The Abwehr Enigma Machine

The objective of this article is to offer a brief account of how the major features of the Abwehr machine were discovered by the distinguished cryptographer "Dilly" Knox. In particular it offers a more detailed explanation of the terms "crab" and "lobster" than it would be possible to display (or for the visitor to read), within a museum environment.

It is important to remember that in August 1941, when Dilly Knox was first given the task of breaking the Abwehr traffic, nothing was known about the machine itself, and the only information about the traffic was that an eight-letter indicator was included in each cipher message.

It was already known that the early commercial-type Enigma used three rotors together with a reflector that could be rotated by hand, but which did not move during the operation of the machine, and that consequently four letters had been required to specify a message setting. It was also well known that one standard German procedure previously encountered had been to encipher each message setting twice. Consequently, as a working hypothesis, it was assumed that for this new traffic a similar type of machine was being used and that the message settings were enciphered twice to give the eight letter indicators.

In order to be able to break the messages it was first necessary to recover the wiring of the three rotors and the reflector. As no cribs were available, Dilly Knox realised that his best hope was to recover the message settings from the indicators intercepted each day (i.e. to decipher the indicators), in order to provide a number of letter pairs for the eight successive machine positions. From these it would then be possible to deduce the wiring of the rotor used in the right–hand position in the machine on any given day, and so over a period of time, to deduce the wiring of all of them. The wiring of the reflector could then be recovered.

In the course of his early investigations, Dilly Knox had an analysis made of certain sequences of letters that could be derived from each day's indicators. He referred to the process of finding these sequences as "boxing", and they lead to a crucial discovery being made that requires some "spade work" to explain.

Suppose that the (unknown) letters of a particular message setting are denoted by the symbols Z U I O and that this message setting, after being enciphered twice, gives the indicator:- S G H R A X T Q. The effect of the Enigma enciphering process (sometimes called a permutation) at the 1^{st} position can be expressed as:- (Z $\rightarrow$ S), and likewise the process at the 5^{th} position can be expressed as:- (Z $\rightarrow$A). As a consequence of the reciprocal nature of all Enigma enciphering processes, another permutation at the 1^{st} position is:- (S $\rightarrow$ Z), and the combined effect of this permutation at the 1^{st} position followed by that at the 5^{th} position, can be expressed as:- (S $\rightarrow$ Z) followed by (Z $\rightarrow$A) , which is equivalent to (S $\rightarrow$A). After omitting the arrow this can be represented by the ordered letter pair (S A). A complete description of the combined effect of these two processes is made up of twenty-six ordered letter pairs. These letter pairs can be linked together to form the closed letter chains or "boxes" for the positions 1 and 5 in the indicators This procedure can also be applied at the other pairs of positions in the indicators to obtain for example the letter boxes for the positions 2 and 6 in the indicators.

The letter "boxes" can be readily derived from the indicators intercepted on a given day, provided that there were enough of them. For example:-

A TABLE OF TWENTY-SIX INDICATORS.																		
1	2	3	4		5	6	7	8			1	2	3	4		5	6	7	8
A	O	Q	S		T	R	T	N			D	Z	Y	P		G	B	I	R
T	R	X	N		Q	L	D	S			X	Q	O	W		Z	H	U	M
P	V	E	Q		A	W	Q	T			N	D	L	F		D	P	F	B
H	J	P	T		K	U	G	Q			M	C	K	O		X	G	O	H
R	S	C	Y		F	F	E	V			W	N	S	D		J	Y	H	X
U	U	I	V		N	C	L	Y			Q	X	A	A		C	M	R	I
O	I	N	G		W	Q	S	J			J	A	H	C		O	V	N	K
Y	E	B	J		S	D	Y	G			B	W	R	B		E	E	V	Z
C	M	V	R		L	K	C	F			K	H	G	X		I	I	J	D
F	T	W	U		Y	N	W	L			L	K	T	E		P	O	X	F
I	P	J	Z		V	A	M	S			S	F	F	M		B	Z	P	W
G	B	Z	H		U	S	Z	O			V	G	M	I		H	J	B	A
E	L	D	L		R	X	A	U			Z	Y	U	K		M	T	K	C

