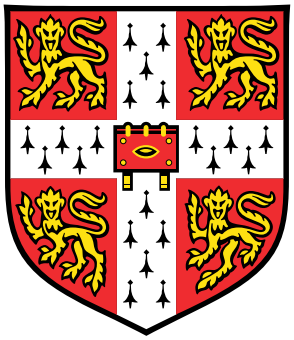
Recreation of the Polish Cyclometer and its role in the breaking of Enigma



Henry A. Evans

Department of Engineering

University of Cambridge

This report is submitted for the degree of

Master of Engineering

Clare College

2019

Contents

Some pages have been omitted
from this online publication

2 Background

2.1 Historical Background

During the 1920s and 30s, directly contrary to the Treaty of Versailles of 1919, Germany was strengthening its military forces and was looking to reclaim its former eastern territories lost after the First World War – territories which, at the time, belonged to Poland. In anticipation of another war with Germany, the Polish government were monitoring German communications to keep track of the threat. However, from 1928, Polish intelligence began intercepting German radio transmissions that were impervious to standard methods of breaking. The ciphertext was "something akin to the work of a blind man who reaches into a printer's cases and takes out pieces of type at random" (Kozaczuk, 1984, p. 6). These were messages that had been sent using a new cipher system, the Enigma code, specifically the military version.

Unable to read these Enigma encoded messages, the Polish Cipher Bureau (*Biuro Szyfrów*) recruited three mathematics students from a cryptology course organised by the Bureau in 1929 in Poznań. These students were Marian Rejewski, Henryk Zygalski and Jerzy Różycki. The Bureau also acquired a commercial Enigma machine from Germany, the type used by business firms, in attempts to solve Enigma. However, the addition of the commercial Enigma machine helped only in the understanding its basic operation. Kozaczuk comments:

> The device was produced on much the same principle as a Yale door lock, mere familiarity with which hardly enables one to open another such lock. One still needs the key. (Kozaczuk, 1984, p. 13)

Crucially, the German military rotors were wired differently from those in the commercial version. Therefore the cryptologists could only make progress by studying the system from a mathematical perspective.

Breaking the Enigma coding system involved two distinct matters:

(i) the theoretical reconstruction of the Enigma itself, specifically the wiring of the rotors and reflector and;

(ii) methods for reconstructing the keys for Enigma exclusively on the basis of radio intercepts.

The solution of the first of the two matters is what many now consider to constitute one of the greatest feats in the entire history of cryptanalysis (Carter, 2008; Perera, 2010). To

fully explain how this was accomplished would be long and complex and is beyond the scope of this report. Notable relevant literature can be found in Carter (2008, pp. 2-7), for a highly abbreviated account, or Kozaczuk (1984, pp. 272-284) for a full mathematical account. However, it is worth mentioning that it was the work of Rejewski, who managed to calculate the exact pattern of internal wiring (including the rotors and reflector) in the military Enigma machine. This was achieved by solving a complex system of mathematical equations, aided by information from French military intelligence and an operational flaw in the Enigma machine itself (it was impossible for a letter to be encrypted by the same letter – one of the major fundamental weaknesses of the Enigma). It also involved intuition, where Rejewski guessed that the connections to the entry wheel (the input to the first rotor) were in alphabetical order (unlike that of the commercial Enigma). Having worked out the wiring pattern, the Cipher Bureau commissioned the AVA Radio Manufacturing Company (*Wytwórnia Radiotechniczna AVA*) to build fifteen doubles (copies of the military Enigma based on the commercial model previously acquired) at the beginning of 1933 (Kozaczuk, 1984, p. 25).

The cyclometer (Polish: *Cyklometr*) is directly concerned with the latter of the two points highlighted above, i.e. as a method for reconstructing the keys for Enigma exclusively on the basis of radio intercepts. In order to appreciate the Polish efforts and understand how the cyclometer works and is constructed, one must first understand the basic theory of Enigma.

2.2 The Basic Theory of the Enigma

2.2.1 The Machine

The Enigma machine consists of electromechanical components that scramble the 26 letters of the alphabet. Its main components are a set of rotors and a reflector, a lampboard, a keyboard and a plugboard (Fig. 2.1). In essence, when one presses a key on the keyboard, a switch is closed and electrical current flows through the plugboard and a set of rotors, and finally results in a bulb illuminating on the lampboard (Fig. 2.2). The main ciphering components are the rotors and a stationary reflector. They are hard-wired internally so as to produce a simple substitution between the inputs and outputs. The combination of all the rotors, reflector and plugboard produces a complex substitution cipher that changes whenever a key is pressed. This is achieved through the stepping of the rotors on each keystroke: the right hand rotor rotates by one step for each keystroke, and the others less frequently. Each letter that is pressed is thus effectively encrypted with a different substitution cipher. This process is self-reciprocal, meaning that to decrypt a message, the

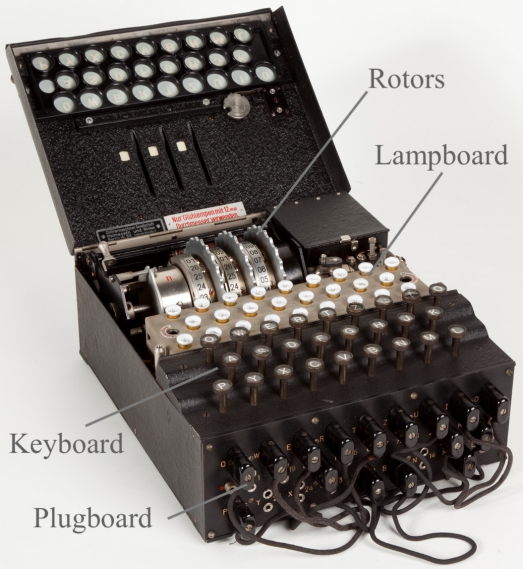


Fig. 2.1. Military model I Enigma machine, displayed with open cover. *Modified from Nassiri (2012).*

