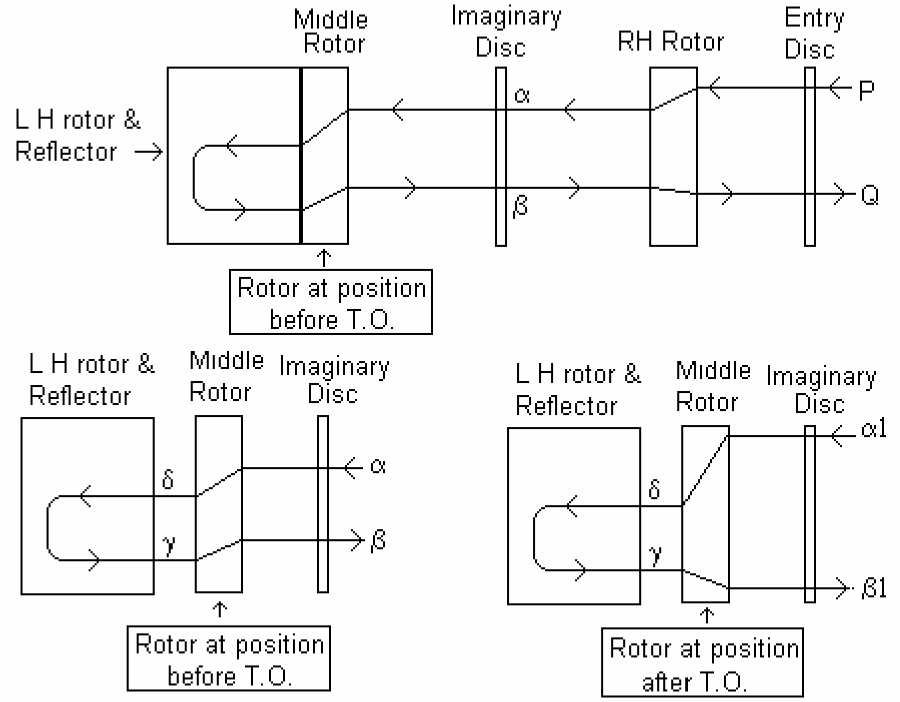
The message has now become: C O D E X B R E A K I N G X A – X B – – – C – Z A

The conjecture:- C O D E X B R E A K I N G X A T X B L E T C H L E Y might seem to be a possibility but there is a clash at the 24th and 25th places in the cipher with the pair of letters 'Z' and 'A' given earlier by the rods. However their advanced locations in the cipher, make it probable that a T.O. of the right hand rotor will have occurred before the 24th place, and that consequently these letters are incorrect. Taking into account that the letter 'C' at the 22nd place appears to be correct, it seems likely that a middle rotor T.O. has occurred either between the 22nd and 23rd or between the 23rd and 24th places in the cipher.
Assuming the conjecture: 'ATXBLETCHLEY' to be correct then up to the 23rd place in the cipher the following new bigrams appear:- (F T), (K L), (U E), (S T), and (V H). However only (K L) at the 19th position, with the rod coupling (i d), gives a useful result by providing the valuable confirmation of the letter pair (V H) at the 23rd position, thus indicating that the T.O. almost certainly must occur between the 23rd and 24th positions. This rod coupling is shown below:-

	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	27	28	29	30	31
	M	**L**	**X**	**V**	**K**	**S**	**C**	**L**	**D**	**U**	**H**	**O**	**H**	**S**	**V**	**F**	**K**	**X**	**K**	**U**	**S**	**D**	**V**	**R**	**P**	**N**	**G**	**C**	**Y**	**A**	**T**
	C	**O**	**D**	**E**	**X**																										
	C	**O**	**D**	**E**	**X**	**B**	**R**	**E**	**A**	**K**	**I**	**N**	**G**	**X**	**A**		**X**	**B**				**C**		**Z**	**A**						
	C	**O**	**D**	**E**	**X**	**B**	**R**	**E**	**A**	**K**	**I**	**N**	**G**	**X**	**A**	T	**X**	**B**	L	E	T	**C**	H	L	E	Y					
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					
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					
	C	**O**	**D**	**E**	**X**	**B**	**R**	**E**	**A**	**K**	**I**	**N**	**G**	**X**	**A**	**T**	**X**	**B**	**L**	**E**	**T**	**C**	**H**	**L**	**E**	**Y**					

The message now appears to be:- 'CODEXBREAKINGXATXBLETCHLEY ? ? ? ? ?'
(With a middle rotor T.O. taking place between the letters 'H'and 'L'.)

