Polish Mathematicians Finding Patterns in Enigma Messages

CHRIS CHRISTENSEN
Northern Kentucky University
Highland Heights, KY 41099
christensen@nku.edu

> *Whenever there is arbitrariness, there is also a certain regularity. There is no avoiding it.* Marian Rejewski [**14b**, p. 235].

This is a story about heroes. Its heroes are three Polish mathematicians who in the decade before World War II broke German Enigma messages. It seems rare that mathematicians are heroes of stories, and it seems even rarer that they are heroes because they are mathematicians. A recent exception is Robert Harris' novel *Enigma* [**7**] (and the 2002 Michael Apted film *Enigma* that was based upon it). In *Enigma*, which is based upon the work of the British World War II codebreakers at Bletchley Park, the hero is Tom Jericho, a mathematician whose successes are loosely based upon the work of Alan Turing. (The novel *Enigma* was reviewed by Peter Hilton who served at Bletchley Park from 1942 until the end of the war in Europe in the June 1996 *Notices of the American Mathematical Society* [**8**].)

World War II seems to mark a change in cryptology. Although mathematician Werner Kunze was recruited as a cryptologist by Germany in World War I[1] and there are examples of mathematicians studying codes and ciphers throughout the history of cryptology, World War II seems to mark the point at which cipher bureaus began to recruit mathematicians for their problem solving abilities—for their abilities to find patterns. The Government Code and Cipher School at Bletchley Park recruited many mathematicians. Probably their two most famous recruits are Alan Turing [**10**] and Gordon Welchman [**27**]. The United States Signals Intelligence Service, which was organized by William Friedman, had among its first recruits two mathematicians, Frank Rowlett [**23**] and Abraham Sinkov [**26**], and statistician Solomon Kullback [**17**]. The heroes of our story Jerzy Różycki (Roozh-IT-ski), Henryk Zygalski (Zig-AHL-ski), and Marian Rejewski (Rey-EF-ski)[2] were mathematics students at Poznań University when they were recruited into a cryptology course in 1929.

The story of the Polish mathematicians' success against Enigma is well known to cryptologists. Rejewski was able to use elementary theorems about permutations to determine the wiring of the Enigma rotors and to determine the Enigma settings. "If ever there was a real-world story problem handed to mathematics teachers on a silver platter, this would be it." [**21**, p. 371]

We will return to the work of the three Polish mathematicians, but first we will take a moment to examine substitution ciphers and the operation of Enigma.

[1] "Kunze was presumably the first professional mathematician to serve in a modern cryptanalytic bureau." [**2**, p. 85]

[2] Guides to pronunciation are taken from [**14**].

Substitution Ciphers

`SAKSP VPAPV YWAVH QLUS`

A substitution cipher is a method of concealment that replaces, for example, each letter of a plaintext message with another letter. Here is the key to a simple substitution cipher:

Plaintextletters :	`abcdefghijklmnopqrstuvwxyz`
Ciphertextletters :	`EKMFLGDQVZNTOWYHXUSPAIBRCJ`.

The key gives the correspondence between a plaintext letter and its replacement ciphertext letter. (It is traditional to use small letters for plaintext and capital letters for ciphertext.) Using this key, every plaintext letter `a` would be replaced by ciphertext `E`, every `e` by `L`, etc. The key describes a permutation of the alphabet. Just as in abstract algebra courses, the internal structure of the permutation is revealed when it is written as a product of disjoint cycles. In this case, our permutation consists of a 10-cycle, two 4-cycles, one 3-cycle, two 2-cycles, and a 1-cycle.

`(aeltphqxru)(bknw)(cmoy)(dfg)(iv)(jz)(s)`

There are $26! = 403{,}291{,}461{,}126{,}605{,}635{,}584{,}000{,}000$ possible keys for such simple substitution ciphers. The security of ciphers often depends on the cipher "having a large key space"—having too many keys for the cryptanalyst to do a brute force attack of trying all the keys. This is certainly the case for our substitution cipher. If the cryptanalyst tried one key per second, it would take 4,667,725,244,520,898,560,000 days to try all possible keys. Yet, such keys are used to encipher the cryptograms that appear regularly in newspapers and puzzle books, and these cryptograms are routinely broken in a few minutes. What makes it possible to break these ciphers?

Patterns. Every language has rules so that the language "makes sense." These rules create patterns in messages that can be exploited by cryptanalysts. Usually cryptograms that appear in newspapers preserve word length and punctuation, but even without that information these simple substitution ciphers can be solved. The letter `e` is the most frequent letter in plaintext English. If we used the key that was described above, we would expect that the most frequent ciphertext letter would be `L`. Now, it might not be, but it is likely that the most frequent ciphertext letter corresponds to one of `e`, `t`, `a`, `o`, `i`, `n`, or `s`. Using letter frequencies and other patterns, simple substitution ciphers are usually quickly solved. Such an attack on ciphertext is called frequency analysis.

Here is a more secure method of enciphering. Instead of using the same permutation to replace each letter of the plaintext, we will have a collection of permutations and will use one permutation to determine the replacement for the first letter, another permutation to determine the replacement for the second letter, etc. Certainly there are enough permutations available to use a different permutation for each plaintext letter. This is the idea for the cipher called a one-time pad; it is the only provably secure cipher. But, there are practical problems that makes it difficult to implement this idea by hand—keeping track of the order in which the permutations will be used and communicating the order to an authorized receiver. The one-time pad is provably secure because it uses a random ordering of the permutations; there are no patterns for the cryptanalyst to discover. The classical Vigenère cipher, which was developed in the Sixteenth Century, is based on a similar idea, but it uses a small number of permutations—typically many fewer than the number of characters in the message. The key for a Vigenère cipher prescribes a rotation among the permutations—permutation number one, permutation number two, . . . , permutation number n—repeated as necessary depending on the length of the plaintext message. The Vigenère cipher was broken in the Nineteenth Century by using frequency analysis to discover patterns that become evident in the sets of ciphertext letters that are enciphered using the same permutation.

Enigma is a mechanical way to generate a large number of permutations. Although it was one of the first, Enigma was not the only machine cipher. For example, during World War II, the United States used William Friedman's SIGABA, and the British used TypeX. In fact, rotor machines dominated cryptography from the 1920s into the 1970s. Enigma began as a device to protect commercial communications.

Enigma

> *If you have no good coding system, you are always running a considerable risk. Transmitted by cable or without wire, your correspondence will always be exposed to every spy, your letters, to being opened and copied, your intended or settled contracts, your offers and important news to every inquisitive eye. Considering this state of things, it is almost inconceivable that persons interested in those circumstances should delay securing themselves better against such things. Yet, ciphering and deciphering has been a troublesome art hitherto. . . . Now, we can offer you our machine "Enigma", being a universal remedy for all those inconveniences.*
>
> Mid-1920s Enigma sales brochure reprinted in the
> July 2001 *Cryptologia*. See [**28**, p. 246].

Although Enigma was only one of a family of machine ciphers, it has attracted the most interest because of the exciting stories of the "duels" between the machine and, first, the Polish and, then, the British codebreakers. The story of the solution of Enigma began to become visible in 1974 with the publication of *The Ultra Secret* by F. W. Winterbotham [**29**]. Since that time much has been written about Enigma and the duel. Because of the secret nature of military cryptography and cryptanalysis, that story is often muddled and contradictory, but there is a clear trail from Arthur Scherbius' 1918 patent of a machine designed to protect commercial communications to the German military Enigma of World War II.

Here is how Enigma works. The Enigma machine consists of four visible components: a keyboard, a plugboard, a rotor system, and a lampboard. (See the front cover and Figure 1.) Enigma has both electric and mechanical parts. The executive summary of its operation is that the operator pushes a plaintext letter on the keyboard and the corresponding ciphertext letter is lighted on the lampboard.

Forget for a moment about the mechanical part of Enigma and follow the electrical action from the keyboard to the lampboard in Figure 2.

When the operator pushes a key on the keyboard (`A` is the key in the diagram), an electrical current passes from the key to the plugboard. The plugboard looks like an old telephone switchboard. There are 26 sockets—one for each letter of the keyboard.

Throughout the war, the Enigma machine evolved and the methods for using it changed. Different branches of the German military used different models of the machine, and the same model was used in a different manner by different branches. So, a description of how Enigma operated is dependent on who was using it and when they were using it. This description applies to the Enigma that the Polish mathematicians were attacking in 1932.