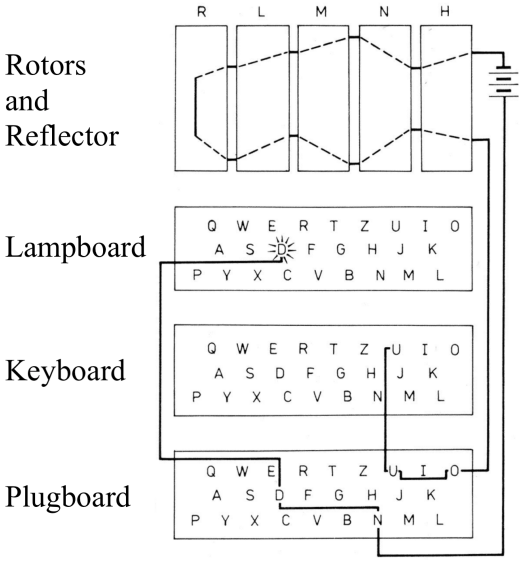


Fig. 2.2. Schematic of current flow though the military Enigma. *Modified from Rejewski (1981, p. 217).*

ciphertext just needs to be 'encrypted' again. It also means that, due to the nature of the reflector, a letter can never be encrypted with itself.

The main security of the Enigma system depends on the settings of the rotors, or what is known as the 'daily key'. It has the following four components:

(i) Rotor Order (*walzenlage*): the order of the three rotors[1] on the shaft

(ii) Rotor Ring Settings (*ringstellung*): each rotor can have its internal ring set to any of 26 positions

(iii) Rotor Starting Position (*grundstellung*): one of the 26 positions of each rotor can be set to appear in the viewing window

(iv) Plugboard Setting (*steckerbrett*): cables can be inserted into the plugboard to connect its letters in pairs.

The four components make up the key. The Germans changed the key quarterly up until 1936, after which it changed monthly, and then daily, leading to the term the 'day's key' (Kozaczuk, 1984; Perera, 2010).

[1] Additional rotors (IV and V) were issued in the build-up to the war. Different branches of the military used different versions of Enigma, some with four rotors.

2.2.2 The Enigma Protocol

It is important to be aware that the German procedures for using Enigma evolved with time. What is described in this report is the protocol that the Polish cryptologists were facing in the period from 1930 until 1938/39.

In order for the Enigma machine to be used for both the encryption and decryption of messages, the receiving Enigma machine must have the same daily key as the transmitting machine. These daily keys were distributed in advance in 'codebooks', so that the receiving operator would know the same set-up as the sender. Rejewski describes the remaining procedure of encipherment:

> The encipherer first set the rotors in the basic position (Grundstellung) established for that day and changed the letters in the commutator by placing the plugs in the appropriate sockets. Then he independently selected the individual key for that message, three letters which he enciphered twice. In this way, he obtained six letters, which he placed at the opening of the message. Next, he set the rotors to the selected individual key and proceeded to encipher his message. (Rejewski, 1984, p. 274)

Rejewski here describes the use of a second type of key, the "individual key", otherwise known as the 'message key'. As he explains, this was a three letter key that was enciphered twice: every Enigma enciphered message therefore started with six letters corresponding to the operator's chosen message key. A receiving operator would enter these first six letters into the Enigma machine, already set to the daily key, and thus recover the (repeated) message key. He would then move the rotors to that key, enter the ciphertext, and the plaintext would appear.

The purpose of sending the message key was to avoid the possibility of intercepting cryptanalysts simply applying frequency analysis to all of the first letters encrypted on a given day, then to all the second letters, and so on (Gaj and Orłowski, 2003; Christensen, 2007). The message key thus prevents the problem of what is termed in cryptanalysis as being 'in depth' – that is, the sending of messages using the same or similar key (Kuhl, 2007). The purpose of sending this message key *twice* was that, for a variety of reasons, radio transmissions were not optimal and thus subject to garbling, resulting in the possible loss of several letters. Since the three letter message key was critical for the receiver to decipher the message, it was repeated.

The German protocol thus necessitated the use of two keys: (i) a daily key and (ii) a message key. To illustrate, given a message key of the sender's individual choice of `NHK`, the sender would first set his Enigma to the daily key, then encrypt `NHKNHK`. For a given

daily key, this may produce FJBRMZ. He would then move the rotors to NHK and encipher the message. The receiving operator would thus first enter FJBRMZ into his machine (already set up to the daily key) and, if done correctly, would be presented with NHKNHK, the repeated message key. He in turn would then move the rotors to NHK and decrypt the ciphertext.

