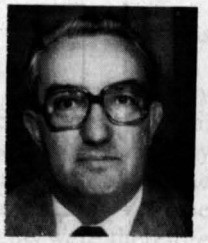
A Classical Cipher Machine: The ENIGMA—Some Aspects of its History and Solution



R. F. CHURCHHOUSE, CBE, FIMA
Department of Computing Mathematics, University of Wales College of Cardiff

1. Encipherment: historical background

ENCIPHERMENT as a means of protecting the security of military, diplomatic or even commercial or personal communications has been used for thousands of years. Until the end of the 1914–18 War encipherment was generally by means of codes and ciphers, the messages frequently being carried by hand, a very slow means of communication, or by telephone or telegraph lines. Interception by an enemy of one's messages under such circumstances is not easy and may be impossible; but a serious disadvantage is that communication with one's own ships and submarines is difficult.

Communication by radio changed all that. Messages could now be sent to any station, on land or sea, and delivery was essentially instantaneous. On the other hand interception of the messages by enemies or competitors was made much easier.

Experience on both sides in 1914/18 had shown that the code and cipher systems then in use were not very secure and it was realised that if messages were to be transmitted by radio, and so regularly intercepted, they must be enciphered by more secure systems than hitherto. The only totally secure system is the use of "one-time pad," which is unbreakable when used properly, but this involves the production and distribution of pages of (genuinely) random numbers, each page being used only once and although this is possible on a moderate scale, e.g., for use on diplomatic traffic to and from embassies, it is out of the question for large scale use between military units in a major war.

The use of codes and ciphers up to 1918 had been largely a manual operation and the more complex the encipherment process the longer it took to encipher/decipher and the more likely that errors would be made. Cryptographers therefore concluded that some form of enciphering machine which could be produced in large numbers was essential and immediately after 1918 a number of individuals put forward proposals for such devices. The idea of an enciphering machine was not new, simple devices had been produced at least as early as the 15th century, but the early 1920s saw proposals for machines that offered far greater security than anything previously, and the one from that era that has become most famous is the ENIGMA.

In this article a brief account is given of the history of the ENIGMA and the mathematical analysis that led to the decryption of over a million messages before 1945. For anyone interested in the part played by ULTRA (intelligence obtained from ENIGMA decrypts) in the War I would recommend the first four volumes of the Official History of British Intelligence.[1–4]

2. History of the ENIGMA

Arthur Scherbius, a German engineer working in Berlin in 1919, was interested in cryptology and other topics and among his inventions were several cipher machines. These were partly mechanical, partly electrical, and involved the use of four rotors, three of which moved on a common shaft whilst the fourth was fixed. In 1923 he co-founded a company to produce these machines and presented them at the Congress of the International Postal Union, where they attracted much favourable comment. His company advertised the machines widely, hoping for orders from large firms, but the response was poor.

In 1926, in great secrecy, the German Navy—which was severely limited in size by the Versailles Treaty—bought one of the machines and analysed it. They were sufficiently impressed that they offered to buy a large number, provided that certain modifications were made.

The machine, in its original form, continued to be offered for sale until 1933 to anyone who cared to buy it but, although some firms and representatives of countries other than Germany bought it, on the whole the commercial sales drive was not a great success.

The machine, known as the ENIGMA, was not patented until 1928, by which time Scherbius was dead. Ironically in 1929 the sales drive was successful in that not only did the German Army decide to order the machine, in secret, but also William Friedman of the US, the greatest cryptanalyst in the world who was to break the Japanese Purple machine some 10 years later, put in an order—a sure sign that he thought it worth detailed examination. The number of orders from the German Navy and Army was potentially large so the success of the machine, from a financial point of view was assured. By the end of the 1939/1945 War something like 30 000 ENIGMAS had been produced. (There was no official German Air Force in 1929, but they were eventually the biggest user and ordered 20 000, out of the over-all total of 30 000, before 1945.)

3. Description of the ENIGMA machine

The original, and simplest, form of the ENIGMA is illustrated in Fig. 1. Significant modifications were introduced later but in this article we shall be mainly concerned with this form.

$R1$, $R2$ and $R3$ are rotors which rotate on a common shaft; U is a fixed reflector (*Umkehrwalze**, in German). Each rotor has 26 contacts on its left side and 26 contacts on its right side. Inside each rotor are 26 wires which connect the contacts on one side to the contacts on the other side. The internal wirings of the rotors were designed so that the output contacts were randomly related to the input contacts to which they were connected; for example in one of the rotors in the

* Referred to at Bletchley as "the Uncle Walter."

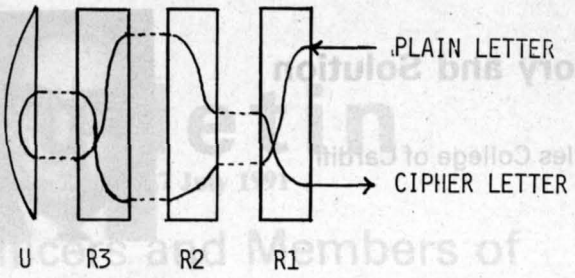


Fig. 1. The ENIGMA machine

original machine:

input contact: *A B C D E F G.....*
was connected to output contact: *B X M J C S G.....*

To encipher a letter, say *C*, the *C* key was pressed on the keyboard. This caused a current, from a battery, to flow through rotor 1, then through rotors 2 and 3, after which the current was turned back by the reflector (*U*) and passed through rotors 3, 2 and 1 in that order before causing a bulb to light up under the appropriate cipher letter, which was then written down, since the ENIGMA had no printer attached.