When the Polish mathematicians began their attack on Enigma, six plugs were in use. Each plug would connect (in a way prescribed by the key) one letter on the plugboard to another. The effect of the plugboard was to swap six pairs of letters and let

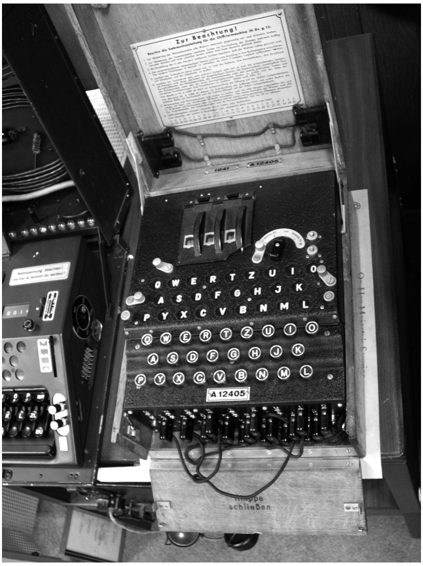

Figure 1 Closed Enigma

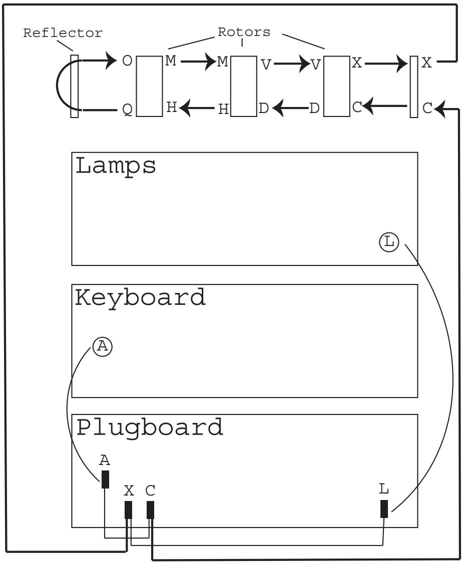

Figure 2 Enigma Diagram

the remaining 14 letters pass through unchanged. The plugboard consisted of six transpositions; 14 letters were fixed by the plugboard permutation. Later in the war, more plugs were used. In the diagram, the plugboard permutation includes the transposition (AC); so, A is replaced by C by the plugboard. (Not all versions of Enigma had a plugboard.)

After passing through the plugboard (*Steckerbrett*, steckerboard), the electrical charge passed into the rotor system. In 1932, the rotor system consisted of three rotors and a reflector. Each rotor permuted the letters of the alphabet. The right-hand side of each rotor had 26 spring-loaded input terminals arranged around the disk; the left-hand side had 26 flat circular output terminals. Each input was wired to an output. The wiring determined the permutation. At the time that the Polish mathematicians began attacking Enigma, the machine had only three rotors; later the machine had as many as eight rotors from which either three or four were installed depending on the type of Enigma in use. Rejewski and the other Polish mathematicians did not know the wirings of the rotors. As we will see later, one of Rejewski's remarkable feats was his determination of the rotor wirings from intercepted messages alone. The three rotors were labelled I, II, and III; the labels identified the rotors but did not correspond to the positions of the rotors in the machine. When placing the rotors in Enigma, all six orderings of the three rotors were possible. In Figure 2, the rotors have been installed in the order I, III, II. The permutations accomplished by the three rotors are:

Rotor I (aeltphqxru)(bknw)(cmoy)(dfg)(iv)(jz)(s)
Cycles 10 4 4 3 2 2 1

Rotor II (a)(bj)(cdklhup)(esz)(fixvyomw)(gr)(nt)(q)
Cycles 8 7 3 2 2 2 1 1

Rotor III (abdhpejt)(cflvmzoyqirwukzsg)(n)
Cycles 17 8 1

Following the diagram, the electrical charge enters the rotor system as C. C enters the right-hand rotor and exits as D, D enters the middle rotor and exits as H, H enters the left-hand rotor and exits as Q, and then Q enters the reflector at the left of the rotor system.

The reflector was “half a rotor.” There were only 26 contacts on the right-hand side of the reflector. Internally, the 26 contacts were joined in pairs by wires to create a permutation consisting of 13 disjoint transpositions. At the time that we are considering, Enigma had just one reflector (reflector A). Its wiring was also not known to the Poles. It creates the following permutation:

Reflector A (ae)(bj)(cm)(dz)(fl)(gy)(hx)(iv)(kw)(nr)(oq)(pu)(st)

In the diagram, Q enters the reflector and exits as O.

Then the electrical charge passes backwards through the rotor system. The O enters the left-hand rotor, passes backwards through it, and exits as M. Then M enters the middle rotor, passes backwards through it, and exits as V. Next V enters the right-hand rotor, passes backwards through it, and exits as X.

The X then passes through the plugboard where it is changed to L, and lamp L lights. The operator would substitute ciphertext L for plaintext A.

This is an unduly complicated way to do a single permutation, but the point of the process is that the mechanical portion of Enigma allows for the generation of a long sequence of different permutations. Each time that a letter on the keyboard is pressed, before enciphering begins, the right-hand rotors turns one letter forward. The output side of the right-hand rotor has a notch that causes the middle rotor to turn forward. Like the odometer of a car, the middle rotor will turn forward one letter once during every 26 turns of the right-hand rotor. Similarly, there is a notch on the output side of the middle rotor that causes the left-hand rotor to turn forward one letter once during every 26 turns of the middle rotor. The theoretical maximum of $26^3 = 17576$ permutations is not actually achieved by Enigma because the mechanical movement of the rotors is such that the middle rotor can “double step”—it can rotate forward on two subsequent presses on the keyboard [**6**]. So, $26 \times 25 \times 26 = 16900$ keys can be pressed on the keyboard before the rotor system returns to the initial permutation. For a given setup of Enigma, 16900 substitution ciphers are generated in order; the period of Enigma is 16900.

The Polish Mathematicians

The King hath note of all that they intend,
By interception, which they dream not of.
—Henry V, Act II, Scene 11[3]

In the 1930s, in direct contradiction of the Versailles Treaty of 1919, Germany was rearming and was looking to reclaim its “lost” territories in the east—territories that were at that time part of Poland. The nervous Poles followed the German buildup by monitoring German radio transmissions. But the Germans had learned from their cryptological mistakes of World War I and were using better encryption—they were using Enigma. Unfortunately for Poland, “there were few persons adept at cryptology in Poland at this time.” [**14**, p. 2]

To solve the problem of the lack of cryptologists, in 1929, the Polish government selected some mathematics students from Poznań University to participate in a cryptology course. Poznań was selected because of its location in an area where students

[3] This quote appears at the beginning of “The History of Hut 8, 1939–1945” by Patrick Mahon. Mahon served in Hut 8 (German Naval cryptanalysis) at Bletchley Park from 1941 until the end of the war; he was director of Hut 8 from 1944 until the end of the war. Alan Turing was the first director of Hut 8.

would be German speakers. Why mathematics students were selected is not clear, but, in a manner that was similar to the later recruiting done by the British for Bletchley Park, the Polish codebreakers were recruited by teachers and colleagues.

> Well, one day or one evening, I don't remember which, one of the younger mathematics students came up to me and said that on such-and-such a day, at such-and-such an hour, Professor [Zdzisław] Krygowski [director of Poznań University's Mathematics Insitute] wanted me to come to the Institute. This student had some sort of list, and he would go and tell each of the persons on the list about this. Not everyone was invited, only a certain number [of] selected students. What the criteria were, I can only guess . . . . I expect it wasn't Professor Krygowski who selected the students but rather Section II [the Intelligence Section of the Polish General Staff] that had made the selection. Probably there had been correspondence between Section II and Professor Krygowski, and on the basis of this correspondence Professor Krygowski had given them a list of all the third- and fourth-year students . . . who were close to graduating, and then Section II had by its own methods conducted some kind of selection. In any case, not all the students were selected . . . . Marian Rejeweski [**14b**, p. 229].

Among the students who were selected were Jerzy Różycki, Henryk Zygalski, and Marian Rejewski.

On March 1, 1929, Rejewski (who is pictured on the front cover) received his master of philosophy in mathematics. Without having completed the cryptology course, because of an interest in actuarial mathematics, he went to Göttingen for a period of training. He returned to Poznań in October, 1930, and took a position as a teaching assistant. He also began work at the Poznań office of the Polish Cipher Bureau [Biuro Szyfrów, BURE-oh SHIF-roof].

During the Summer of 1932, the Poznań office was disbanded and Rejewski, Różycki, and Zygalski (the latter two had just graduated) became employees of the Cipher Bureau in Warsaw.

So begins the story of the Polish mathematicians and their duel with the Enigma machine. The most important of these was Rejewski, and in what follows we will focus on two applications of the theory of permutations to the attack on Enigma—determining the order of the Enigma rotors and determining the wiring of the Enigma rotors.

Setting Up Enigma

> *When two Enigma machines are set to the same key and their three wheels are in the same positions, the electrical connections through their steckerboards and scramblers will produce the same thirteen pairings of the twenty-six letters of the alphabet. . . . Thus, if pressing letter-key* `K` *on one of the machines causes lamp* `P` *to be lit, then pressing letter-key* `P` *on the other machine will cause lamp* `K` *to be lit.* [**27**, p. 45]

Two Enigma operators could communicate only if their Enigma machines were set up using the same key. Daily keys were provided to the operators in a book, for example, for a month at a time. There were several settings which made up the Enigma key. In 1932, the following made up the key.

Plugboard: The key specified which 6 pairs of letters were to be connected on the plugboard. For example, `CO DI FR HU JW LS`.

Rotor order: The key specified the order in which the rotors were placed in the rotor system (from left to right). For example, I III II.

Ring setting: There was a ring around the circumference of each rotor on which the letters of alphabet A, B, . . . , Z or the numbers 01, 02, . . . , 26 were engraved. This ring could be rotated around the circumference and then held in place with a pin. The ring setting of the key indicated the letter of the alphabet on the ring that corresponded to the position of the pin. For example, P K M. The purpose of the ring setting was to set the letters on the ring with respect to the internal wiring of the rotor. The permutations that were given in Section 3 for each rotor assume that the ring setting for each is A. Another effect was to position the turnover notch. The notch was in a fixed position on the left side of each rotor. Changing the ring setting changed the position of the turnover with respect to the internal wiring of the rotors.

Groundsetting: This portion of the key specified the position of each rotor at the beginning of sending or receiving a transmission. The groundsetting indicated which letter on each ring should be visible in the windows above the three rotors, for example, N K U. These settings made up the key.