2.2.3 Number of Enigma Keys

In general, the number of possible Enigma keys depended on (i) the plugboard; (ii) the wiring of the rotors; (iii) the order and orientation of the rotors; (iv) the wiring of the reflector and; (v) the ring settings. Authors' calculations often differ for multiple reasons, including whether three or five rotors are considered and whether every possible wiring arrangement is considered. On development of the cyclometer, the Polish cryptologists had already reconstructed the wiring of the rotors and the reflector, and six plugboard leads were in use at the time. They were thus faced with a number of possible keys of:

$$\begin{aligned}\text{Key space} &= \underbrace{100,391,791,500}_{\text{plugboard (6 leads)}} \times \underbrace{3!}_{\text{rotor order}} \times \underbrace{26^3}_{\text{rotor orientations}} \times \underbrace{26^2}_{\text{ring settings}} \\ &= 7,156,755,732,750,624,000\end{aligned}$$

It is worth noting the total theoretical number of different possible keys that the cryptologists were faced with prior to Rejewski determining the internal wiring of the military Enigma machine. Instead of choosing from 3! combinations for the rotor order, they would be faced with $26! \times (26!-1) \times (26!-2) \approx 7 \times 10^{79}$ ways of ordering all the possible rotor combinations in the machine. They would also have faced $\frac{26!}{(13! \times 2^{13})} \approx 8 \times 10^{12}$ different possibilities for the wiring of the reflector. Finally, the plugboard had the potential to have zero to thirteen leads, giving the total number of possible plugboard combinations of 532,985,208,200,576.[2] This results in a possible key space of approximately $3{\times}10^{114}$. To put this into context, the number of atoms in the entire observable universe is approximately 10^{80} (Perera, 2010).[3] The Germans thus thought that the difficulties in overcoming Enigma were "insurmountable" (Kozaczuk, 1984, p. 21): the strength of such an incomprehensibly large key space led the Germans to have complete confidence in the security of the Enigma system (Perera, 2010; Singh, 1999).[4]

[2] See Miller (2010, p. 61) for calculation of this number.

[3] Kahn (2012) further emphasises this point by saying that if a thousand cryptologists were to each test four keys every minute of every day by brute-force, then it would take 1.8 billion years to try all possible keys.

[4] It was learnt in a report published after the war that German cryptographers, at least, did in fact understand that the Enigma was not necessarily unbreakable (Huttenhain and Fricke, 1945) – they just found it inconceivable that anyone would go to the immense effort required (Bamford, 2001, p. 17).

3 Theory

3.1 Exploiting German Procedures of Double Encipherment

Prior to 1936, the Poles had already developed techniques for recovering the keys.[5] However, the increasingly frequent changes of the Enigma set-up to daily changes in 1936 meant that simple paper-and-pencil techniques were becoming laborious and time-consuming. In addition to this, as of October 1936, the Germans changed the number of pairs of letters swapped on the plugboard from five to between six and eight, meaning that it became difficult to use established methods which often relied on the fact that the plugboard did not change every letter (Rejewski, 1981; Gaj and Orłowski, 2003). Rejewski thus sought other techniques of determining the key.

He turned his attention (once again[6]) to the German procedure of double encipherment of the message key. By the nature of doubly enciphering the message key as demonstrated in Section 2.2.2, he knew a simple pattern: he knew that the first and fourth letters were the same. Similarly, he also knew that the second and fifth letters, and the third and sixth letters were the same.

These first six letters were enciphered using the first six permutations for that day, starting with the basic position or daily key. Rejewski labelled these first six permutations **A**, **B**, **C**, **D**, **E** and **F**, or (Carter, 2008, p. 4):

Enigma position	1^{st}	2^{nd}	3^{rd}	4^{th}	5^{th}	6^{th}
Enigma permutation	**A**	**B**	**C**	**D**	**E**	**F**

To demonstrate Rejewski's attack, return to the example given in Section 2.2.2. Rejewski would not have known that the chosen message key was `NHK`, but he would have had access to the intercepted first six letters of the message containing `FJBRMZ`. Say that the first (and hence the fourth) letter of plaintext was denoted by `x`, Rejewski would have known that $\mathbf{A}(\mathtt{x}) = \mathtt{F}$ and $\mathbf{D}(\mathtt{x}) = \mathtt{R}$ (i.e. by permutation **A**, $\mathtt{x} \to \mathtt{F}$, and by permutation **D**, $\mathtt{x} \to \mathtt{R}$). Because the Enigma ciphers are self-reciprocal (Section 2.2.1), if $\mathbf{A}(\mathtt{x}) = \mathtt{F}$ then $\mathbf{A}(\mathtt{F}) = \mathtt{x}$. Thus, for the composition $\mathbf{D} \circ \mathbf{A}$, we have:

$$\mathbf{D} \circ \mathbf{A}(\mathtt{F}) \coloneqq \mathbf{D}(\mathbf{A}(\mathtt{F})) = \mathbf{D}(\mathtt{x}) = \mathtt{R}$$

Rejewski denoted the composite permutation $\mathbf{D} \circ \mathbf{A}$ as **AD**.[7] Thus we can see that $\mathtt{F} \to$

[5] These included what were known as the 'grill method', which was applied in conjunction with the 'clock method', a method developed by Różycki, and the so-called 'ANX method'.

[6] The double encipherment was also exploited in reconstructing Enigma's internal connections.

[7] The composite permutation of **AD**, for example, is the effect of permutation **A** followed by permutation **D**. Note that for disjoint cycles, the order of composition does not matter.

x → R, or simply the transposition F → R. Analogous calculations can be made for **BE** and **CF** giving J → M and B → Z respectively.