When the plain-text letter key was pressed the rightmost rotor (*R*1) moved on one position, so after 26 letters had been enciphered *R*1 was back in its original position.

Attached to *R*1 was a metal ring with a single notch cut into it. Once in each complete revolution of *R*1 this notch reached a position opposite a lever and when this happened the rotor to the left of *R*1, that is *R*2, was moved on one position.

Similarly there was a metal ring attached to *R*2; it also had a single notch cut into it and when this notch reached the position opposite another lever the leftmost rotor *R*3 was moved on one position and *R*2 also moved on one position (otherwise *R*3 would have kept on moving until *R*2 moved off its notch position).

After $26 \times 25 \times 26$ letters had been enciphered, but not before, all three rotors would normally have returned to their original positions (certain positions cannot reoccur but can be used as *starting* positions).

The reflector, *U*, did not move at all; its function was to provide a connection between pairs of output contacts from *R*3 in order to send the current back through the three rotors in the reverse direction.

Two consequences of the use of the reflector can easily be seen:

(*i*) if letter *C*, say, enciphers to *X* then at the same position letter *X* enciphers to *C*—for the current simply flows in the reverse direction along the same path;

(*ii*) no letter can ever encipher to itself—for the reflector connects *pairs* of contacts so the current in the second half of the encipherment must follow a different path from that in the first half of the encipherment.

These are cryptographic weaknesses of the machine; the first in particular was exploited by the Poles in their solution of the pre-War ENIGMA.

An advantage of having a reflector is that, as is evident from (*i*), there is no need to distinguish between encipherment and decipherment; typing in the cipher text produces the original plain text provided only that

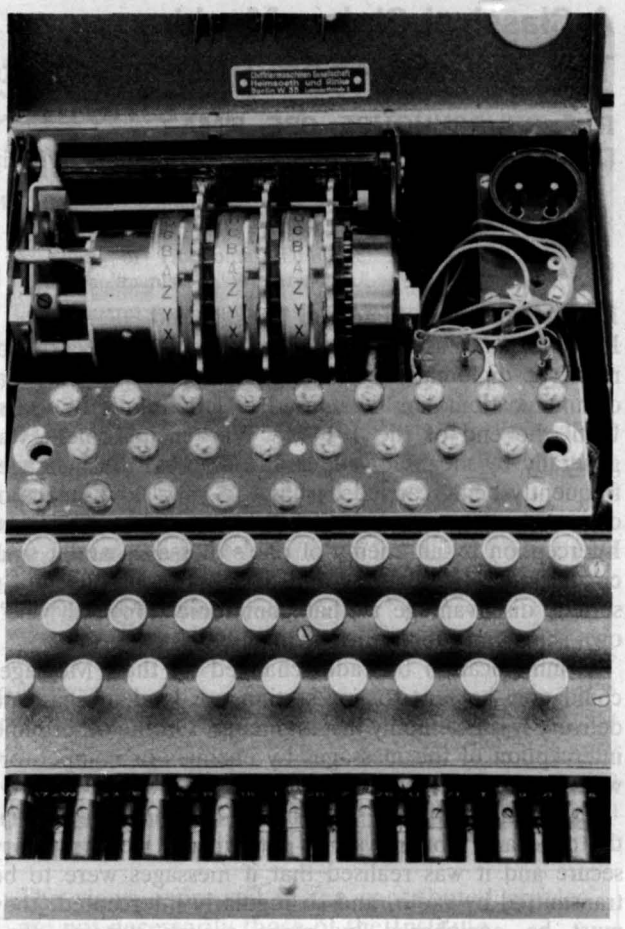


Fig. 2. The ENIGMA with the cover raised. Note the three rotors and the relector (version B), the bulbs which indicate the cipher letters and the plugboard (at the front)

the three rotors are started at the same positions as they were when the message was enciphered. (See Figs. 2–4.)

4. Increasing the security of the basic ENIGMA

In all versions of the ENIGMA the order of the 3 rotors could be changed by means of a lever which made it possible to take them off the drive shaft and put them back in a different order. There were therefore initially 6 possible wheel orderings.

If a cryptanalyst knew everything about the machine, including the internal wirings of the three rotors, or if he had an identical machine available how much work would he have to do to decipher an intercepted message when he did not know the order of the three wheels or their settings at the start of the message?

Since there are 6 possible wheel orderings and each wheel can be set in any one of 26 positions a "brute force" attack would involve making

$$6 \times (26)^3 = 105\,456$$

trial decipherments to see which one produced intelligible text.