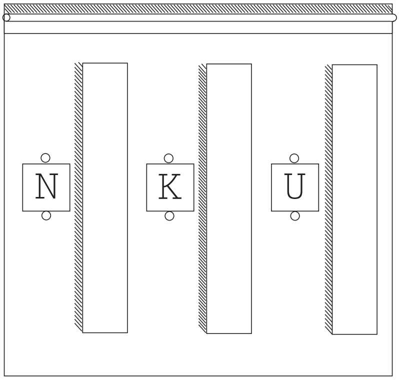

Figure 3 Enigma Rotor Cover closed with setting at NKU

The Number of Enigma Keys

> *[If] a man were able to adjust, day and night, a new key at every minute, it would take him 4000 years to try all those possibilities through on[e] after another.*
>
> Mid-1920s Enigma sales brochure reprinted in the July 2001 *Cryptologia*. See [**28**, p. 252].

The security of Enigma depends on its having a large key space. The size of the keyspace equals the number of possible plugboard settings × the number of possible rotor orders × the number of possible ring settings × the number of possible ground settings.

The number of possible plugboard settings: Assume that n plugs are being used. There are

$$\frac{[26 \times 25] \times [24 \times 23] \times [22 \times 21] \times \cdots \times [(26 - 2n + 2) \times (26 - 2n + 1)]}{2^n \times n!}$$

ways to connect n plugs into the plugboard. Here is a table which shows the number of connections for each of the possible number of plugs.

n	Number of connections	n	Number of connections
0	1	7	1,305,093,289,500
1	325	8	10,767,019,638,375
2	44,850	9	53,835,098,191,875
3	3,453,450	10	150,738,274,937,250
4	164,038,875	11	205,552,193,096,250
5	5,019,589,575	12	102,776,096,548,125
6	100,391,791,500	13	7,905,853,580,625

When the Poles began to attack Enigma, six plugs were in use. So, there were 100,391,791,500 ways to connect the six plugs into the plugboard. Later the Germans used ten plugs.

The number of possible rotor orders: There are six ways to arrange the three rotors in order in the rotor system.

The number of possible ring settings: Only the positions of the notches on the right-hand and middle rotors contributed to the cryptographic security of Enigma. So, we will say that there are $26^2 = 676$ possible ring settings.

The number of possible groundsettings: There are $26^3 = 17576$ choices of the letters to appear in the windows.

So, effectively, the number of possible keys was

$$100,391,791,500 \times 6 \times 676 \times 17576 = 7,156,755,732,750,624,000$$

which would seem to be secure enough.

Enigma Ciphers

> *. . . we shall see that cryptography is more than a subject permitting mathematical formulation, for indeed it would not be an exaggeration to state that* abstract *cryptography is* identical *with abstract mathematics.*
>
> A. A. Albert [**1**, p. 903]

There are $26! = 403,291,461,126,605,635,584,000,000$ simple substitution cipher permutations, but there are many fewer possible Enigma substitution cipher permutations. Consider the diagram (Figure 4) "Enigma's functional circuit" that is based upon a figure in [**14e**, p. 274] and uses Rejewski's notation. S represents the plugboard (*Steckerbrett*); N represents the right-hand, or fast, rotor; M represents the middle rotor; L represents the left-hand, or slow, rotor; and R represents the reflector.

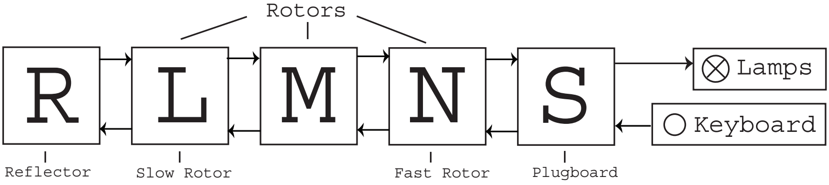

Figure 4 Enigma's functional circuit

Think of S, N, M, L, and R as permutations. There is one permutation missing from Enigma's functional circuit. There should be a permutation P: N ← S corresponding to the motion of the fast rotor which moves forward one letter every time a key is pressed. $P = (\texttt{abcdefghijklmnopqrstuvwxyz})$. Rejewski's attack on Enigma uses only the first six ciphertext letters; so, he assumes that the middle and left-hand rotor do not move, but if they do move, his method will not work. Because the middle rotor turns only once in every 26 turns of the fast rotor, it is reasonable to assume that the middle rotor and the left-hand rotor do not move during the first six encryptions. For the first enciphered letter, the permutation is

$$\mathrm{SPNMLRL^{-1}M^{-1}N^{-1}P^{-1}S^{-1}} = \mathrm{(SPNML)R(SPNML)^{-1}}.$$

Rejewski composes his permutations from left to right, and we will follow his notation.

For the second enciphered letter, the permutation is

$$\mathrm{SP^2NMLRL^{-1}M^{-1}N^{-1}P^{-2}S^{-1}} = \mathrm{(SP^2NML)R(SP^2NML)^{-1}}.$$

Whether the middle and left-hand rotors move or not, an Enigma permutation is always a conjugate of the reflector. So, an Enigma permutation is always a product of 13 disjoint transpositions. There are no more than

$$\frac{\binom{26}{2}\binom{24}{2}\cdots\binom{2}{2}}{13!} = 7{,}905{,}853{,}580{,}625$$

such permutations, many fewer than the 26! possible simple substitution permutations.

The fact that every Enigma permutation is a product of 13 disjoint transpositions is what permits Enigma to encipher and decipher in the same mode. Every Enigma permutation is self-reciprocal.

But, being self-reciprocal can also be a weakness. The reflector permutation guarantees that every Enigma permutation is self-reciprocal, but it also guarantees that no letter can be enciphered as itself. The latter was useful information for British cryptanalysts. The cryptanalysts who attacked Enigma would know, for example, that ciphertext T did not correspond to plaintext t. The same rule usually applies to cryptograms that appear in newspapers (so-called "aristocrats")—no letter ever substitutes for itself. With such a rule, we would know, for example, that the trigraph JFE could not represent plaintext the.

The Entry Permutation

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

The Enigma Keyboard[4]

There is another permutation that was not considered in the "Enigma functional circuit"—the entry permutation. For the original, commercial Enigma, the entry permutation corresponded to the order of the keys on the Enigma keyboard q → A, w → B, e → C, . . . :

Output from Plugboard:	abcdefghijklmnopqrstuvwxyz
Entry into Rotors:	JWULCMNOHPQZYXIRADKEGVBTSF.

[4] The arrangement of the keys on an Enigma keyboard differs slightly from the arrangement on a keyboard today.

In the process of solving for the wirings of the rotors, Rejewski assumed that the entry permutation—the permutation from the plugboard into the right-hand rotor—was the same as for the commercial Enigma, but permutations that should have been similar were not.

> . . . it finally occurred to me [Marian Rejewski] that the cause of my failure may have been merely a mistaken assumption as to the connections of the entry drum. [**14d**, p. 257]

Dillwyn ("Dilly") Knox, a British codebreaker who was also attacking Enigma, was also stumped by the entry permutation.

> I [Marian Rejewski] have the fullest grounds to believe that the British cryptologists were unable to overcome the difficulties caused by the connections in the entry drum. When the meeting of Polish, French, and British cipher bureau representatives took place in Poland in July 1939, the first question that the British cryptologist Dillwyn Knox asked was: What are the connections in the entry drum? Knox's niece, Penelope Fitzgerald states in her book *The Knox Brothers*, published in 1978, that Knox was furious when he learned how simple it was.
>
> What . . . were the connections in the entry drum? It turned out later that they can be found by deduction, but in December 1932, or perhaps in the first days of 1933, I obtained those connections by guessing. I assumed that, since the keyboard keys were not connected with the successive contacts in the entry drum in the order of the letters on the keyboard, then maybe they were connected in alphabetical order; that is, the permutation caused by the entry drum was an identity and need not be taken into account at all. The hypothesis turned out to be correct. [**14d**, pp. 257 & 258]

The permutation from the plugboard to the rotor system was:

Output from Plugboard:	`abcdefghijklmnopqrstuvwxyz`
Entry into Rotors:	`ABCDEFGHIJKLMNOPQRSTUVWXYZ`.

Peter Twinn was one of the first mathematicians recruited to Bletchley Park. Twinn was working with Knox when the Poles revealed the secret of the wiring from the keyboard to the entry drum. In *The Telegraph* [November 17, 2004] obituary of Twinn, he is quoted as saying:

> I know in retrospect it sounds daft. It was such an obvious thing to do. Rather a silly thing, that nobody, not Dilly Knox, not Alan Turing, ever thought it worthwhile trying.

Sometimes it is good to guess.

Rotor Order and Groundsetting

> *The double encipherment of each text setting . . . was a gross error. It enabled us to attack the million-odd combinations of wheel order and ring settings without bickering about the vast number of steckerboard cross-connections in which the German experts had placed their trust . . . .*
>
> Gordon Welchman [**27**, p. 164]

The quote refers to techniques used by the codebreakers at Bletchley Park, but it also applies to the power of Rejewski's methods. Rejewski was able to discover patterns in the Enigma messages and apply the theory of permutations to defeat the plugboard and determine the rotor order and groundsetting.