Dealing with a turn-over of the middle rotor:
The next stage of the work requires an understanding of the effect of a middle rotor T.O., which will change the rod coupling letter pairs, in the way shown in the following diagrams:-



The first diagram shows the pair of contacts (α and β) on the imaginary disc connected to the pair of contacts P and Q on the Entry disc through the R.H. rotor, before the middle rotor T.O. has taken place. The second diagram shows how two contacts (δ and γ) on the L.H. rotor are connected to the pair of contacts (α β) on the imaginary disc through the middle rotor, before the T.O. The third diagram shows how the same two contacts (δ and γ) are connected to the pair of contacts ($\alpha1$ $\beta1$) on the imaginary disc through the middle rotor after the T.O.

The diagrams show that both of the pairs of contacts (α β) and ($\alpha1$ $\beta1$) on the imaginary disc are connected to the contacts (δ γ) through the middle rotor, in just the same way as the contacts (P and Q) on the Entry Disc are connected to the contacts (α β) through the R.H. rotor.
This means that the correct relationships between the contacts (α β), ($\alpha1$ $\beta1$), and (δ γ) will appear in the rod square table for the middle rotor, as shown in the following diagram:-

(pre T.O.) ↓ ↓ (post T.O.)

	1	2	3		s1	s2			
q									
w									
δ					α	$\alpha1$			
γ					β	$\beta1$			

Part of the rod square for the middle rotor

It follows that the correct rod square table for the middle rotor will contain a pair of adjacent columns (i.e. those corresponding to the 'pre' and 'post' middle rotor T.O. positions), that will satisfy the following conditions:-
(i) One pair of corresponding cells in these two columns will contain the two elements α and $\alpha1$
(ii) A second pair of corresponding positions in the same columns will contain the two elements $\beta1$ and $\beta2$
(iii) The positions of these two adjacent columns in the table will give the 'pre' and 'post' T.O. positions of the middle rotor.
(As the uppercase letters in the rod square tables are now being used to represent contacts on the imaginary disc, these entries in the table must be changed (mentally) to their lower case forms.)

The diagram shows that once the rod square has been correctly identified, and its original setting (s1) has been found, then any rod coupling (α β) found before the T.O. can be used to find the corresponding rod couplings ($\alpha1$ $\beta1$) after the T.O. and vice-versa.

A procedure for identifying the middle rotor (from the two remaining ones), together with its position before the T.O. is as follows:-
First consider the following bigrams that must occur after the T.O. :-
At the 24th position bigram (R L) gives the rod coupling (o w)
At the 25th position bigram (P E) gives the rod coupling (k i)
At the 26th position bigram (N Y) gives the rod coupling (l t)
(None of these couplings happen to provide any additional letters of the plain text.)

An important point is that these couplings must correspond to others that were valid before the T.O. had occurred, and which could be found from the appropriate column of the rod square table for the correct middle rotor, provided that the T.O. position of this rotor were known.

If assumptions are made for both the identity of the middle rotor and its starting position, then the appropriate two columns of the rod square table for this rotor can be used to find a set of corresponding ‘pre T.O’ rod couplings from the known ‘post T.O.’ couplings given above. If however either of these assumptions are wrong, then it is very likely that logical inconsistencies will occur between these and the original ‘pre T.O.’ couplings previously found, and when this happens two or more of the couplings will have a letter in common. Otherwise the couplings need to be checked to see if they give ‘promising’ letters of plain-text when set up against the cipher. Originally a tedious process of elimination (involving up to 2 × 26 = 52 trials) would have been necessary to find the correct combination of assumptions.
To see how this works in practice remember that the pre-T.O. rod couplings enumerated earlier were:- (u q), (t s), (o y),(r k), (b x), (a n), (l z), (w v), (m h) and (i d).

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

Rod square Rotor II

If the middle rotor is assumed to be rotor II, initially set to its 1st position, then from the 1st and 2nd columns of this rod square, the three post T.O. rod couplings (o w), (k i) and (l t) are found to have the corresponding pre T.O. couplings (j u), (w k), and (r p). Comparing these with the list of couplings given above, it can be seen that all three are inconsistent, (for example the couplings (u q) and (j u) are contradictory), this implies that at least one of the initial assumptions must be wrong.

If the setting of the assumed middle rotor (still rotor II) is changed to position 3, then the 3rd and 4th columns of the rod square table give the corresponding pre T.O. couplings:- (r k), (b x) and

(t s). As each of these appears on the original list of couplings, there are no inconsistencies, and consequently the two assumptions (i.e. that the middle rotor is rotor II and that it was set to the 3rd position) are probably correct. The rod pairs for these couplings also confirm some of the bigrams found previously, thus providing further evidence that these assumptions are the correct ones.
By using the 3rd and 4th columns in the rod square in the reverse order, the remaining original rod couplings can be used to find their corresponding 'post' T.O couplings, and two of them providing additional information are:- (u q) → (b v) and (l z) → (h g).

The new rod coupling (b v) gives at the 31st place the bigram (K T), and the new coupling (h g) gives at the 30th place the bigram (R A).