If the cryptanalyst did not have the machine and did not know the internal wirings of the rotors the number of trial decipherments using brute force would be increased by a factor of

$$(26!)^3 = 10^{80}$$

giving a total "work factor" of about 10^{85}, a number which is so enormous that we can safely say that brute

Fig. 3. The ENIGMA ready for use. The rotors are set at *AAB*, the letter *C* has just been enciphered and the cipher letter *J* has lit up

force attack on an unknown ENIGMA is impossible. If he did not know the wiring of the reflector the situation would be even worse: that is, an over-all work factor of more than 10^{100}.

Good cryptographers, however, assume that their opponents have acquired a copy of the machine and so only need to find the wheel orders and initial settings in order to decipher the messages, and in this case only 105 456 trials have to be made. In the days before computers this was still a very formidable task, hardly feasible in fact, though even on a PC it would be easy today. In the pre-computer era of the 1930s however it was clear that even with a copy of the machine available

Fig. 4. One of the rotors. Note the notch in the ring at position *M*

a more sophisticated attack than brute force was desirable.

Crytographers of course, including the German Navy experts who analysed the original ENIGMA in 1926, would want to make the machine secure against any attack that they themselves could devise, even on the assumption that their opponents had a copy of the machine available. Various improvements were therefore introduced, not all at once, but over a period spanning about 15 years (1928–1943). These included:

(*i*) increasing the number of rotors in the set available;
(*ii*) introducing a plugboard between the keyboard and *R*1, interchanging pairs of letters—this is equivalent to introducing a static rotor, *R*0 say, of a special type, between *R*1 and the keyboard, but this "rotor" unlike the others can be rewired every day;
(*iii*) making the ring, which is on a rotor, moveable so that the notch can be active at any setting of the wheel rather than always at the same place;
(*iv*) making the alphabet "tyre," which surrounds the case enclosing the wiring, moveable—this makes any knowledge of likely "indicators" (initial settings of the wheels) much less valuable;
(*v*) replacing the reflector (this was done in 1937).

These modifications were all introduced over the years into the military (including Air Force, Naval and State Security (SD)) versions of the ENIGMA and made it much more secure against the original method of attack. The number of rotors in the set was increased from 3 to 5 in December 1938, and this increased the work factor tenfold since the number of possible wheel orderings was now 60 instead of 6. The plugboard ("*Steckerverbindungen*" in German) in its initial form allowed the interchange of only 12 of the 26 letters (*i.e.*, 6 pairs) but later on the number of interchanged pairs was increased to 8, and later still to 10.

The original set of 3 rotors was common to all commercial ENIGMAS but the military versions had a differently wired set of three and, naturally, rotors 4 and 5 were not available commercially either. For further security the German Navy had two more rotors, known as 6 and 7 which were not used by the Army, Air Force or SD ("*Sicherheitdienst*") and, furthermore, the Navy used a 4-rotor ENIGMA from February 1942. The fourth rotor was static and, effectively, produced a variable reflector. (For further information on this see Appendix 2.)

In the early days of the ENIGMA the rotor order was changed very infrequently, every 3 months until 1938, but this very long period was steadily reduced and by 1945 the rotors were changed every 8 hours.

Typically then, by 1939, the work factor associated with the military ENIGMA assuming that the reflector and all the rotor wirings (5) were known (they were not, at that date) would be the product of

60—possible wheel orderings
$(26)^2$—ring settings on *R*1 and *R*2
$(26)^3$—initial rotor positions
10^{11}—approximate number of pairs on a 6-pair plugboard. (The "tyre settings" would not increase the work factor in a brute force attack.)

The product of these numbers is about 10^{20}, which seems to indicate that even with a supercomputer such as

a Cray 2 today (and there were no computers at all in 1939) the task is hopeless and the ENIGMA is secure; but it was not, even in 1932.

5. The Achilles heel of the ENIGMA

With a work factor of something like 10^{20}, even when all the details are known, a cipher machine might seem to be very secure. The security of cipher machines, or of any method of encryption, can however be compromised by bad operating procedure or by mistakes of various kinds. It was a bad operating procedure that allowed a small team of Polish cryptanalysts to succeed in reading a high percentage of pre-War ENIGMA traffic, and, although the operating procedure was later changed, the vastly increased traffic in wartime combined with observed bad habits of the operators enabled the cryptanalysts at Bletchley throughout the rest of the war to read enormous amounts of material—about 84 000 messages a month, on average, from mid 1943 to 1945, for example.

The value of decrypts decreases with the time taken to obtain them and sometimes the Allied commanders in Normandy, and elsewhere, received the information too late to be of immediate use, but at other times the information was available within an hour or so of its original transmission.

What was the bad operating procedure that provided the initial route to the reading of all this traffic? Unlike most of the ENIGMA story it is relatively easy to explain. (Other attacks, such as were employed at Bletchley later, were too complex to explain in an article such as this.)

When an operator wishes to send a message on a 3-wheel rotor machine such as the ENIGMA he must let his intended recipient know the settings of the three rotors at the start of the message: this information is called "the indicator." All operators belong to a network, of which there were many, and will know on any particular day which rotors are to be in which position and which pairs of letters are to be joined in the plugboard (which was a standard feature of military ENIGMAS), this information having been distributed to all members of the network in book form in advance. Different networks, of course, use different rotor orders, etc. The settings for any particular message, however, must be left to the operators since it is essential that messages should not all use the same initial settings and, in any case, no one knows how many messages will have to be sent on any given day, and so how many "indicators" will be needed. Until late 1938 the operators were therefore provided with a "ground-setting" for each day, an initial setting of the three wheels, which they would only use to encipher the setting *which they themselves had chosen* and which would then be used for encryption of the full message.