If enough messages were intercepted, the full composite ciphers of **AD**, **BE** and **CF** could be deduced. Rejewski writes:

> If we have a sufficient number of messages (about eighty) for a given day, then, in general, all the letters of the alphabet will occur in all six places at the openings of the messages. In each place they form a mutually unique transformation of the set of letters into themselves, that is, they are permutations ... They may be represented as disjunctive products of cycles and then assume a very characteristic form, generally different for each day. (Rejewski, 1984, p. 274)

To demonstrate this, we will investigate several somewhat artificially generated enciphered message keys:

FJA GLK GBW WFB WLB DQV DCE FNX ANS RUO RVO SKL

The product of disjoint cycles can be found by investigating the first and fourth letters of the enciphered message keys: for example, F → G followed by G → W, followed by W → D, followed by D → F, finally returning to F and completing the cycle (this would be followed by F → G etc. again indefinitely). This forms a cycle of length four. The letters would be placed in parentheses, giving (fgwd). This could be done similarly for the next cycle, where A → R followed by R → S, and so on, such that the fragment of the cycle is (ars...).[8]

From the keys of further messages, there would arise further cycles, such that the totality of the cycles formed from the first and fourth letter would appear. In this case, it may transpire that the complete disjoint cycle structure of **AD** is given by:

$$\mathbf{AD} = (\texttt{fgwd})\,(\texttt{lvyp})\,(\texttt{arshxjzte})\,(\texttt{bikocnmuq})\,, \tag{1}$$

with lengths of 4, 4, 9, 9.

Similarly, the disjoint cycles for **BE** and **CF** may transpire to be:

$$\mathbf{BE} = (\texttt{jlqsxz})\,(\texttt{aehbfy})\,(\texttt{cnugd})\,(\texttt{iwpor})\,(\texttt{vk})\,(\texttt{tm})\,,$$
$$\mathbf{CF} = (\texttt{aktznhwbvrodc})\,(\texttt{exiqfsolmyujg})$$

giving lengths of 6, 6, 5, 5, 2, 2 and 13, 13 respectively.

[8] This example is in fact taken from the catalogue reconstruction (Section 4.4), for a rotor order of (III, II, I) and starting position of 'ZZZ'.

Rejewski named the set of permutations the 'characteristic set', or the 'characteristic' for short. The configuration of the characteristics "seldom repeated and, therefore, to a certain degree defined a given day" (Rejewski, 1981, p. 224). Thus, if one were to produce the characteristics for every $3! \times 26^3 = 6 \times 17,576 = 105,456$ possible Enigma set-ups, one could compare with these the characteristics obtained from the message keys for a given day, determining the daily key of the rotors.

To achieve this in practice within a realistic timeframe, the Polish cryptologists devised an electromechanical instrument: they named this the cyclometer.

3.2 The Proof of Rejewski's Theorem

To see how these characteristics relate back to the Enigma machine itself, in addition to providing insight into important theorems regarding the composition of Enigma permutations, it is worth proving one of Rejewski's theorems:

If two permutations of the same degree consist solely of disjunctive transpositions, then their product will include disjunctive cycles of the same lengths in even numbers. (Rejewski, 1984, p. 277).

Suppose that the transposition (a_1a_2) was in permutation **A**. Then the letter a_3 would appear in permutation **D** in some transposition (a_2a_3). Were $a_3 = a_1$, then the cycle would be complete. If not, then a_3 must be in some other transposition in **A** other than (a_1a_2), say (a_3a_4). Now, a_4 must be in some transposition in **D**, say (a_4a_5). This process could continue. In other words:

$$(a_1a_2) \in \mathbf{A} \qquad \text{and} \qquad (a_2a_3) \in \mathbf{D}$$

If $a_1 \neq a_3$ then,

$$(a_3a_4) \in \mathbf{A} \qquad \text{and} \qquad (a_4a_5) \in \mathbf{D}$$

The above can continue and thus be generalised such that :

$$\mathbf{A} = (a_1a_2)(a_3a_4)\ldots(a_{2k-3}a_{2k-2})(a_{2k-1}a_{2k})$$
$$\mathbf{D} = (a_2a_3)(a_4a_5)\ldots(a_{2k-2}a_{2k-1})(a_{2k}a_1)$$

The letter a_1 must eventually appear in the permutation **D**. Schematically, we have:

$$a_1 \xrightarrow{\mathbf{A}} a_2 \xrightarrow{\mathbf{D}} a_3 \ldots a_{2k-1} \xrightarrow{\mathbf{A}} a_{2k} \xrightarrow{\mathbf{D}} a_1$$

Performing the operation of **AD**, we will always get two cycles of the same length:

$$\mathbf{AD} = (a_1 a_3 a_5 \dots a_{2k-3} a_{2k-1})\,(a_{2k} a_{2k-2} \dots a_6 a_4 a_2)$$

This is repeated to exhaust all the letters in the permutation.

Thus, the theorem shows that disjoint cycles always come in pairs and in equal lengths. This is a key observation of Rejewski, often called Rejewski's Theorem.

3.3 The Effect of the Plugboard

A potential complication has so far been overlooked: the effect of the plugboard. This is investigated by first understanding the Enigma algorithm.

Rejewski represented the Enigma rotors as L, M and N from left to right, such that L was the slow rotor and N the fast. Additionally, R represents the reflector and S the plugboard (Fig. 3.1). We can also define a permutation, P, corresponding to the motion of the fast rotor which moves forwards on each keystroke, such that P changes each letter into the next letter of the alphabet.