Recall that the effective number of Enigma keys is

$$100{,}391{,}791{,}500 \times 6 \times 676 \times 17576 = 7{,}156{,}755{,}732{,}750{,}624{,}000$$

where 100,391,791,500 corresponds to the number of possible connections of the plugboard. The product $6 \times 17576 = 105{,}456$ corresponds to the number of possible rotor orders and groundsettings. (We will, as Rejewski did at this point, ignore the $26^2 = 676$ ring settings. Recall that the ring settings set the position of the turnovers [and we are assuming that turnover did not occur], and the ringsettings set the relation between the letters on the circumferences of the wheels with respect to the internal wiring [and Rejewski had other methods to determine that relationship].) Rejewski was able to reduce the large number of keys to the smaller 105,456, which is not small but is more manageable than 7,156,755,732,750,634,000.

Recall that Enigma was designed to generate a long sequence of simple substitution ciphers. The goal was to defeat frequency analysis by effectively using a different permutation to encipher each plaintext letter of a message. That is a good idea. But, there is still a problem, and the problem is called "depth." Say that every Enigma operator sets up his machine according to the instructions and begins every message with the same groundsetting—the same letters appearing in the windows on top of the Enigma. Permutation P_1 will encipher the first letter of every message, P_2 will encipher the second letter of every message, ... , P_{50} will encipher the fiftieth letter of every message, ... This would happen for every message enciphered by every operator. If it were possible to intercept a large number of messages, say 100, then the first letter of each message would have been enciphered with P_1. If we stripped off the first letter of each message we would have 100 ciphertext letters each enciphered with the same simple substitution cipher. We could apply frequency analysis (perhaps, modified for this letter to use frequencies of initial letters) to this collection and have a chance of determining P_1. And, we could proceed similarly for the second letter of each message, the third letter of each message, etc. This is called depth. Although there might not be repetition of ciphers within a message, there is repetition within the collection of 100 messages.

Prior to World War I, most cryptanalysis was done by lone cryptanalysts working in "Black Chambers" attacking individual ciphertext messages. The use of radio in World War I changed the nature of cryptanalysis. Suddenly there were hundreds or thousands of messages that could be attacked by teams of cryptanalysts.

German Enigma procedures were designed to defeat the problem of depth. At the time that the Poles first encountered Enigma, Enigma procedures required that each Enigma message be enciphered using a different setting of the rotors—different letters appearing in the windows on top of the machine. It was left to each operator to determine the three-letter message setting. If each message were enciphered with a different message setting, depth would not occur. But, how would the message setting be sent from the sender to the receiver? How would the key be distributed? The solution that the Germans decided upon was to use Enigma to encipher the message setting—the three-letter message setting was enciphered using the groundsetting. Because radio transmission was subject to garbling, the operators sent the message setting twice. So, preceding each ciphertext message were six letters that were two copies of the message setting enciphered with the first six permutations beginning with the groundsetting. Rejewski calls these first six permutations A, B, C, D, E, and F.

For example, say we have decided our message setting will be NKU. After setting up Enigma according to the instructions given in the key, we first encipher nkunku. Let us assume that these letters encipher to JHNQBG. These six letters would be sent in the preamble to the ciphertext. When the receiving operator received the transmission, he would set his machine according to the instructions given in the key. Beginning with the groundsetting, he would press the keys JHNQBG. The lamps nkunku should light. The operator would then set his rotors to NKU, and enter the ciphertext; the plaintext message should appear.

It was in these enciphered double message settings that Rejewski discovered a pattern.

Rejewski would not have known the message setting NKU, but he would have known that the first letter, say ?, of the message setting was changed to J by permutation A and changed to Q by permutation D. A: ? → J and D : ? → Q . Because Enigma ciphers are self-reciprocal, we know that AD: J → ? → Q.

The composition AD changes J to Q. Similarly, BE changes H to B, and CF changes N to G.

Now what remains is to collect enough ciphertext messages.

> 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. Marian Rejewski [**14e**, p. 274]. Cf. [**14d**, p. 234].

Here is a list of 65 enciphered double message settings AUQ AMN, . . . , ZSJ YWG taken from [**2**, p. 390].

AUQ AMN
BNH CHL
BCT CGJ
CIK BZT
DDB VDV
EJP IPS
FBR KLE
GPB ZSV
HNO THD
HNO THD
HXV TTI
IKG JKF
IKG JKF
IND JHU
JWF MIC
JWF MIC
KHB XJV
KHB XJV
LDR HDE
LDR HDE
MAW UXP
MAW UXP
NXD QTU
NXD QTU
NLU QFZ
OBU DLZ
PVJ FEG
QGA LYB
QGA LYB
RJL WPX
RJL WPX
RJL WPX
RJL WPX
RFC WQQ
SYX SCW
SYX SCW
SYX SCW
SYX SCW
SYZ SCW
SJM SPO
SJM SPO
SJM SPO
SUG SMF
SUG SMF
TMN EBY
TMN EBY
TAA EXB
USE NWH
VII PZK
VII PZK
VQZ PVR
VQZ PVR
WTM RAO
WTM RAO
WTM RAO
WKI RKK
XRS GNM
XRS GNM
XOI GUK
XYW GCP
YPC OSQ
YPC OSQ
ZZY YRA
ZEF YOC
ZSJ YWG

Consider the first and fourth letters of each indicator. We can notice that the composition cipher AD replaces A by A, B by C, C by B, D by V, E by I, F by K, G by Z, etc. The composition cipher AD is

abcdefghijklmnopqrstuvwxyz
ACBVIKZTJMXHUQDFLWSENPRGOY.

In terms of disjoint cycles,

$$\mathrm{AD} = \texttt{(a)(bc)(dvpfkxgzyo)(eijmunqlht)(rw)(s)},$$

and the lengths of the cycles are 10 10 2 2 1 1.

Similarly,

$$\mathrm{BE} = \texttt{(axt)(blfqveoum)(cgy)(d)(hjpswizrn)(k)},$$

and the lengths of the cycles are 9 9 3 3 1 1.

$$\mathrm{CF} = (\texttt{abviktjgfcqny})(\texttt{duzrehlxwpsmo}),$$

and the cycles are 13 13.

Rejewski saw that the disjoint cycles assume a very characteristic form, "generally different for each day [i.e., for each groundsetting] . . . ." [**14e**, p. 274] Furthermore, Rejewski realized that the cycle structure is not affected by the plugboard. For example, consider

$$\mathrm{A} = \mathrm{SPNMLRL^{-1}M^{-1}N^{-1}P^{-1}S^{-1}} \quad \text{and} \quad \mathrm{D} = \mathrm{SP^4NMLRL^{-1}M^{-1}N^{-1}P^{-4}S^{-1}}.$$

$$\begin{aligned} \mathrm{AD} &= \left(\mathrm{SPNMLRL^{-1}M^{-1}N^{-1}P^{-1}S^{-1}}\right)\left(\mathrm{SP^4NMLRL^{-1}M^{-1}N^{-1}P^{-4}S^{-1}}\right) \\ &= \mathrm{S}\left(\mathrm{PNMLRL^{-1}M^{-1}N^{-1}P^{-1}}\right)\mathrm{S^{-1}S}\left(\mathrm{P^4NMLRL^{-1}M^{-1}N^{-1}P^{-4}}\right)\mathrm{S^{-1}} \\ &= \mathrm{SP_1P_4S^{-1}} \end{aligned}$$

where $\mathrm{P_1} = \mathrm{PNMLRL^{-1}M^{-1}N^{-1}P^{-1}}$ and $\mathrm{P_4} = \mathrm{P^4NMLRL^{-1}M^{-1}N^{-1}P^{-4}}$ are each determined only by the rotor order and groundsetting. Because of the theorem from elementary permutation theory that the disjoint cycle structure of a permutation and a conjugate of the permutation are the same, the disjoint cycle structure of AD is the same as it would be if there were no plugboard; the effect of the plugboard has been nullified!

Similarly, the disjoint cycle structure of BE and CF is not affected by the plugboard. Rejewski can determine the rotor order and ground setting without considering the 100,391,791,500 possible plugboard connections. Momentarily, he also ignored the 676 ring settings, and he is, therefore, left with "only" the possible $6 \times 17576 = 105{,}456$ rotor orders and groundsettings.

Rejewski assumed that the middle (and left-hand) rotor did not turn during these six permutations. Because the middle rotor turned only once during 26 turns of the right-hand rotor, this was a reasonable assumption. If a turnover did occur, his method would not work.

For each of the 105,456 settings, the Poles determined the characteristic disjoint cycles. To do this they devised a machine called a cyclometer. (See Figure 6, p. 261.)

The cyclometer consisted of two sets of Enigma rotors. One of the six rotor orders (e.g., I III II) was selected and both sets of Enigma rotors were arranged in that order. Then the first set of rotors was set to a groundsetting (e.g., NKU), and the second set of rotors was stepped three positions beyond the groundsetting (NKX). So, the rotors were set up as if they were permutations A and D. Again, it was assumed that the middle rotor did not turn during the six indicator permutations.

A charge was applied to one of the letters, say A. The charge passed through the first rotor system and the output of the first rotor system passed through the corresponding lamp, say N. Then N entered the second rotor system and the output of the second rotor system, say J, passed through the corresponding lamp and entered the first rotor system. This process continues until the charge returns to A. The diagram[5] shows the situation when (ajqe) is a cycle of the permutation created by the cyclometer. Because that permutation is conjugate to AD, AD also contains a 4-cycle. Notice that applying current to any of A, J, Q, or E would result in the same cycle. Also notice that this 4-cycle results in the lighting of eight lamps; G, N, H, and S also light and correspond to another 4-cycle of the permutation AD. If a charge were applied to G, N, H, or S, the same lamps would light.