If the ground setting for the day were *LTE*, say, and the operator chose *PCM* as his indicator he would set the rotors to *LTE* and then encipher *PCM twice* in succession producing, say, *BFQRKD*. The operator then reset the rotors to his chosen setting, *PCM*, and enciphered the message. The transmitted text then consisted of groups indicating the net, the sender, recipient, time, priority, etc., then the twice-enciphered indicator, *BFQRKD*, followed by the enciphered message itself.

This double encipherment of the indicator was the Achilles heel of the ENIGMA and although the system of having a common ground-setting was changed in 1938, which made exploitation of the process more difficult, double encipherment of the indicator continued until May 1940, after which poor operator habits were exploited at Bletchley.

Encipherment of the indicators twice in succession provided the cryptanalyst with information on the encipherment of identical letters repeated three positions apart. Thus, in the case above:

(*i*) the letter which produces *B* at position 1 produces *R* at position 4,

(*ii*) the letter which produces *F* at position 2 produces *K* at position 5,

(*iii*) the letter which produces *Q* at position 3 produces *D* at position 6.

One doubly enciphered indicator was not much use but on a typical net many messages would be sent each day and all the indicators were enciphered at the same ground setting. About 60 such indicators were needed to determine the identity and setting of the fast rotor ($R1$), assuming that the wirings of all the rotors in the set were known. In this article we assume that this is so, but in section 6 there is a short account of how the wirings were actually acquired.

5.1. Exploitation of the doubly enciphered indicators

During the encipherment of six letters the fast rotor, $R1$, moved six times. The middle rotor, $R2$, only moved if $R1$ passed through the position where its ring had its notch, the leftmost rotor $R3$ only moved if $R2$ passed through its notch position. In 21 cases out of 26 therefore only $R1$ moved during the double encipherment of the three letter indicator, which meant that the entire mechanism to the left of the fast rotor, *i.e.*,

$$(R2)(R3)(U)(R3)^{-1}(R2)^{-1},$$

was equivalent to a simple substitution, S say, during the encipherment of the six letters. Since all the indicators were enciphered at the ground-setting a list of 60 or more of these hexagraphs provided a great deal of information about the only two effective components of the enciphering mechanism, viz. the wiring of $R1$ and the simple substitution S. Furthermore S is a reflector type substitution and so can be represented as a set of 13 transpositions of the form, say, $(AD)(BR)\ldots$ and, indeed, the whole ENIGMA degenerates to the form RSR^{-1} and is equivalent to 13 transpositions when R ($=R1$ in fact) remains in one position.

The ENIGMA under these circumstances may be represented diagrammatically in Fig. 5. (There might be a plugboard present; for the Military ENIGMA there would, but that does not affect the basic attack.)

If $R1$ passed through a notch position during the six letter encipherment the single simple substitution S had to be replaced by first one, $S1$, and then another, $S2$. On rare occasions, when $R3$ also moved, a third simple substitution, $S3$, would also be necessary. The solution in these cases would be more difficult but might be helped by other means. To illustrate how the indicators were used we make use of a small scale example, based upon an alphabet of only 8 characters with a single letter indicator which is doubly enciphered. (A more realistic

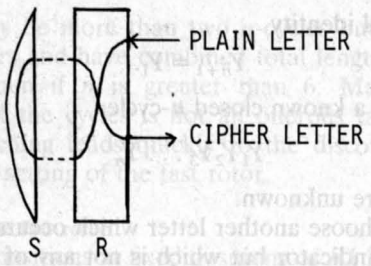


Fig. 5. Effective ENIGMA when $R2$, $R3$ are stationary

example, for those who are interested, is given in Appendix 1.)

5.2. Small scale example

Shown diagrammatically in Fig. 6 is a mini-ENIGMA consisting of an 8-point rotor, $R1$, and reflector S. $R1$ is shown at position 1 and the single letter indicator is enciphered twice, with $R1$ at positions 1 and 2. Since $R1$ moves it is better to show its effect in matrix form. The matrix is easily generated because it has a simple diagonal property that is given by the rule:

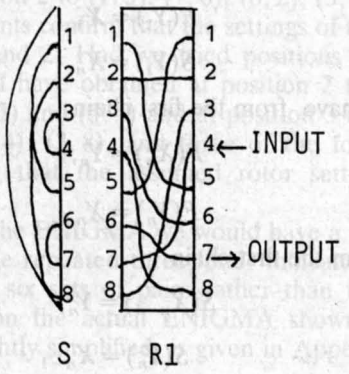


Fig. 6

If X enciphers to Y at rotor position n then $X-1$ enciphers to $Y-1$ at rotor position $(n+1)$—imagine the wires of $R1$ in Fig. 6 moving up one position each time $R1$ moves—all the arithmetic being (mod 8) for this example, (mod 26) for the real ENIGMA. (In the ENIGMA itself the direction of motion of the rotor and the ordering of the alphabet were both in the opposite direction to that shown, but the effect is the same.)