Two of the sets of boxes that can be constructed from these indicators are:-
The 1 –5 letter "boxes":-
A T Q C L P (A) , B E R F Y S (B) , D G U N (D) , H K I V (H) J O W (J) , M X Z (M)

The 2 – 6 letter "boxes":-
O R L X M K (O), V W E D P A (V), S F Z B (S), G J U C (G), H I Q (H), N Y T (N)

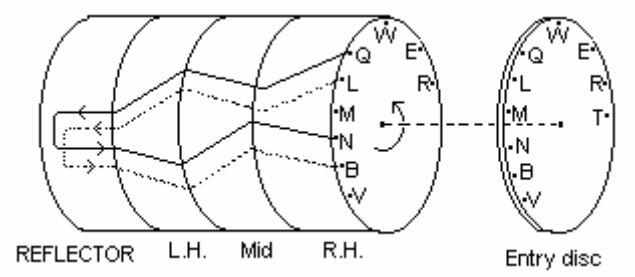
Note that the bracketed letters are strictly redundant, they are included here to emphasise the closed nature of the boxes, which as can be seen, always occur in pairs of equal length. The bracketed letters will subsequently be omitted.

Consider the first box from each of the above sets: i.e. A T Q C L P and O R L X M K. A comparison of these, with the circular "qwertzu" sequence of terminal letters on the Enigma entry disc (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) will confirm the truth of the following statement:-
If each letter in the second box is located in the "qwertzu" sequence, and is then replaced in the box by the following letter in this sequence, then the new box so formed is identical to the first box. (Making a sequence of replacements like those described here, became known as **"buttoning up"**.)
So that in this particular case the "buttoning up" replacements are:-
O $\rightarrow$ A, R $\rightarrow$ T, L $\rightarrow$ Q, X $\rightarrow$ C, M $\rightarrow$ L, and K $\rightarrow$ P, thus obtaining all the letters in the first box:- A T Q C L P. This remarkable relationship also exists between the other corresponding pairs of boxes from the two sets.

This was the unexpected discovery mentioned earlier. It should be emphasised that this special relationship between the pairs of boxes only occurs for some message settings. Dilly Knox called the occurrence of this relationship a **"crab"**, and he had the insight to understand the reason why it happened, which subsequently lead him to make a number of useful deductions about the (as yet unknown) design of the Abwehr machine.
It must be pointed out that usually the limited number of indicators intercepted on a particular day, would be very unlikely to provide all the information needed to complete the boxes. It was however possible to carry out the buttoning up process far enough, using

the incomplete boxes, to determine whether or not the relationship described above was true for the indicators obtained that day.

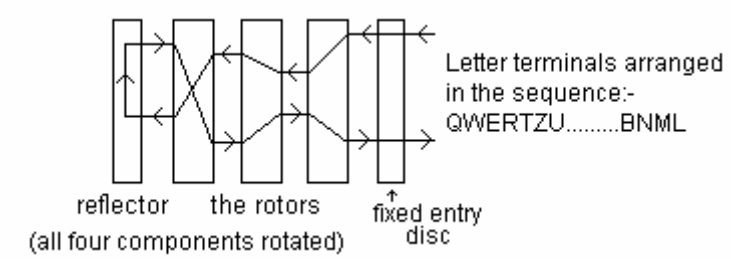
An explanation of a crab:-
Suppose that a key on the machine, say "Q", is pressed so that an electric current passes from terminal Q on the entry disc, through the rotors and reflector, back through the rotors to another terminal on the entry disc (say N), so that the machine has enciphered Q as N (and clearly N as Q, if key N had been pressed instead). This means that there is a continuous circuit loop through the rotors and reflector, joining the corresponding terminals Q and N on the entry disc.
If, during the process of enciphering a second letter, the three rotors and the reflector **all happen to turn by one position**, as indicated by the arrow, this circuit loop will move to the position shown by the dotted line and will then connect together the two terminals L and B on the entry disc.