[5] This diagram is based upon an example and diagram in [**4**]

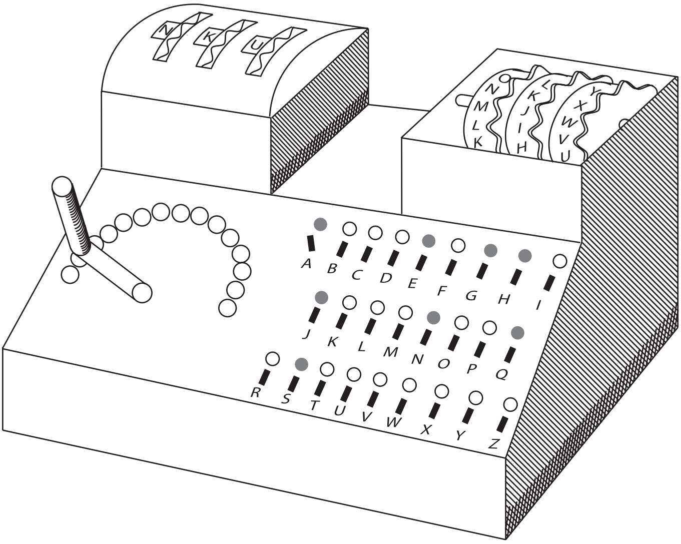

Figure 5 Cyclometer

The cyclometer is equipped with a rheostat so that the amount of current in the circuit can be varied according to the number of lamps that are lit. (In case many lamps are lit, the current can be increased to strengthen the light coming from the lamps; if few lamps are lit, the lower current would be less likely to burn out the filaments.)

The eight lamps that are lit told the Poles that AD contained two 4-cycles.

Then a charge was applied to a letter other than A, J, Q, E, G, N, H and S; and another pair of disjoint cycles was determined. This process was continued until the lengths of all of the disjoint cycles of AD were known.

Then both rotors were moved forward one position—to NKV on the first rotor and NKY on the second rotor. The permutation that the cyclometer now creates is conjugate to BE, and the lengths of the disjoint cycles of BE are determined. Then each rotor is advanced forward one more position to create a permutation conjugate to CF, and the lengths of the disjoint cycles of CF are determined.

The Poles catalogued the lengths of the disjoint cycles to all $6 \times 17576 = 105{,}456$ possible rotor orders and groundsettings. These lists of the lengths of disjoint cycles were called the characteristics of the permutation. Apparently no copies of their catalogue still exist; so, it is not known how the Polish mathematicians ordered the characteristics.

The mapping from rotor orders and groundsettings to characteristics is not one-to-one. Several rotor orders and groundsettings can result in the same characteristic.

Rejewski describes the use of the cyclometer:

> One had to note on a card the position of the drums and the number of bulbs that were lit, and to order the cards themselves in a specified way, for example by the lengths of the cycles.
>
> 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 grille [another method of cryptanalysis used by the Poles]. Once all six card catalogues [one for each of the six possible orders of the rotors] were ready, though, obtaining a daily key was usually a matter of ten to twenty minutes. The card told the drum positions [the letters appearing in the window on the top of the Enigma], the box from which the card had been taken told the drum sequence [the ordering of the rotors], and

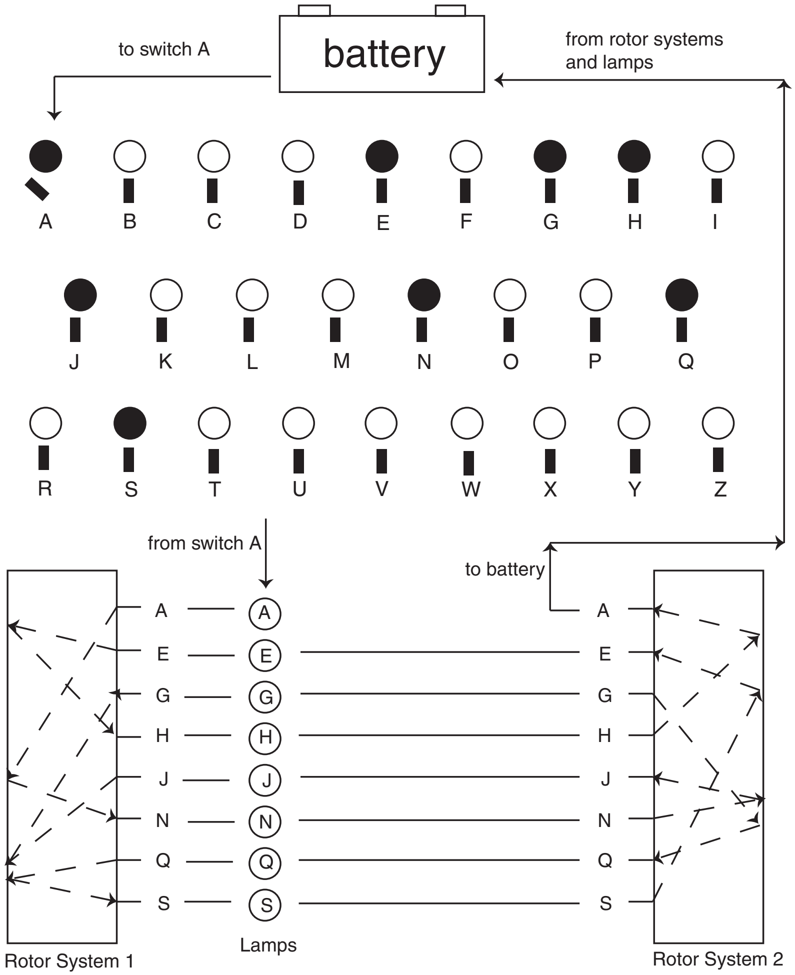

Figure 6 Cyclometer diagram

> the permutation S [the permutation resulting from the plugboard] was obtained by comparing the letters of the cycles of permutations AD, BE, CF, which were obtained by tapping on the machine's keyboard. [**14d**, pp. 263 & 264]

How far from being one-to-one is the mapping from rotor orders and groundsettings to characteristics? Carter conducted a modern reconstruction of a portion of a catalogue (see [**4**, p. 10f]); he used one rotor order and reflector B, which was not the reflector in use when the Poles were assembling their catalogue.[6] Carter comments:

> It now seems apparent that the use of the catalogue to determine the daily starting positions, from the composite cycle pattern could not have been an entirely straightforward procedure. In bad cases, the number of possibilities given by the catalogue would have been daunting and, if attempted, would have required the subsequent checking of large numbers of possible alternative starting positions. For the majority of patterns however, the starting positions would have been

[6] The wiring of reflector A had not yet been rediscovered when Carter constructed his catalogue. The wiring was reconstructed and published in 2000.

> found immediately from the catalogue, or at most after checking on only a few alternatives [**4**, p. 11].

Kuhl [**16**] considered all rotor orders and groundsettings and used reflector A, which was the reflector in use when the Poles were assembling their catalogue.

Soon after the Poles completed the catalogue there was a change in Enigma.

> Unfortunately, on 2 November 1937, when the card catalogue was ready, the Germans exchanged the reversing drum [reflector] 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. Marian Rejewski [**14d**, p. 264]

Rejewski's Theorems

> *Nonetheless, the Polish mathematicians at B.S.-4* [Biuro Szyfrów-4, the German cipher office]*—thanks to the cycle principle discovered by Marian Rejewski, . . . were able to quickly distinguish total chaos from the merely ostensible chaos that resulted when initially ordered impulses flowed through the machine's innards.* [**14**, pp. 42 and 43]

In addition to the theorem that conjugation preserves disjoint cycle structure, Rejewski in his two papers [**14d**] and [**14e**] explicitly states four theorems and uses another.

THEOREM 1. (THEOREM ON THE PRODUCTS OF TRANSPOSITIONS) *If two permutations of the same degree consist solely of disjoint transpositions, then their product will consist of disjoint cycles of the same length in even numbers.*

He argues its proof as follows:

$X = (a_1a_2)(a_3a_4)(a_5a_6)\ldots(a_{2k-3}a_{2k-2})(a_{2k-1}a_{2k})$
and $Y = (a_2a_3)(a_4a_5)(a_6a_7)\ldots(a_{2k-2}a_{2k-1})(a_{2k}a_1)$,
then $XY = (a_1a_3a_5\ldots a_{2k-3}a_{2k-1})(a_{2k}a_{2k-2}\ldots a_6a_4a_2)$.

"If, in this manner, we have not exhausted all the letters in the permutation, we continue our procedure until we have done so." [**14e**, p. 278]

Composing permutations is a routine activity in abstract algebra courses, but what Rejewski needed to do was factor the permutations AD, BE, and CF.

THEOREM 2. (CONVERSE TO THE THEOREM ON THE PRODUCT OF TRANSPOSITIONS) *If a permutation of even-numbered degree includes cycles of the same length in even numbers, then this permutation may be regarded as a product of two permutations, each consisting solely of disjoint transpositions.*

Recall that each of AD, BE, and CF satisfy the conditions of this theorem. Its proof is immediate from what was noted above.

Given $XY = (a_1a_3a_5\ldots a_{2k-3}a_{2k-1})(a_{2k}a_{2k-2}\ldots a_6a_4a_2)$,
then we can write $X = (a_1a_2)(a_3a_4)(a_5a_6)\ldots(a_{2k-3}a_{2k-2})(a_{2k-1}a_{2k})$
and $Y = (a_2a_3)(a_4a_5)(a_6a_7)\ldots(a_{2k-2}a_{2k-1})(a_{2k}a_1)$.