The first two columns of the encipherment matrix of $R1$ and the fixed transpositions of the reflector, S, are therefore

		$R1$		S	
	1	5	1	1	5
	2	2	7	2	8
	3	8	6	3	4
	4	7	8	4	3
Input	5	1	2	5	1 Output
	6	3	5	6	7
	7	6	3	7	6
	8	4	4	8	2

Now trace the path of an input of 1 with the rotor in position 1.

$$1 \rightarrow 5 \rightarrow 1 \rightarrow 5$$
$$R \quad S \quad R^{-1}$$

(in using the matrix form of R for *de*cipherment we look up the appropriate number, 1, in column 1 and note the number of the row, 5, in which it occurs).

If we encipher 1 with the rotor in position 2 we get

$$1 \rightarrow 1 \rightarrow 5 \rightarrow 6$$
$$R \quad S \quad R^{-1}$$

Therefore the double encipherment of the single letter indicator 1 would be the cipher pair: 56. Similarly it will be found that the double encipherment of the single letter indicator 2 is: 33.

Taking both $R1$ and S into account the encipherment matrix for positions 1 and 2 of $R1$ is

	1	5	6
	2	3	3
	3	2	2
Input	4	7	5 Output
	5	1	4
	6	8	1
	7	4	8
	8	6	7
Position		1	2

Note that encipherment at position 1 of $R1$ can be represented by the 4 transpositions

$$(1,5),(2,3),(4,7),(6,8)$$

and at position 2 of $R1$ by

$$(1,6),(2,3),(4,5),(7,8).$$

The complete list of the 8 cipher pairs that can be generated in this way is:

56, 33, 22, 75, 14, 81, 48, 67.

For a reason that is explained below we now "chain" these pairs together, viz:

(56)(67)(75)	gives the cycle (567)
(33)	gives the cycle (33)
(22)	gives the cycle (22)
(14)(48)(81)	gives the cycle (148).

Note that there are two cycles of length 1 and two cycles of length 3. It was proved by Marian Rejewski, the young Polish mathematician/cryptanalyst who was one of the team of 3 who broke the ENIGMA in December 1932, that cycles generated in this way will always occur in pairs, as we shall see.

The cryptanalyst will be able to discover these cycles provided that he is given a sufficiently large set of enciphered indicators although, unlike us in this mini-example, he will not know which plain text inputs produce which cipher pairs. At random some of the plain text letters of the ENIGMA indicators will repeat and so therefore will their cipher equivalents, which means that some of the information from the indicators will be redundant. In practice this redundancy is likely to be much more than we would expect at random since operators tend to pick certain letter combinations (such as *AAA*, *ABC* or *QWE*—the first three letters of the keyboard) as indicators much more frequently than others, a fact which was heavily exploited by the cryptanalysts, before 1932 and subsequently.

Recalling that the encipherment

$$RSR^{-1},$$

provided by the ENIGMA is reflective it follows that when R is in any given position encipherment can be represented as four transpositions in the example, and as 13 transpositions for the ENIGMA itself. As noted above the four transpositions with R at position 1 are

$$(1,5),\ (2,3),\ (4,7),\ \text{and}\ (6,8)$$

and at position 2 of the rotor the four transpositions are

$$(1,6),\ (2,3),\ (4,5)\ \text{and}\ (7,8).$$

Now if we look at the pairs of cycles associated with encipherments at positions 1 and 2 we have (567) and (148)

$$\text{and (2) and (3)}$$

and we note that the two single cycles (2), (3) form a transposition in both positions 1 and 2, and if the two 3-cycles are written

$$\begin{array}{ll} 567 & 5\ldots \\ 184 & 1\ldots \end{array}$$

(one of the cycles in each pair is to be written in reverse order as we shall see below) we see that the vertical pairs (5, 1), (6, 8), (7, 4) are the transpositions at position 1 of the rotor and the diagonal pairs (6, 1), (7, 8), (4, 5) are the transpositions at position 2 of the rotor. The 1-cycle pair (2, 3) is a transposition at both positions.

With the aid of some simple mathematical logic we can now see how the use of these cycles reveals the identity and setting of the rotor $R1$. (I have not seen Rejewski's analysis but, with the advantage of hindsight, I assume that it must have been something like that given in the next section.)

5.3. Relationship between cycles

Assuming that $R2$ and $R3$ are stationary throughout the double encipherment of an indicator let $F(X)$ denote the encipherment of X in the first encipherment of the indicator and let $S(X)$ denote the encipherment of X in the second encipherment of the indicator. We do not know X but we do know $F(X)$ and $S(X)$. Thus we will have information of the type (for the ENIGMA):

$F(X_1) = Y_1$ as the first letter of an indicator,

$S(X_1) = Y_2$ as the fourth letter of the same indicator.

Given a large enough number of indicators we now look for the occurrence of Y_2 as the *first* letter of an indicator viz:

$F(X_2) = Y_2$ and then it follows that

$S(X_2) = Y_3$ (fourth letter of same indicator),

where Y_2 and Y_3 are known but X_2 is unknown. We continue in this way chaining fourth letters to first letters then vice versa, and so on.