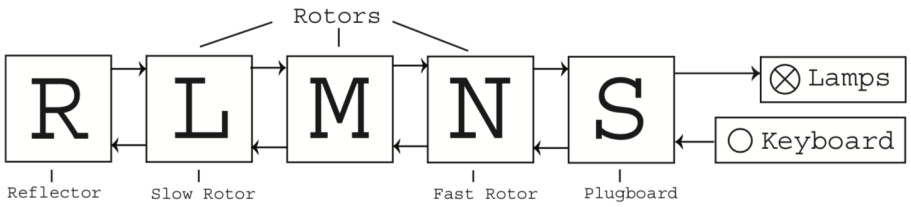


Fig. 3.1. Enigma's functional circuit. Cf. Fig. 2.2. *Reproduced from Christensen (2007, p. 254), based upon Rejewski (1984, p. 274).*

Based on Fig. 3.1, the first six (unknown) permutations of a message, **A**, **B**, **C**, **D**, **E** and **F**, can be written as:

$$\begin{aligned}
\mathbf{A} &= SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}S^{-1} \\
\mathbf{B} &= SP^2NP^{-2}MLRL^{-1}M^{-1}P^2N^{-1}P^{-2}S^{-1} \\
&\dots \\
\mathbf{F} &= SP^6NP^{-6}MLRL^{-1}M^{-1}P^6N^{-1}P^{-6}S^{-1}
\end{aligned}$$

and hence the (known) composite permutations as:

$$\begin{aligned}
\mathbf{AD} &= SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^3NP^{-4}MLRL^{-1}M^{-1}P^4N^{-1}P^{-4}S^{-1} \\
\mathbf{BE} &= SP^2NP^{-2}MLRL^{-1}M^{-1}P^2N^{-1}P^3NP^{-5}MLRL^{-1}M^{-1}P^5N^{-1}P^{-5}S^{-1} \\
\mathbf{CF} &= SP^3NP^{-3}MLRL^{-1}M^{-1}P^3N^{-1}P^3NP^{-6}MLRL^{-1}M^{-1}P^6N^{-1}P^{-6}S^{-1}
\end{aligned}$$

Permutation S (the effect of the plugboard) is applied as the first step, and permutation S^{-1} as the last step to each composite permutation, thus acting on the machine through conjugation. Permutation theory states that *permutations and any of its conjugates have the same cycle type.* That is, conjugate permutations have the same number of cycles of equal length. In fact, only the elements that the inverse of the permutation map into the cycle are changed by the conjugate. This is simple to show: first, consider the conjugate permutation $\rho\pi\rho^{-1}$. Given the single cycle $\pi = (a_1 a_2 \ldots a_k)$, then $\pi a_i = a_{1+(i \bmod k)}$ for $i = \{1,2,\ldots,k\}$. Thus, for $b_i = \rho a_i$ we obtain:

$$\rho\pi\rho^{-1}b_i = \rho\pi a_i = \rho a_{1+(i \bmod k)} = b_{1+(i \bmod k)},$$

and hence

$$\rho\pi\rho^{-1} = (b_1 b_2 \ldots b_k)$$

Therefore $\rho\pi\rho^{-1}$ is also of cycle length k.

Consequently, the disjoint cycle structures of **AD**, **BE** and **CF** are of the same size and length given the conjugate effect of the plugboard. Hence, their sizes and lengths are independent of the plugboard. This is an extremely important deduction[9] – had this not been true, building the catalogue would have required the consideration of not just the 105,456 possible settings of the rotors, but also the 100,391,791,500 different plugboard combinations for six leads (or 532,985,208,200,576 for any number of plugboard leads; Section 2.2.3). The above can thus be simplified to give:

$$\begin{aligned}
\mathbf{AD} &= SP_1P_4S^{-1} \\
\mathbf{BE} &= SP_2P_5S^{-1} \\
\mathbf{CF} &= SP_3P_6S^{-1}
\end{aligned}$$

where $P_\alpha = P^\alpha NP^{-\alpha}MLRL^{-1}M^{-1}P^\alpha N^{-1}P^{-\alpha}$, $\alpha = \{1,2,3,4,5,6\}$, and is determined only by rotor order and starting position.

[9] Some consider this the "theorem that won the war" (Bauer, 2000; Deavours, 1981). Whilst this is an obvious exaggeration, it can be said with some confidence that it indeed helped.

In deducing these equations, Rejewski assumed that only the fast rotor, rotor *N*, moves. Thus, if rotors *M* or *L* were to step, then these equations would not hold. Rejewski tacitly assumed this, as this assumption holds on average for twenty-one out of twenty-six cases (Rejewski, 1984, p. 255).

3.4 The Cyclometer

3.4.1 The Catalogue

Sections 3.1 through to 3.3 proved that if an exhaustive list of characteristics could be produced for every expression of **AD**, then, by comparison with the characteristic for a given day, the set-up (the daily key) could be determined. Furthermore, as a result of the reflector, the Enigma permutations **A**, **B**, **C**, **D**, **E** and **F** are products of 13 disjoint transpositions. It follows that there are 101 ways of decomposing 13 into the sum of positive integers (Carter, 2008, p. 32). Thus, the products **AD**, **BE**, and **CF** can have 101 different characteristics each, or $101^3 = 1,030,301$ characteristics in total, based upon three lists. There are $3! \times 26^3 = 6 \times 17,576 = 105,456$ possible rotor settings: the fact that there are significantly more characteristics than there are rotor settings suggests that it was likely that a given day's characteristic corresponded to either a unique arrangement of the rotors, or at least to a small number of arrangements that could be rapidly tested.