The complete sequence of letter terminals around the entry disc is:-
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 (as read clockwise from the right-hand side, in the opposite direction to the rotor movement), and it will be observed that the two letters L and B are respectively one position behind Q and N in the entry disc sequence. (i.e. Q $\rightarrow$ L and N $\rightarrow$ B).
The diagram helps to explain the unexpected relationship between the pairs of boxes described earlier, if it is assumed that during the repeated encipherment of each message setting, a simultaneous turn-over of all three rotors and the reflector occurs between the 1st and 2nd positions and again between the 5th and 6th positions. These will result in the orientation of the rotors and reflector at the positions 2 and 6, being exactly one step in advance of their corresponding orientations at the positions 1 and 5. This in turn implies that both the 1 - 5 and 2 –6 letter boxes are derived from the same set of Enigma circuit loops, but for the 2 –6 boxes, the loops are always one position "behind" those for the 1 - 5 boxes. Hence the letters of the 2 - 6 boxes are also all one behind the corresponding letters in the 1 – 5 boxes, as detected on the QWERTZU…. sequence of terminals of the entry disc.
The deductions made by Dilly Knox following the discovery of the existence of "crabs" were:-
(i) The machine had a reflector which could be turned by hand like the commercial machine but which also moved during operation. (In contrast to the standard service Enigma for which there was a fixed reflector.)

(ii) The machine had an entry disc on which the letter terminals were arranged in a circular pattern in the order QWERTZU…….BNML (clockwise when viewed from the right-hand side).

(iii) The rotors had a large number of turn-over positions, as otherwise "crabs" would be very rare. This was a feature not previously encountered (the standard service rotors had only one or two turn-over positions).



(iv) That there would be other positions at which all the rotors and the reflector turned over simultaneously, but without it happening again four positions later, as it did for a "crab"; Dilly Knox called this a "**lobster**", claiming that it was half a "crab".
A lobster could be of assistance in the decipherment of the indicators, as will be shown later, and Knox immediately organised a "lobster hunt".

The procedure used by the Abwehr operators was basically the same as that used before the war for the standard service version of the Enigma. The operator first adjusted all the ring settings and then set up the machine, locating the three rotors in a particular order. Both of these operations were carried out according to the instructions he had been given for the day. Then the reflector and three rotors were turned to the positions prescribed for the base setting (Grundstellung) for that day, so that the designated letter on each ring appeared in the corresponding window on the machine.
The operator then decided on the starting positions for the reflector and rotors that he intended to use (i.e. the **message setting)**, and enciphered this four-letter sequence twice in succession on the machine, to produce the eight letters that made up the **indicator**. He then turned the reflector and rotors to the positions of his chosen message setting and proceeded to encipher the message.
For example:- cipher position: 1 2 3 4 5 6 7 8 (relative to the Grundstellung)
message setting: G E S A G E S A
indicator: S Y A T V Q Y G

The process of deciphering the indicators involved an examination of the daily sets of intercepted indicators known as the "**keyblocks**".

If a sufficiently large keyblock was available then the complete boxes could be found, making the problem of deciphering the key block a relatively easy one.
In practice this seldom if ever occurred and only incomplete boxes would be obtained so that an alternative strategy had to be adopted.
This was to begin by making assumptions for the message settings of one or two chosen indicators, and to determine the logical implications these had for other indicators, bearing in mind the following facts:-
(i) Every indicator was composed of its twice-enciphered message setting.
(ii) That at any position in one of the indicators if "A" was enciphered as "B" then, at the same position , "B" would be enciphered as "A".
If it was also assumed that a lobster occurred between positions 1 and 2, then other implications could be made (as shown in the later example).
If as a consequence of all the implications arising it was found that a logical inconsistency occurred, then one or more of the initial assumptions was wrong, and a fresh start had to be made.