Since there are only 26 letters available eventually the chain must close, that is we reach a point where

$$F(X_n) = Y_n$$

and then $S(X_n) = Y_1$.

At this point we have a system of n pairs of equations

$$\begin{aligned} F(X_i) &= Y_i \\ S(X_i) &= Y_{i+1} \end{aligned} \qquad i = 1, \ldots, n$$

and one final identity

$$Y_{n+1} = Y_1.$$

The Y_i form a known closed n-cycle

$$Y_1 Y_2 Y_3 \ldots Y_n$$

but the X_i are unknown.

Now we choose another letter which occurs as the first letter of an indicator but which is not any of the Y_i, and we form the chain beginning with this, and so on until we have used up all available letters. Sooner or later we will be bound to use a letter which is in fact X_1, although we will not know this. Let us see what happens when we choose X_1 as the start of a new chain (whether we choose it as the first or later letter of a chain is irrelevant to the analysis).

Since $F(X_1) = Y_1$, by the reflective property

$$F(Y_1) = X_1$$

and since $S(X_n) = Y_1$ it follows that

$$S(Y_1) = X_n.$$

So our new chain begins:

$$\begin{aligned} F(Y_1) &= X_1 \\ S(Y_1) &= X_n. \end{aligned}$$

We also have, from the first chain

$$F(X_n) = Y_n,$$

so

$$F(Y_n) = X_n.$$

Also, from the first chain

$$S(X_{n-1}) = Y_n,$$

so

$$S(Y_n) = X_{n-1}$$

and our new chain is extended to

$$\begin{aligned} F(Y_1) &= X_1 \\ S(Y_1) &= X_n \\ F(Y_n) &= X_n \\ S(Y_n) &= X_{n-1}. \end{aligned}$$

Continuing in this way we construct a system of n pairs of equations

$$\begin{aligned} F(Y_i) &= X_i \\ S(Y_i) &= X_{i-1} \quad i = n, \ldots, 2, 1 \end{aligned}$$

and the final identity $X_0 = X_n$.

We therefore have a second n-cycle

$$X_n X_{n-1} \ldots X_2 X_1.$$

This not only proves that cycles must occur in pairs it also shows that every n-cycle is related to another n-cycle and that if we align the pair correctly, writing one forward and the other in reverse order, viz.

$$\begin{array}{l} Y_1\ Y_2\ Y_3 \ldots Y_n\ Y_1 \ldots \\ X_1 X_2 X_3 \ldots X_n X_1 \ldots \end{array}$$

the vertical pairs give the transpositions of RSR^{-1} (Y_i, X_i) at the *first* setting of $R(=R1)$ and the diagonal pairs (Y_{i+1}, X_i) give the transpositions of RSR^{-1} at the *fourth* setting of $R1$.

There may be more than two n-cycles but since they occur in pairs and have combined total length of 26 this cannot happen if n is greater than 6. Matching and alignment of the cycles is not an onerous task and the correct matching leads quickly to the discovery of the identity and setting of the fast rotor.

5.4. Setting the fast rotor

The transpositions at fixed positions of $R1$ having been discovered the cryptanalyst now enciphers each transposition pair at the appropriate setting every known rotor at all 26 starting positions in turn. At the correct setting of the correct rotor the decipherments of each related pair in an indicator (1st-4th, 2nd-5th, 3rd-6th) will produce a pair related by a simple substitution, given by S. Furthermore, since S is reflective, S consists of 13 transpositions. Detection of the correct rotor and its initial setting is therefore quite straightforward, since only the correct solution will give consistent transpositions and incorrect settings will quickly produce contradictions. In the example above the pairs (1, 5), (2, 3), (4, 7), (6, 8) encipher at position 1 to (5, 1), (2, 8), (7, 6), (3, 4) and the pairs (1, 6), (2, 3), (4, 5), (7, 8) encipher at position 2 to (1, 5), (7, 6), (8, 2), (3, 4).

These agreements confirm that the settings of the rotor are positions 1 and 2. Had we tried positions 2 and 3 instead we would have obtained at position 2 the pairs (1, 2), (7, 6), (8, 3) and (5, 4) and at position 3 the pairs (6, 2), (5, 7), (1, 4), (3, 8), and three of the four pairs conflict, showing that the assumed rotor settings are incorrect.

In the case of the ENIGMA we would have a lot more evidence since the repeated three letter indicator allows encipherment of six sets of pairs rather than two. An example based on the actual ENIGMA shown in the photographs, slightly simplified, is given in Appendix 1.

5.5. Setting R2 and R3

When $R1$ has been set and the 6-letter indicators deciphered "back" to S we have 13 pairs such as (AG), (BR), ... which are the result of enciphering identical pairs of (unknown) letters through

$$S = R_2 R_3 U R_3^{-1} R_2^{-1}.$$

Since R_2 and R_3 are from a known set of rotors, and U is known, a set of tables can be constructed which show which pairs can occur when rotor A is at position X and rotor B is at position Y. With 5 rotors in the set this would involve the use of 12×676 tables (one of the 5 rotors is eliminated since it is $R1$). Before computers were available this would have been an enormous task but simulators ("Bombes") were built to carry out the work; the original Polish version (1938) contained, in effect, 6 ENIGMAS.