Rejewski notes two other results that follow from the proof of his *Theorem on the Product of Transpositions*:

THEOREM 3. *Letters entering into one and the same transposition of permutation X or Y, enter always into two different cycles of the permutation XY.*

and

THEOREM 4. *If two letters found in two different cycles of the same length of the permutation XY belong to the same transposition, then the letters adjacent to them (one to the right, the other to the left) also belong to the same transposition.*

Lawrence [**20**] proves a generalization of Rejewski's factoring method.

Rejewski also notes one more fact about conjugation. Rejewski does not call this a theorem, but we will here. Say, we consider a conjugation of the permutation H.

THEOREM 5. *If* $\mathrm{H(i) = j}$*; i.e.,* $\mathrm{H = (\ldots i\, j \ldots)}$*; then* $\mathrm{T^{-1}HT = (\ldots T(i)T(j) \ldots)}$. *Notice that this implies that* $\mathrm{H = (\ldots i\, j \ldots)}$ *and* $\mathrm{T^{-1}HT = (\ldots T(i)\ T(j) \ldots)}$ *have the same disjoint cycle decomposition.*

For a proof, Rejewski notes that $\mathrm{T(i)(T^{-1}HT) = i(HT) = H(i)T = T(j)}$.

In particular, we note that this means that the entries of the permutations can be ordered so that

$$\begin{aligned} \mathrm{H} &= \big(\ \ldots\ldots \quad \mathrm{i} \quad \mathrm{j} \quad \ldots\ldots\ \big) \\ \mathrm{T^{-1}HT} &= \big(\ \ldots \quad \mathrm{T(i)} \quad \mathrm{T(j)} \quad \ldots\ \big) \end{aligned}$$

which describes the permutation T in two-row notation.

These theorems are used by Rejewski to determine the wiring of the right-hand (fast) rotor using the disjoint cycle description of AD, BE, and CF.

Finding the Wiring of the Right-Hand Rotor—The Fast Rotor

> *Still working in isolation, Rejewski's next step was to develop a mathematical representation of the working Enigma machine. He was hoping that the knowledge of permutations A to F would enable him to work out the wiring of the wheels. He had reduced the problem to a set of six equations involving three unknown permutations, and he was wondering whether they could be solved, when, at just the right moment, he was given four documents from the German traitor Asche.*
>
> Gordon Welchman [**27**, p. 210]

Rejewski was also able to use the enciphered double indicators to determine the wiring of the right-hand (fast) rotor. This was accomplished by solving systems of equations that resulted from the patterns determined by the composed permutations AD, BE, and CF.

To see how Rejewski did this, we will closely follow his example [**14e**, p. 281f].

First, recall that Rejewski was able to determine the composed permutations provided that he had enough messages—provided that in the collection of 6-letter indicators each letter occurred at least once in each of the first three positions. Recall that we have determined the composed permutations to be:

AD = (a)(bc)(dvpfkxgzyo)(eijmunqlht)(rw)(s)
BE = (axt)(blfqveoum)(cgy)(d)(hjpswizrn)(k)
CF = (abviktjgfcqny)(duzrehlxwpsmo).

Rejewski wants to factor these permutations into A, B, C, D, E, and F. His description of what he did is terse:

> We assume that thanks to the theorem on the product of permutations, combined with a knowledge of encipherer's habits, we know separately the permutations A through F. [**14e**, p. 282]

A = (as)(br)(cw)(di)(ev)(fh)(gn)(jo)(kl)(my)(pt)(qx)(uz)

B = (ay)(bj)(ct)(dk)(ei)(fn)(gx)(hl)(mp)(ow)(qr)(su)(vz)

C = (ax)(bl)(cm)(dg)(ei)(fo)(hv)(ju)(kr)(np)(qs)(tz)(wy)

D = (as)(bw)(cr)(dj)(ep)(ft)(gq)(hk)(iv)(lx)(mo)(nz)(uy)

E = (ac)(bp)(dk)(ez)(fh)(gt)(io)(jl)(ms)(nq)(rv)(uw)(xy)

F = (aw)(bx)(co)(df)(ek)(gu)(hi)(jz)(lv)(mq)(ns)(py)(rt).

It is easy to see that the factors do not violate any of the theorems, but how did Rejewski factor them?

Let us consider factoring AD = (a)(bc)(dvpfkxgzyo)(eijmunqlht)(rw)(s).

First, consider the two 1-cycles. From Theorem 2, if $(a_1)(a_2)$ in XY, (a_1a_2) appears in X and (a_2a_1) appears in Y.

(a)(s) appears in AD; so, (as) appears in both A and D.

Next, consider the two 2-cycles. From the Theorem 2, if $(a_1a_3)(a_4a_2)$ appears in XY, then $(a_1a_2)(a_3a_4)$ appears in X and $(a_2a_3)(a_4a_1)$ appears in Y.

AD contains two transpositions, and there are two possible orders of the elements within them: (bc)(rw) or (bc)(wr). [Although the order of the elements is not important to writing the permutation as a product of disjoint cycles, it is important to the factoring.]

Therefore, either (br)(cw) appears in A and (rc)(wb) appears in D, or (bw)(cr) appears in A and (wc)(rb) appears in D. There are two possibilities.

Finally, consider the two 10-cycles.

From Theorem 2, if $(a_1a_3a_5\ldots a_{2k-3}a_{2k-1})\,(a_{2k}a_{2k-2}\ldots a_6a_4a_2)$ appears in XY, then $(a_1a_2)\,(a_3a_4)\,(a_5a_6)\ldots(a_{2k-3}a_{2k-2})\,(a_{2k-1}a_{2k})$ appears in X and $(a_2a_3)\,(a_4a_5)\,(a_6a_7)\ldots(a_{2k-2}a_{2k-1})\,(a_{2k}a_1)$ appears in Y.

For (dvpfkxgzyo)(eijmunqlht), there are ten possible orders:

Order number 1:

AD =(dvpfkxgzyo)(eijmunqlht)

A = (dt)(hv)(pl)(fq)(kn)(xu)(gm)(zj)(yi)(oe)

D = (tv)(hp)(lf)(qk)(nx)(ug)(mz)(jy)(io)(ed)

⋮

Order number 3:

AD =(dvpfkxgzyo)(jmunqlhtei)

A = (di)(ve)(pt)(fh)(kl)(xq)(gn)(zu)(ym)(oj)

D = (iv)(ep)(tf)(hk)(lx)(qg)(nz)(uy)(mo)(jd)

⋮

Order number 10:

AD =(dvpfkxgzyo)(teijmunqlh)

A = (dh)(vl)(pq)(fn)(ku)(xm)(gj)(zr)(ye)(ot)

D = (hv)(lp)(qf)(nk)(ux)(mg)(jz)(iy)(eo)(td).

So there are 1 × 2 × 10 = 20 possible factorizations of AD. Here Rejewski gets some help from the Enigma operators.

> . . . it is a well-known phenomenon that man, as a being endowed with consciousness and memory, cannot imitate chance perfectly, and it is the cryptologist's task, among other things, to discover and make proper use of these deviations from chance.
>
> Marian Rejewski [**14d**, p. 254]

Just as our selection of `NKU` for our message setting earlier in this paper was not random, Enigma operators did not usually choose random 3-letter strings for their message settings. Often they used initials, patterns in rows or diagonals of the keyboard, etc. Rejewski was able to exploit his knowledge of the operators' habits to reduce the number of possible factorizations. Eventually he was able to arrive at the factorizations

$$\begin{aligned}
A &= \mathtt{(as)(br)(cw)(di)(ev)(fh)(gn)(jo)(kl)(my)(pt)(qx)(uz)}\\
B &= \mathtt{(ay)(bj)(ct)(dk)(ei)(fn)(gx)(hl)(mp)(ow)(qr)(su)(vz)}\\
C &= \mathtt{(ax)(bl)(cm)(dg)(ei)(fo)(hv)(ju)(kr)(np)(qs)(tz)(wy)}\\
D &= \mathtt{(as)(bw)(cr)(dj)(ep)(ft)(gq)(hk)(iv)(lx)(mo)(nz)(uy)}\\
E &= \mathtt{(ac)(bp)(dk)(ez)(fh)(gt)(io)(jl)(ms)(nq)(rv)(uw)(xy)}\\
F &= \mathtt{(aw)(bx)(co)(df)(ek)(gu)(hi)(jz)(lv)(mq)(ns)(py)(rt)}.
\end{aligned}$$

In terms of the individual permutations of the Enigma circuit, we have

$$\begin{aligned}
A &= SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}S^{-1}\\
B &= SP^2NP^{-2}MLRL^{-1}M^{-1}P^2N^{-1}P^{-2}S^{-1}\\
C &= SP^3NP^{-3}MLRL^{-1}M^{-1}P^3N^{-1}P^{-3}S^{-1}\\
D &= SP^4NP^{-4}MLRL^{-1}M^{-1}P^4N^{-1}P^{-4}S^{-1}\\
E &= SP^5NP^{-5}MLRL^{-1}M^{-1}P^5N^{-1}P^{-5}S^{-1}\\
F &= SP^6NP^{-6}MLRL^{-1}M^{-1}P^6N^{-1}P^{-6}S^{-1}
\end{aligned}$$

where P is the entry permutation and

$$\begin{aligned}
P &= \mathtt{(abcdefghijklmnopqrstuvwxyz)}\\
P^2 &= \mathtt{(acegikmoqsuwy)(bdfhjlnprtvxz)}\\
P^3 &= \mathtt{(adgjmpsvybehknqtwzcfilorux)}\\
P^4 &= \mathtt{(aeimquycgkosw)(bfjnrzvdhlptx)}
\end{aligned}$$

Etc.