In the absence of any prior knowledge, one random guess for a message setting seems as as good as any other, but in this situation it was possible to take other factors into account, so that associated letter groups like "QWER" or "KARL" were considered to be more likely guesses than random sequences such as "XHLQ". It should be remembered that it

was known at the time that many of the Enigma operators in the German Armed Services were often using message indicators and settings based upon first names, etc. and so it was realistic to assume that the Abwehr operators might have adopted similar practices. A first impression of this strategy, which involved a considerable element of "trial and error", is probably not an appealing one, but to paraphrase a remark expressed by a member of the original BP group who used it "*Codebreaking in practice involves a great deal of trial and error, an inconvenient fact but one that is true in real life.*"
The assumption about the undisciplined behaviour of the German operators turned out to be true, but the preliminary work that had to be done to establish it, must have required patience and determination (a slice of good fortune would also have been helpful).

The frequent use of stereotyped message settings by the Abwehr operators made the task of deciphering the keyblocks rather more straightforward. The settings that they used included first names, obvious sequences of keyboard letters (e.g. QWER) and a variety of obscene German words, and the knowledge of these transformed the task of deciphering the indicators into a linguistic puzzle, which has been described, by one who should know, as "*setting guessing*"! The very simple example given below should not mislead the reader into the belief that this was easy. A set of logically consistent outcomes would not usually have been reached as readily as the example might suggest.

The eight indicators shown in the following keyblock, were selected from a much larger number to enable a simple demonstration of this approach to be given. The indicators were all derived from four letter German first names (mostly female), and they have been placed in a convenient order to facilitate the decipherment of the first seven of them (the last one is left as an exercise for the reader).

	1	2	3	4		5	6	7	8
(a)	S	Y	A	Y		V	Q	Y	G
(b)	T	Z	A	Y		S	K	Y	G
(c)	U	Y	T	Y		W	Q	F	G
(d)	L	Z	E	Y		Q	K	M	G
(e)	Y	Z	G	Y		A	K	O	G
(f)	Y	J	A	Y		A	G	Y	G
(g)	K	Q	E	Y		R	T	M	G
(h)	U	B	G	D		W	N	O	V

An examination of the indicators (a) (b) and (f) shows that the 3rd and 4th letters in all three of the corresponding message settings must be the same (it is also evident that the last letter is the same in seven of the message settings).

A consideration of some possible German first names might suggest that the letters "S" and "A" are promising candidates for the 3rd & 4th positions (and the 7th & 8th positions), and it is realistic to make a guess that the message settings for the indicators (a) and (b) might be "ELSA" and "LISA".

A number of logical deductions can now be made and are shown in the following table. The indicators and the two guessed message settings are given in upper case type, and all the consequent logical deductions made from them are shown in lower case.

From the two guesses, additional plain text letters can now be found for the positions designated by the following ordered number pairs representing respectively the rows and columns in the table:-

Letter "L" in (3, 2) and in (3, 6), "S" in (6, 3), and in (6, 7).

Letter "A" in (3, 4), (3, 8), (4, 4), (4, 8), (5, 4), (5, 8), (6, 4), (6, 8), (7, 4) and (7, 8).

Then as a consequence of the reciprocal properties of any Enigma encipherment, the letter pair (T L) in the 1st column implies the letter "T" in (4, 1), and also in (4, 5).
The letter pair (Z I) in the 2nd column implies the letter " I " in (4, 2), (4, 6), (5, 2), and (5, 6).