Once all the rotors have been set the ground-setting is known and so the indicators of all messages on that net in that cipher period can be decrypted and all messages read.

6. Recovery of an unknown ENIGMA

When the cryptanalyst begins work on a machine, such as the ENIGMA, where the basic design is known, but none of the details of the internal wirings of the rotors, he faces a formidable task. Until the rotor wirings have been recovered the messages will be unreadable.

There are essentially two ways in which the internal wirings might be recovered:

(1) obtaining, by fair means or otherwise, a copy of the machine;
(2) obtaining the plain texts and corresponding cipher texts and indicators of a large number of messages.

In the case of the ENIGMA, the wirings of the rotors of the commercial machine were readily available, but not those of the original military version. However the French had a spy (known as Asché) who provided them with plain texts and indicators and these were passed to the Poles and enabled them in 1932 to recover rotors 1, 2 and 3. Subsequent rotors (4, 5, 6, 7) were recovered by capture of U-boats and weather ships during the War. Had such captures not been made recovery of the rotors 4–7 would have been possible but would have taken a very long time and would have depended on favourable combinations of known and unknown rotors, e.g., $R1$, $R2$ known, $R3$ unknown, together with a substantial plain text.

7. The effects of the solution of ENIGMA

Less than 20 years ago little or nothing was published about the work at Bletchley and the earlier work by the Poles and French but the publication of various memoirs[5,6,7] and, more recently, the magnificent volumes of the Official History of Intelligence during the War[1–4,8,9] have revealed a great deal of information in the light of which many of the major events of the War in the West and Middle East have had to be reassessed. ENIGMA played relatively little part in the war in the Pacific, where the key cipher device was the Japanese "Purple" machine. A glance at the indexes of the volumes of the official history under the keyword "ENIGMA" will reveal just how important a part Bletchley played in many of the major battles, including the Battle of Britain in 1940, the naval battle of Matapan in 1941, the battle of El Alamein in 1942, the war against the U-boats, and the invasion of Normandy and the subsequent battles in France in 1944–5. There were of course times when ENIGMA traffic could not be decrypted or was decrypted too late to be of much use. It should also be said that whilst the British and American "equivalents" of the ENIGMA, TYPEX and SIGABA, were not "broken," the usage of some of the lower level Allied codes and ciphers was sometimes, particularly in the early years of the War, deplorable and led to heavy losses, particularly in convoys.

There is a lesson which is relevant even today. The weakness of the ENIGMA was not so much its intrinsic design as the poor operational procedures, the double encipherment of the indicator, and the non-random choice of the three letters in the first instance. The same problem is with us today in careless choice of computer passwords, which makes life easy for hackers, virus planters, fraudsters and others of that ilk.

In conclusion however we must acknowledge the cryptanalytic skill of the Poles in 1932 in solving the original ENIGMA. This was a remarkable feat and their decision, in 1939, to tell the British and French what they had done, and how they had done it, made a difference of at least 6 months in Bletchley's subsequent and continued success, thanks to Alan Turing and a host of mathematicians and others, against the increasingly difficult later versions. For a mathematician it is a doubly

fascinating story and now that a great deal of it is in the public domain some 50 years after the events we can give credit to Scherbius who designed the ENIGMA, and the mathematicians who solved his original enigma, those who increased its complexity and those who resolved it again and again. There have been people, including mathematicians who thought that pure mathematics had no practical applications. How wrong they were!

References

1. Hinsley, F. H., *et al.*, "British Intelligence in the Second World War," vol. 1, HMSO, 1979.
2. *ibid*, vol. 2, HMSO, 1981.
3. *ibid*, vol. 3, Part 1, HMSO, 1984.
4. *ibid*, vol. 3, Part 2, HMSO, 1988.
5. Winterbotham, F. W., "The Ultra Secret," Weidenfeld and Nicholson, 1974.
6. Lewin, R., "Ultra goes to War," Hutchinson, 1978.
7. Garlinski, J., "Intercept; the Enigma War," Magnum Books, 1979.
8. *ibid*, vol. 4, "Security and Counter-Intelligence," HMSO, 1990.
9. Howard, M., "British Intelligence in the Second World War," vol. 5, "Strategic Deception," HMSO, 1990.

Appendix 1

Example: Setting the fast rotor on an ENIGMA

The data for this example were generated by the actual ENIGMA shown in the photographs. To shorten the analysis, however, some simplifications, as compared to wartime practice, have been introduced. The simplifications are:

(*i*) there is no plugboard;

(*ii*) the indicators consist of a single letter enciphered at two consecutive positions at the ground setting.

The effect of (*i*) is undoubtedly to make life easier for the cryptanalyst but it also makes the solution more "pure" in that operator characteristics are not assumed; (*ii*) has no effect on the method of solution; identical letters are enciphered at consecutive settings of the fast rotor rather than three positions apart and there is, of course, less evidence available than from a three letter indicator. On the other hand the probability of movement of the middle rotor during the encipherment of the indicator is reduced from 5/26 to 1/26, so the probability of valid analysis is increased.