Rejewski and his colleagues set up a card catalogue system to contain the lengths and cycles of the characteristics for each of the 105,456 possible setting of the rotors. No copies of the Polish catalogue exist (Carter, 2008; Christensen, 2007) (see also Section 1.1) and few details of how the data were organised remain, with the exception of one brief reference from Rejewski that implies that the cards for different rotor orders were kept in separate boxes (Rejewski, 1981, p. 225).[10]

3.4.2 The Construction and Operation

The cyclometer (Fig. 3.2) comprised of a panel upon which there were 26 mounted lamps, switches, their respective letters, a single rheostat, and a source of current. It also consisted of two sets of Enigma rotor systems; the rotors did not have adjustable rings, and were permanently fixed to the ring settings 'ZZZ' (Carter, 2008, p. 11). Few other details regarding the mechanical construction of the cyclometer exist, either in historical or contemporary documentation.

[10] Carter discovered that Rejewski and his colleagues would have represented the cycles by ordinal numbers assigned to the 101 ways of decomposing the number 13. These ordinal numbers would then have been used to represent and order the characteristics.

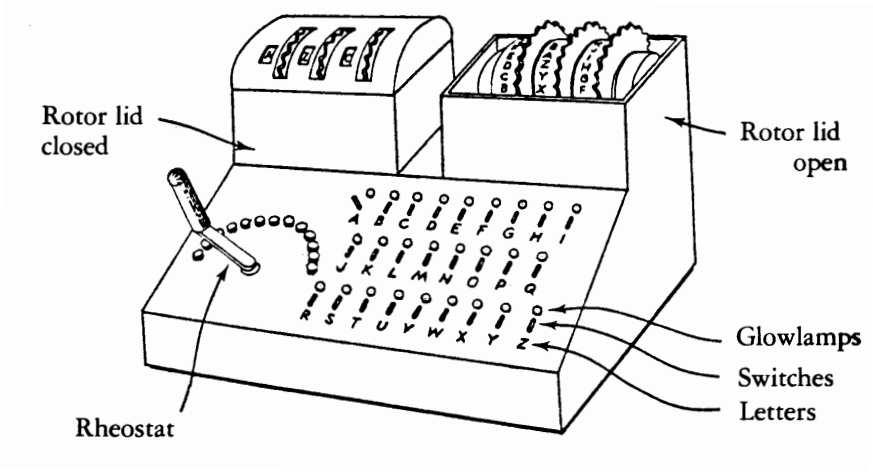


Fig. 3.2. The cyclometer. *Reproduced from Rejewski (1984, p.284).*

The cyclometer was set up such that the right hand rotor system, the second rotor system, was three positions in advance of the first, left hand rotor system. Otherwise, their order was identical. Therefore, in effect, the left hand system represented permutation **A** and the right **D** (or **B** and **E** or **C** and **F** depending on what was being investigated). Upon application of current to any of the 26 bulbs, not only would that bulb illuminate, but also all the bulbs that belonged to the same disjoint cycle and to the other cycle in the pair of equal length. In other words, the current flows first through the rotor system representing permutation **A**, then through the system representing **D**, then back through **A** and so on, until the cycle is complete. Schematically, this is the same as in Section 3.2:

$$a_1 \xrightarrow{\mathbf{A}} a_2 \xrightarrow{\mathbf{D}} a_3 \ldots a_{2k-1} \xrightarrow{\mathbf{A}} a_{2k} \xrightarrow{\mathbf{D}} a_1$$

Thus, the cyclometer determines the cycle characteristics for permutation **AD** in their pairs of equal length: the number of illuminated bulbs is twice that of the cycle lengths of the pair. Having recorded this, the operator would observe which bulbs had not yet illuminated, and instead throw the switch of one of these. The process would be repeated to obtain the succeeding permutation cycles until all of the disjoint cycles of **AD** were known, such that all 26 letters had been accounted for.

Subsequently, the right hand rotor (rotor N) for each system would be advanced by one position, thus to represent permutations **B** and **E**. The above would be repeated, obtaining the characteristics of **BE**,[11] and then again to obtain **CF**.

[11] Since permutation **BE** is one position ahead of **AD**, it is also permutation **AD** for the next rotor starting position.

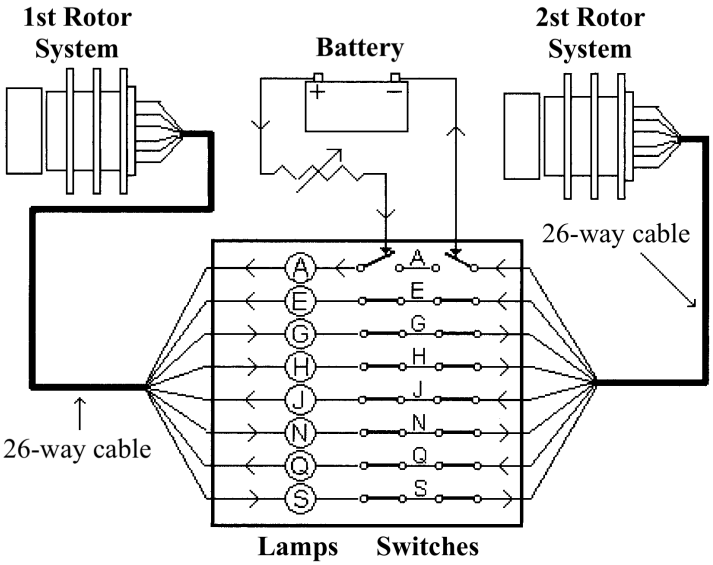


Fig. 3.3. Schematic of cyclometer's operation. *Reproduced from Carter (2008, p. 11).*