	1	2	3	4		5	6	7	8
	S	**Y**	**A**	**Y**		**V**	**Q**	**Y**	**G**
1.	E	L	S	A		E	L	S	A
	T	**Z**	**A**	**Y**		**S**	**K**	**Y**	**G**
2.	L	I	S	A		L	I	S	A
	U	**Y**	**T**	**Y**		**W**	**Q**	**F**	**G**
3.	o	l	g	a		o	l	g	a
	L	**Z**	**E**	**Y**		**Q**	**K**	**M**	**G**
4.	t	i	n	a		t	i	n	a
	Y	**Z**	**G**	**Y**		**A**	**K**	**O**	**G**
5.	r	i	t	a		r	i	t	a
	Y	**J**	**A**	**Y**		**A**	**G**	**Y**	**G**
6.	r	o	s	a		r	o	s	a
	K	**Q**	**E**	**Y**		**R**	**T**	**M**	**G**
7.	a	n	n	a		a	n	n	a
	U	**B**	**G**	**D**		**W**	**N**	**O**	**V**
8									

<u>If the assumption is made that there is a lobster between positions 1 and 2, then other letter pairs can be deduced:-</u> Using the "buttoning up" procedure described earlier, but in the reverse direction from the 2nd position to the 1st, the letter pair (Z I) in the 2nd column provides the corresponding letter pair (U O) in the 1st column, so that the letter "O" can be placed in (3, 1), and (3, 5). The (German) name in the 3rd row can now credibly be inferred to be "OLGA", and hence the letter "G" is placed in (3, 3) and (3, 7).

The letter pair (T G) in the 3rd column, then gives the letter "T" in (5, 3) and (5, 7).
A plausible assumption can now be made that the name in the 5th row is "RITA", so letter "R" is placed in (5, 1) and (5, 5). These imply letter "R" in (6, 1) and (6, 5), strongly suggesting the name "ROSA" in row 6, so that letter "O" can be placed in (6, 2) and (6, 6).

The letter pair (A R) in the 5th column implies the letter "A" in (7,5) and hence also in (7,1). If the name in the 7th row is assumed to be "ANNA", then the implied letter pair (E N) in the 3rd column gives the name "TINA" in the 4th row, which is feasible.

The fact that all of the names deduced seem plausible would appear to justify all the assumptions made. A verification of the lobster between the 1st and 2nd columns can in general be made by applying the "buttoning up" procedure to all the letter pairs in the 1st column, to derive the corresponding letter pairs in the 2nd column, and then looking for any inconsistencies between the resulting sequence of implications for the letter pairs in the 2nd and 6th columns. However this procedure can only be applied to a larger set of indicators than the one given here.

In this example the presence of a lobster has materially assisted in the decipherment process by enabling a letter pair at the 1st position to be deduced from a letter pair at the 2nd position. A lobster can also be used to provide letter pairs at the 2nd position from given ones at the 1st position. It should however be noted that the presence of a lobster is not necessary for the successful decipherment of a key block, as it is known that it was sometimes achieved without one.

The decipherment of the indicators in a given key block provided a number of letter pairings at each of the eight consecutive positions of the machine. These enabled the wiring of the right-hand rotor used for their encipherment to be determined.

This could be done by using the sets of letter pairings to deduce the structure of what were known as the “rods” for the rotors. An explanation of the nature and significance of the “rods” would require the introduction of substantially more material, and consequently this aspect of the work will not be addressed here. Sufficient to say that a technique known as “rodding”, had been invented by Dilly Knox before the war, and it was used to decipher messages made on versions of the Enigma machines not fitted with a plug-board.

After the decipherment of several keyblocks, the short sequences of turn-overs obtained for each rotor could be “fitted” together to construct the complete sequences, which was known as the rotor “wheel tracks”. The three rotors were designated by colours to distinguish them, and it was ultimately found that the “green” rotor had 11 turn-over positions, the “blue” rotor 15 positions and the “red” rotor 17 positions.

An additional problem was to find how these turn-over positions were related to the letters on the rings attached to each rotor, and this could not be solved until a message had been broken, the task being first accomplished by Dilly Knox.

These notes do not attempt to address the techniques used for the routine breaking of the Abwehr signals after the structure of the machine had been completely recovered. It is known that different methods were used over time to meet changing circumstances.

One point of great importance to remember is that it was not possible to make use of long message cribs, containing say a dozen or more letters, in the way that was done for the traffic of the German Armed Services. The Abwehr signals could not be broken by this method because of the very frequent occurrence of the rotor turn-overs.

Frank Carter