Note: These pairs of rods are shown above set to the 27th position of the R.H. rotor. If the rods are tried when set to the 1st position of the R.H. rotor that was used in all the previous diagrams, then they do not provide any useful results at the 24th, 25th and 26th places in the cipher, which would be the only three 'post' T.O. places currently within their span.

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	27	28	29	30	31	
M	**L**	**X**	**V**	**K**	**S**	**C**	**L**	**D**	**U**	**H**	**O**	**H**	**S**	**V**	**F**	**K**	**X**	**K**	**U**	**S**	**D**	**V**	**R**	**P**	**N**	**G**	**C**	**Y**	**A**	**T**	
C	**O**	**D**	**E**	**X**																											
C	**O**	**D**	**E**	**X**	**B**	**R**	**E**	**A**	**K**	**I**	**N**	**G**	**X**	**A**		**X**	**B**				**C**		**Z**	**A**							
C	**O**	**D**	**E**	**X**	**B**	**R**	**E**	**A**	**K**	**I**	**N**	**G**	**X**	**A**	T	**X**	**B**	L	E	T	**C**	H	L	E	Y						
																									b	T	B	C	Z	***K***	E
																									v	Y	R	V	X	***T***	J
																									h	J	W	S	***R***	S	Q
																									g	R	H	Q	***A***	E	A
C	**O**	**D**	**E**	**X**	**B**	**R**	**E**	**A**	**K**	**I**	**N**	**G**	**X**	**A**	**T**	**X**	**B**	**L**	**E**	**T**	**C**	**H**	**L**	**E**	**Y**				**R**	**K**	
C	**O**	**D**	**E**	**X**	**B**	**R**	**E**	**A**	**K**	**I**	**N**	**G**	**X**	**A**	**T**	**X**	**B**	**L**	**E**	**T**	**C**	**H**	**L**	**E**	**Y**	**X**	**P**	**A**	**R**	**K**	

The two additional bigrams give the plaintext letters R and K, so that the plain-text becomes:-
C O D E X B R E A K I N G X A T X B L E T C H L E Y – – – R K
Credibly leading to the message:-
C O D E X B R E A K I N G X A T X B L E T C H L E Y X P A R K

Concluding remarks:

In addition to the meticulous care that would have been necessary during the elimination procedures described above, the wartime successes required considerable linguistic ability and creative imagination. It was often necessary to make correct inferences about the context of messages expressed in German or Italian, based only on the fragmentary evidence of some of the letters contained in them.

If the reader does not consider the deductions made in this example to be plausible, it is suggested that a visit to the Exhibition at BP might be of interest, as some of the deductions actually made during the breaking of a genuine cipher message on display are quite surprising and show that much higher levels of skill and imagination were required for success than are suggested by the somewhat contrived example given above.

A brief historical post-script:
The following short summary on how the first break was made in 1940, may give the reader some insight into the difficulties encountered at the time:- When the Italians entered the War in June 1940, it was thought likely that their Navy might still be operating the same type of Enigma machine as they had used at the time of the Spanish Civil War, and the attempts to break their ciphers were based on this assumption. For the technique of 'rodding' to succeed it was essential to have accurate cribs, and initially a serious difficulty was the lack of knowledge about the stereotyped forms of text that were likely to occur in the Italian messages.

In the absence of anything more specific, Dilly Knox instructed his assistants (a group of young women known as 'Dilly's girls') to use 'PERX' as a crib for the first four characters of each intercepted signal (= 'FOR' followed by a 'space'), and for those cases when this did not lead to any inconsistencies between the crib and the first four letters of a cipher message, to record any other letters that could be found by the rods in the hope that these might provide some clues about the plain text.

These assistants worked continuously for three months at this task without having any success until September 1940, when one of them, Mavis Lever, a nineteen-year-old student whose University course had been interrupted by the war, achieved a remarkable break.
With the message on which she was then working, for a particular starting position for the 'green' rotor (i.e. rotor I), the rods had given the letter 'S' in the 4th place, which clashed with the letter 'X' in the crib (i.e. resulting in the letter sequence 'PERS' instead of 'PERX' as was anticipated).

If Miss Lever had obeyed her instructions, she would have rejected this rotor starting position, and gone on to try the next one. However in a moment of inspiration she decided to assume that the crib 'PERX' was in fact wrong and guessed that it was 'PERSONALE'. After making this assumption and continuing with the 'rodding' process, she was gratified to find that the additional letters of plain-text then given by the rods made good sense, so that the first part of the message turned out to be:- PERSONALEXPERXSIGNORX…. (X= "space").
(More information on how this was done is to be found in the Exhibition.)

This was a most remarkable and valuable achievement, as it proved, (after three months effort!) that the Italians were indeed still using the same early version of the Enigma machine. From this message and others, which were subsequently broken, a vocabulary of useful cribs was built up which greatly increased the effectiveness (and speed) of the "rodding" technique.

Frank Carter