Rejewski substitutes $Q = MLRL^{-1}M^{-1}$. This permutation is a factor of each of A, B, C, D, E, and F because Rejewski assumed that no turnover occurred during the double encipherment of the message setting; so, the middle and left-hand rotor are assumed to be fixed.

$$\begin{aligned}
A &= SPNP^{-1}QPN^{-1}P^{-1}S^{-1}\\
B &= SP^2NP^{-2}QP^2N^{-1}P^{-2}S^{-1}\\
C &= SP^3NP^{-3}QP^3N^{-1}P^{-3}S^{-1}\\
D &= SP^4NP^{-4}QP^4N^{-1}P^{-4}S^{-1}\\
E &= SP^5NP^{-5}QP^5N^{-1}P^{-5}S^{-1}\\
F &= SP^6NP^{-6}QP^6N^{-1}P^{-6}S^{-1}
\end{aligned}$$

The unknowns are Q, S, N, and their inverses. Rejewski wants to determine N.

As it turned out, the Polish Cipher Bureau had information that made S, the plugboard permutation, known.

> . . . I had a set of six equations with three unknowns—S, N, and Q. And just as I was wondering how to solve this set, quite unexpectedly on 9 December 1932, at just the right moment, I was given a photocopy of two tables of daily keys for September and October 1932.
>
> Now, the situation had changed radically. Since the key tables also contained the daily changes in the commutator connections, I could now regard S as known and transfer it . . . to the left side of the set . . .
>
> Marian Rejewski [**14d**, p. 256]

The French had purchased the information (along with other information about Enigma) from the German traitor Hans Thilo Schmidt (code name Asché). In 1932, German Enigma procedures called for changing the order of the three rotors once per quarter. Because September is in one quarter of the year and October is in the next, the information from Schmidt provided the plugboard connections when two different rotors were in the right-hand rotor location.

Kahn [**13**, p. 66] claims that " . . . the Poles had a stroke of luck. The Germans changed the rotors every three months, or quarter of a year. Fortunately, the keys that Schmidt had supplied straddled two different quarters." And, Budiansky [**3**, p. 102] echoes and strengthens Kahn's statement: " . . . if it were not for the changes in the rotor order, Rejewski would have hit another impasse . . . ." Lawrence [**18**] suggests that even if Rejewski only had received data for one rotor order he still would have been able to determine the Enigma wiring. In [**19**], Lawrence considers whether Rejewski needed the information obtained from Asché to solve his six equations and obtain the wiring of the rotors. But, through Asché, information about S was available to Rejewski for two different quarters, and he did use it to determine the wiring of two Enigma rotors.

> Also known, thanks to materials obtained by intelligence, are the plug connections S for the given day:
>
> $$S = \texttt{(ap)(bl)(cz)(fh)(jk)(qu)}.$$
>
> Marian Rejewski [**14e**, p. 282]

So, the remaining unknowns are Q and N.

Rejewski transfers S to the left side of each of the six equations.

$$\begin{aligned}
&S^{-1}AS = PNP^{-1}QPN^{-1}P^{-1}\\
&S^{-1}BS = P^2NP^{-2}QP^2N^{-1}P^{-2}\\
&S^{-1}CS = P^3NP^{-3}QP^3N^{-1}P^{-3}\\
&S^{-1}DS = P^4NP^{-4}QP^4N^{-1}P^{-4}\\
&S^{-1}ES = P^5NP^{-5}QP^5N^{-1}P^{-5}\\
&S^{-1}FS = P^6NP^{-6}QP^6N^{-1}P^{-6}
\end{aligned}$$

Then, because he also knows P, he transfers it to the other side of each equation.

$$\begin{aligned}
U &= P^{-1}S^{-1}ASP &&= NP^{-1}QPN^{-1}\\
V &= P^{-2}S^{-1}BSP^2 &&= NP^{-2}QP^2N^{-1}\\
W &= P^{-3}S^{-1}CSP^3 &&= NP^{-3}QP^3N^{-1}\\
X &= P^{-4}S^{-1}DSP^4 &&= NP^{-4}QP^4N^{-1}\\
Y &= P^{-5}S^{-1}ESP^5 &&= NP^{-5}QP^5N^{-1}\\
Z &= P^{-6}S^{-1}FSP^6 &&= NP^{-6}QP^6N^{-1}
\end{aligned}$$

Actually, Rejewski needs only the first four of these. He substitutes for S, the various powers of P, and A, B, C, and D and determines U, V, W, and X.

$$\begin{aligned}
&\mathrm{U} = \texttt{(ax)(bu)(ck)(dr)(ej)(fw)(gi)(lp)(ms)(nz)(oh)(qt)(vy)}\\
&\mathrm{V} = \texttt{(ar)(bv)(co)(dh)(fl)(gk)(iz)(jp)(mn)(qy)(su)(tw)(xe)}\\
&\mathrm{W} = \texttt{(as)(bz)(cp)(dq)(eo)(fw)(gj)(hl)(iy)(kr)(mu)(nt)(vx)}\\
&\mathrm{X} = \texttt{(ap)(bf)(cu)(dv)(ei)(gr)(ho)(jn)(ky)(lx)(mz)(qs)(tw)}
\end{aligned}$$

Next, Rejewski forms products.

$$\begin{aligned}
&\mathrm{UV} = (\mathrm{NP}^{-1}\mathrm{QPN}^{-1})(\mathrm{NP}^{-2}\mathrm{QP}^{2}\mathrm{N}^{-1}) = \mathrm{NP}^{-1}(\mathrm{QP}^{-1}\mathrm{QP})\mathrm{PN}^{-1}\\
&\mathrm{VW} = \mathrm{NP}^{-2}(\mathrm{QP}^{-1}\mathrm{QP})\mathrm{P}^{2}\mathrm{N}^{-1}\\
&\mathrm{WX} = \mathrm{NP}^{-3}(\mathrm{QP}^{-1}\mathrm{QP})\mathrm{P}^{3}\mathrm{N}^{-1}
\end{aligned}$$

Rejewski notes that (because each is a conjugate of $\mathrm{QP}^{-1}\mathrm{QP}$) “the products have the same configuration of cycles, which is as it should be.” [**14e**, p. 282]

$$\begin{aligned}
&\mathrm{UV} = \texttt{(aepftybsnikod)(rhcgzmuvqwljx)}\\
&\mathrm{VW} = \texttt{(akjcevzydlwnu)(smtfhqibxopgr)}\\
&\mathrm{WX} = \texttt{(aqvloikgnwbmc)(puzftjryehxds)}
\end{aligned}$$

He then eliminates the common expression $\mathrm{QP}^{-1}\mathrm{QP}$ between UV and VW

$$\begin{aligned}
\mathrm{VW} &= \mathrm{NP}^{-2}(\mathrm{QP}^{-1}\mathrm{QP})\mathrm{P}^{2}\mathrm{N}^{-1}\\
&= \mathrm{NP}^{-1}\mathrm{N}^{-1}(\mathrm{NP}^{-1}(\mathrm{QP}^{-1}\mathrm{QP})\mathrm{PN}^{-1})\mathrm{NPN}^{-1}\\
&= \mathrm{NP}^{-1}\mathrm{N}^{-1}(\mathrm{UV})\mathrm{NPN}^{-1}\\
&= (\mathrm{NPN}^{-1})^{-1}(\mathrm{UV})(\mathrm{NPN}^{-1})
\end{aligned}$$

and similarly between VW and WX.

$$\mathrm{WX} =(\mathrm{NPN}^{-1})^{-1}(\mathrm{VW})(\mathrm{NPN}^{-1})$$

Because $\mathrm{VW} = (\mathrm{NPN}^{-1})^{-1}(\mathrm{UV})(\mathrm{NPN}^{-1})$, Theorem 5 can be used to find several possibilities for NPN^{-1}. Similarly, because $\mathrm{WX} =(\mathrm{NPN}^{-1})^{-1}(\mathrm{VW})(\mathrm{NPN}^{-1})$, Theorem 5 can be used to find possibilities for NPN^{-1}.

> We should ... write VW beneath product UV in every possible way, and likewise, product WX beneath product VW. Of all these possible ways, one will give the same result in both cases. This will be the expression that we need. Writing VW beneath UV, and WX beneath VW, in every possible way is rather tedious. However, there are various tricks and technical means that make this subscription unnecessary, but whose description and, especially, justification would take us too far afield. It will suffice to say that products UV, VW, and WX should be subscribed in the following way:
>
> $$\begin{aligned}\mathrm{UV} &= \texttt{(aepftybsnikod)(rhcgzmuvqwljx)}\\ \mathrm{VW} &= \texttt{(ydlwnuakjcevz)(ibxopgrsmtfhq)}\end{aligned}$$
>
> $$\begin{aligned}\mathrm{VW} &= \texttt{(ydlwnuakjcevz)(ibxopgrsmtfhq)}\\ \mathrm{WX} &= \texttt{(uzftjryehxdsp)(caqvloikgnwbm)}\end{aligned}$$
>
> For, in both cases, we obtain for NPN^{-1} the same expression:
>
> $$\mathrm{NPN}^{-1} = \texttt{(ayuricxqmgovskedzplfwtnjhb)}$$
>
> Marian Rejewski [**14e**, pp. 282 & 283]

To find N, Rejewski uses Theorem 5 again.