An illustrative example helps to clarify the operation.[12] Consider the composite permutation **AD** for a particular rotor set-up:

$$\mathbf{AD} = \begin{pmatrix} \texttt{abcdefghijklmnopqrstuvwxyz} \\ \texttt{JRUXAWNSFQYTBHMDEVGILPKZCO} \end{pmatrix}$$

In disjoint cycles, this is:

$$\mathbf{AD} = \underbrace{(\texttt{ajqe})}_{\lambda}\underbrace{(\texttt{gnhs})}_{\mu}(\texttt{brvpdxzom})\,(\texttt{cultifwky})$$

with lengths of 4, 4, 9, 9. We shall denote the first two cycles of length 4 labels λ and μ.

Suppose switch `A` was thrown, a letter part of λ. This would connect the battery and rheostat into series via a double pole double throw switch (Fig. 3.3). The current would flow through lamp `A`, and pass into the first rotor system, representing permutation **A**. Its output from **A** is, say, `N`, part of μ. The current ('as letter `N`') would then pass through lamp `N` and into the second rotor system, representing permutation **D**. This may emerge, as say, `J`, part of λ. After a certain number of passes, the current would return to lamp `A`. Schematically, we have:

$$\texttt{a} \xrightarrow{\mathbf{A}} \texttt{n} \xrightarrow{\mathbf{D}} \texttt{j} \xrightarrow{\mathbf{A}} \texttt{g} \xrightarrow{\mathbf{D}} \texttt{q} \xrightarrow{\mathbf{A}} \texttt{s} \xrightarrow{\mathbf{D}} \texttt{e} \xrightarrow{\mathbf{A}} \texttt{h} \xrightarrow{\mathbf{D}} \texttt{a}$$

[12] This example and its relevant diagrams are based upon Carter (2008, pp. 10-12).

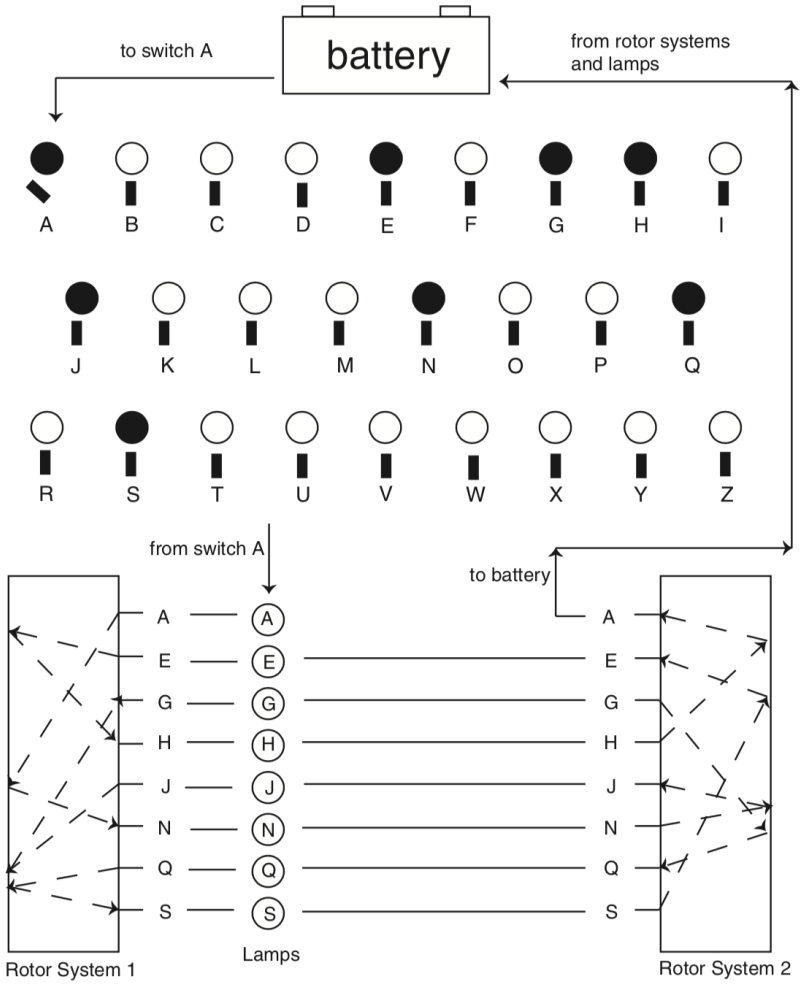


Fig. 3.4. Schematic of cyclometer's operation based on Carter (2008, p. 10). For clarity, the second rotor system is reversed in the diagram from that of the physical orientation (as in Fig. 3.3). *Reproduced from Christensen (2007, p. 261).*

Thus, all the lamps in the cycles λ and μ have been illuminated. They would display on the panel as shown in Fig. 3.4. The number of illuminated lamps, 8, is double the number of letters in one of the cycles of **AD**. If switch A were then re-closed, and any other letter in cycles λ or μ opened, the same pattern would emerge. If any letter other than in cycles λ or μ were thrown, the remaining 18 lamps would light, displaying the other pair of disjoint cycles.