The total number of trials required for an ENIGMA based upon a set of 7 rotors would, in these circumstances, be some multiple of $182(=7\times 26)$. The method to be described would find the correct rotor and its setting in all cases but to keep the account within reasonable bounds the identity of the rotor is assumed known. Only one particular rotor at one particular setting consistently produces confirmatory digraphs so there is no point in illustrating hundreds of incorrect cases. Suffice to show the rapid rejection of an incorrect "solution" and the confirmation of the correct one.

Data From a batch of two-letter enciphered indicators consisting of doublets enciphered at a common ground-setting the following representative set of 26, sorted by the first letter of the enciphered indicator have been extracted:

AB	*GH*	*ML*	*SJ*	*YG*
BQ	*HC*	*NU*	*TV*	*ZE*
CD	*IR*	*OO*	*UM*	
DK	*JT*	*PI*	*VY*	
EZ	*KS*	*QN*	*WX*	
FF	*LP*	*RA*	*XW*	

(Any conflicts in these digraphs would have indicated an error.)

It is believed that the fast rotor used was Rotor II which enciphers as follows at setting *A*:

Input: *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

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

Problem What is the setting of the fast rotor at the encipherment of the first letter of each indicator?

Preparatory work To try all possible settings of the rotor would require the construction of a 26×26 *encipher* table and a 26×26 *decipher* table which would give the encipherment (decipherment) of every letter at every rotor setting.

To generate these tables is easy for if α enciphers to β at setting n then $(\alpha-1)$ enciphers to $(\beta-1)$ at setting $(n+1)$; and similarly for the decipher table. Since the decipher table is just the complement of the encipher table a knowledge of the encipherment of *A, B, C,* ... *Z* at setting *A,* as given above, enables us to generate both 26×26 tables.

It will suffice, for this example, to write down the first few lines of the *encipher* table, see Table I.

For *decipherment* we look up the cipher letter in the row of the table corresponding to the rotor setting and read the input letter at the top of its column. For example the decipherment of *S* at setting *B* is *R*.

Solution (1) We must first find the cycles generated by the indicators as explained in Sections 5.2 and 5.3. We know that these must occur in pairs of equal length and we find, by the process of chaining:

A B Q N U M L P I R *C D K S J T V Y G H*	of length 10
E Z *W X*	of length 2
F *O*	of length 1

To obtain the solution we must align pairs of equal length, with one of the pair written in reverse order, so

Table I

Input letter

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

that vertical pairs of letters form transpositions at setting 1 and diagonal pairs (SW to NE) form transpositions at setting 2. There are obviously 20 (10×2) ways of aligning these pairs.

Fortunately the alignment of the 1-cycles is unique, *FO* is a transposition both at setting 1 and at setting 2. We therefore begin by exploiting this information and following up its consequences.

(2) *Suppose the rotor is at setting A*
Then *FO enciphers* to *SE* at setting *A* and *SE deciphers* to *RJ* at setting *B*. This implies that *RJ* is a diagonal pair so the alignment of the 10-cycles is

A B Q N U M L P I R
K D C H G Y V T J S

This, in turn, implies that *AK* is a transposition at setting *A* and so since

AK enciphers to *BF* at setting *A*
and *BF* deciphers to *DF* at setting *B*

we conclude that *DF* should be a transposition (diagonal pair) at setting 2. However we know that *OF* is a transposition at setting 2, so we have a contradiction (and *DF* contradicts the *DQ* given by the 10-cycles, for good measure).

We conclude that setting *A* is incorrect.

(3) *Suppose the rotor is at setting B*
Proceeding as before:

FO enciphers to *FT* at setting *B*
and *FT* deciphers to *UK* at setting *C*

This implies that the alignment of the 10-cycles is

A B Q N U M L P I R
T J S K D C H G Y V

If this is correct *AT* is a transposition at setting *B*, and so:

since *AT* enciphers to *WH* at setting *B*
and since *WH* deciphers to *TB* at setting *C*

we conclude that *TB* should be a transposition (diagonal pair) at setting *B* and we see that this agrees with the alignment of the 10-cycles above.

This is encouraging so we try another vertical pair, e.g., *RV*:

since *RV* enciphers to *SG* at setting *B*
and since *SG* deciphers to *NS* at setting *C*

we deduce that *NS* should also be a diagonal pair, and this is indeed the case.

(4) We conclude that the fast rotor is Rotor II and is set at position *B* at the start. (Confirmation of the other transpositions is left as an exercise for the reader.)

Appendix 2

Introduction of the Fourth Rotor

I am grateful to Dr. Shaun Wylie, who worked on German Naval Enigma at Bletchley, for providing the information on which the following is based.

The fourth rotor was a thin stator, which did not move during encipherment, but which could be set in any of 26 positions. It was placed between the slow rotor and the reflector. In order to make room for this additional rotor the original reflector was replaced by a thin version. The combined width of the thin reflector and thin stator was the same as that of the original "thick" reflector.

In order to keep all Enigmas compatible throughout the modification period the thin rotor and stator were so designed that when the stator was set at a particular setting the combined effect was the same as that of the original thick reflector. (Shaun adds that at Bletchley they usually referred to this arrangement as "the split *Umkehrwalz*" and he thinks that there were eventually two stators and two reflectors.)