All of the bulbs that are illuminated are in fact electrically connected in series. The rheostat on the left hand side of the machine is thus used to vary the voltage drop across the bulbs: since the cycle lengths vary, the number of bulbs in series changes, meaning that the total voltage drop across the bulbs can be small or large depending on whether the cycle is short or long respectively. The operator should therefore start out with a high resistance

across the rheostat (and hence a low voltage drop across the bulbs) to prevent burning out the filaments and gradually decrease its resistance to increase the bulbs' brightness.

In this fashion, with the help of the cyclometer, the Polish cryptologists catalogued every characteristic for all 105,456 possible rotor orders and starting positions. Rejewski writes:

> This job took a long time, over a year, since we carried it out along with our normal work at reconstructing daily keys using the grill. Once all six card catalogs were ready, though, obtaining the daily key was usually a matter of ten to twenty minutes. The card told the drum positions [the rotor positions], the box from which the card had been taken told the drum sequence [the rotor order], and permutation S was obtained by comparing the letters in the cycles of the characteristic with the letters in the cycles of permutations AD, BE, CF, which were obtained by tapping on the machine's keyboard. (Rejewski, 1981, p. 225)

It should be reiterated that, since it was assumed that the middle and left-hand rotors did not move (Section 3.3), the cyclometer's characteristics were, on average, correct for 21 times out of 26.

3.4.3 Historical Postlude

Rejewski writes:

> Unfortunately, on 2 November 1937, when the card catalog was ready, the Germans exchanged the reversing drum that they had been using, which they designated by the letter A, for another drum, a B drum, and, consequently, we had to do the whole job over again, after first reconstructing the connections in drum B, of course. (Rejewski, 1981, p. 225)

Some pages have been omitted
from this online publication

References

Bamford, J. (2001). *Body of Secrets*. Century.

Bauer, F. L. (2000). *Decrypted Secrets: Methods and Maxims of Cryptology*. Springer-Verlag, Berlin, second edition.

Carter, F. (2008). *The First Breaking of Enigma*. Bletchley Park Trust.

Christensen, C. (2007). Polish Mathematicians Finding Patterns in Enigma Messages. *Mathematics Magazine*, 80(4):247–273.

Deavours, C. (1981). Afterwards. In Rejewski, M., editor, *How Polish Mathematicians Broke the Enigma Cipher*, volume 3, pages 229–232. Institute of Electrical and Electronics Engineers (IEEE).

Ertel, W., Jans, L., Herzhauser, W., and Feßler, J. (2010a). An Enigma Replica and its Blueprints. *Cryptologia*, 35(1):16–21.

Ertel, W., Jans, L., Herzhauser, W., and Feßler, J. (2010b). Enigma-pläne: Erstellt für einen nachbau der historischen chiffriermaschine. Technical report, Hochschule Ravensburg-Weingarten, University of Applied Sciences, Weingarten.

Flack, T. (2018). Personal communication.

Gaj, K. and Orłowski, A. (2003). Facts and myths of enigma: Breaking stereotypes. In *Lecture Notes in Computer Science*, pages 106–122. Springer Berlin Heidelberg.

Huttenhain, O. and Fricke (1945). OKW/Chi Cryptanalytic Research on Enigma, Hagelin and Cipher Teleprinter Messages. *TICOM*.

Kahn, D. (2012). *Seizing the Enigma*. Pen & Sword Books Ltd.

Kozaczuk, W. (1984). *Enigma: How the German Machine Cipher Was Broken and How It Was Read by the Allies in World War Two*. Arms & Armour Press.

Kuhl, A. (2007). Rejewski's catalog. *Cryptologia*, 31(4):326–331.

McCarthy, J. (2018). Personal communication.

Miller, R. (2010). The Cryptographic Mathematics of Enigma. In Perera, T., editor, *Inside Enigma*. Radio Society of Great Britain.

Nassiri, A. (2012). File:Enigma (crittografia) - Museo scienza e tecnologia Milano.jpg — Wikimedia Commons, the free media repository. https://en.wikipedia.org/wiki/Enigma_machine. Online; accessed May 15, 2019.

Perera, T. (2010). *Inside Enigma*. Radio Society of Great Britain.

Rejewski, M. (1981). How Polish Mathematicians Broke the Enigma Cipher. *IEEE Annals of the History of Computing*, 3(3):213–234.

Rejewski, M. (1984). Appendix E, The Mathematical Solution of the Enigma Cipher by Marian Rejewski. In Kozaczuk, W., editor, *Enigma: How the German Machine Cipher Was Broken and How It Was Read by the Allies in World War Two*. Arms & Armour Press.

Sale, T. (n.d.). The Breaking of Enigma by the Polish Mathematicians. https://www.codesandciphers.org.uk/. Online; accessed May 20, 2019.

Schmeh, K. (2016). British expert builds Enigma cracking machine. http://scienceblogs.de/klausis-krypto-kolumne/2016/07/10/britischer-experte-baut-enigma-knackmaschine-nach/. Online; accessed May 14, 2019.

Singh, S. (1999). *Code Book, The: The Secret History of Codes and Code-breaking*. Fourth Estate.