> Subscribing beneath permutation NPN^{-1} permutation P in all possible ways, of which there are twenty-six, we will obtain [using Theorem 5] twenty-six variants of the permutation N. For example, one variant is [**14e**, p. 283]:
>
> $$\mathrm{NPN}^{-1} = (\texttt{ayuricxqmgovskedzplfwtnjhb})$$
> $$\mathrm{P} = \mathrm{N}^{-1}(\mathrm{NPN}^{-1})\mathrm{N} = (\texttt{abcdefghijklmnopqrstuvwxyz})$$
>
> For this variant, after the upper row has been placed in alphabetical order, we obtain:
>
> $$\mathrm{N} = \begin{pmatrix}\texttt{abcdefghijklmnopqrstuvwxyz}\\ \texttt{azfpotjyexnsiwkrhdmvclugbq}\end{pmatrix}$$

The Polish Doubles

After only a month of continuous and highly concentrated effort, [Rejewski] had worked out the electrical connections of the three wheels that were used at that time in the German Enigma. He was able to have a replica of the machine constructed.

Gordon Welchman [**27**, p. 15]

By December, 1932, Rejewski knew the wiring of the Enigma rotors and was able to determine the settings based upon the double encipherment of the message indicators. By the middle of January, 1933, the Poles were able to read Enigma messages.

> In 1938, the situation was aggravated. The Germans changed the encryption procedure on January 15, and introduced on December 15 a fourth and a fifth rotor, which now gave 60 instead of the previous 6 possible rotor orders.
>
> The Poles had to find out the wiring of the new rotors quickly, and they were lucky. Among the traffic they regularly decrypted were signals from the S.D. (*Sicherheitsdienst*), the intelligence service of the Nazi Party. The S.D. did not change their encryption procedure, but introduced the new rotors in December 1938. These rotors came from time to time into the position of the fast rotor and their wiring would be reconstructed the same as previously with the first three rotors. [**2**, p. 395]

Soon the Poles had several Enigma "doubles" built.

Fearing that war would begin soon, the Poles met, on July 24 and 25, 1939, with British and French cryptologists in the B.S.-4 facility in Kabackie Woods outside Warsaw.[7] It was at this meeting that the Poles revealed the extent of their abilities to read Enigma and told the French and British that each would receive a Polish-made Enigma double.

One of the Polish Enigma doubles is now on display in the Sikorski Polish Museum in London. (See Figure 7, p. 269.) The Enigma plugboard is not visible behind the lampboard. This is a 3-rotor Enigma, but the machine had five rotors from which the three in use were chosen. The two rotors on the right are in storage; the three rotors on the left are installed.

At the beginning of September, 1939, Poland was attacked by Germany.

[7] A photograph of the site as it now exists may be found in [**11**].

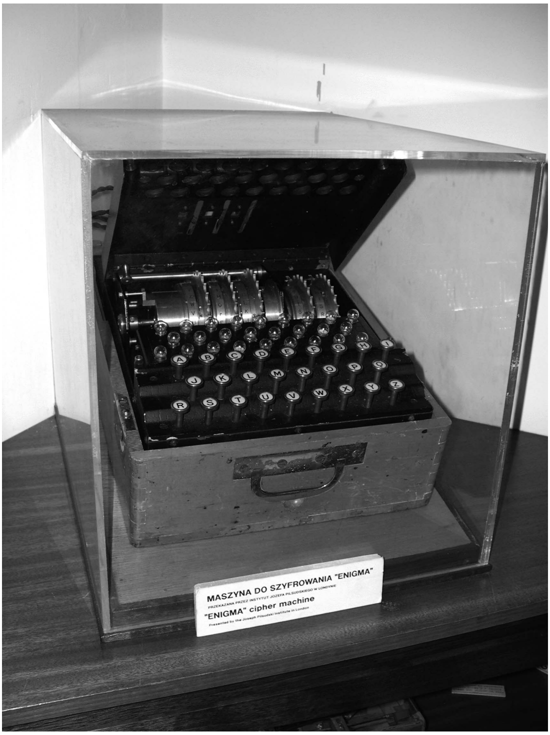
MASZYNA DO SZYFROWANIA "ENIGMA"
PRZEKAZANA PRZEZ INSTYTUT JOZEFA PILSUDSKIEGO W LONDYNIE
"ENIGMA" cipher machine
Presented by the Joseph Pilsudski Institute in London

Figure 7 Polish Enigma Double

What Happened to the Polish Mathematicians?

> *Mathematicians are often thought of as being rather remote individuals, indulging in activities which have little or no relevance to real life.*
>
> Frank Carter [**4**, p. 4]

On September 5, 1939, B.S.-4 was told to evacuate Warsaw on a special train. The Polish mathematicians crossed the border into Romania, traveled through Italy, and eventually crossed the border into France. On October 20, 1939, the Polish mathematicians, from a site not far from Paris, resumed their attack on the German ciphers. On June 22, 1940, French Premier Pétain signed an armistice which divided France; on June 24 the Poles were flown to North Africa. In Algiers, they took on new identities and returned to France to resume signal intelligence in Vichy France. They operated from a site near the town of Uzès near the Mediterranean coast. The Poles occasionally spent two- or three-month periods at the North African station, and on January 9, 1942, Różycki died when the French ship *Lamoricière* carrying him and other staff back to France from Algeria was sunk.

Just prior to the German occupation of the free zone of France, Rejewski and Zygalski fled to the Italian zone, then back to France, and "on the night of 29 January 1943, . . . set out with [a] smuggler for the [Spanish] border." [**14**, p. 150] On the trip, the smuggler demanded from them at gunpoint more money for the trip. Upon arriving in neutral (but sympathetic to Germany) Spain, the Poles were arrested. Upon their release they made their way to Madrid.

Near the end of July, they made their way to Portugal and were taken by boat to a British naval vessel waiting off the coast.

For the remainder of the war, Rejewski and Zygalski worked at a Polish Signals Battalion in Boxmoor near London. The British codebreakers at Bletchley Park were now routinely breaking Enigma; the Poles worked on German S.S. and S.D. ciphers.

Stuart Milner-Barry, who was playing chess for the British team in Argentina when war broke out, became a codebreaker and later became director of Hut 6 (German Army and Air Force cryptanalysis); he speculates about why the Polish codebreakers were not invited to Bletchley Park.

> It was always a mystery to me that the Polish contingent was not incorporated at Bletchley during the war, where they would no doubt have made an invaluable contribution; but in fact they were side-tracked in France and had to be evacuated when the Germans overran the whole of the country. I can only assume there were security doubts, and I believe the Poles continued to operate their own organization, but I feel there must have been a sad waste of resources somewhere.
>
> Stuart Milner-Barry [**9**, pp. 92 & 93]

After the war, Rejewski returned to Poland in November, 1946.

> ... for reasons of practical and family nature, it proved difficult for Rejewski to find employment as a mathematician at an institution of higher learning, and, in the early postwar period, he felt it imprudent to apply for a job in cryptology .... for 20 years [Rejewski] worked in the administrations of various concerns in Bydgoszcz, and in February 1967 retired [**14**, p. 224].

Rejewski died in 1980.

Henryk Zygalski remained in England after the war and taught in London. He died in 1978.

Bletchley Park is now a museum that honors the work of the British codebreakers. Outside the Bletchley Park cottage in which the British codebreakers made their first break into Enigma is a tablet that honors the work of the Polish codebreakers. A copy of that tablet has been placed on the west wall of the former Ministry of War office in Pilsudski Square in Warsaw where the Polish codebreakers worked.

> *This plaque commemorates the work of Marian Rejewski, Jerzy Różycki, and Henryk Zygalski, mathematicians of the Polish intelligence service, in first breaking the Enigma code. Their work greatly assisted the Bletchley Park code breakers and contributed to the allied victory in World War II.*[8]

For further study. Beginning with the publication of *The Ultra Secret* in 1974 [**29**], some information about Enigma has become public. Although other information is still classified, there are many websites and papers and books about Enigma. Here are some to use for further study.

There are many Enigma websites; some include virtual Enigma machines. Two sites to start with are the official website of Bletchley Park:

`http://www.bletchleypark.org.uk/`

and Tony Sale's World War II Codes and Ciphers:

`http://www.codesandciphers.org.uk/`

[8] The English version of the statement on the tablet honoring the Polish codebreakers at Bletchley Park.

The National Security Agency's website:

http://www.nsa.gov/history/histo00007.cfm

contains downloadable publications about cryptological history including Enigma.

Wikipedia is also an excellent reference for cryptological topics.

There are also many books. The standard reference for cryptological history is *The Codebreakers* by David Kahn [**12**].

When Kahn's book appeared in 1967, Enigma was unknown to the public. The revised and updated book published in 1997 contains some material about Enigma, but his *Seizing The Enigma: The race to break the German U-boat codes 1939–1943* [**13**], which was published in 1991, is a more complete history of Enigma.

Simon Singh's *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptograph* [**25**] has prompted some popular interest in cryptology, but should be read or used with some caution (see, for example [**21**]).

Two good readable recent histories of World War II codebreaking are *Enigma: The Battle for the Code* by Hugh Sebag-Montefiore [**24**] and *Battle of Wits: The complete story of codebreaking in World War II* by Stephen Budiansky [**3**].

The history of the Polish codebreakers is written in *Enigma: How the German Machine Cipher Was Broken, and How it was Read by the Allies in World War Two* by Wladyslaw Kozaczuk (translated by Christopher Kasparek) [**14**] and also in *Enigma: How the Poles Broke the Nazi Code* [**15**].

The Hut Six Story by Gordon Welchman [**27**] and *Codebreakers: The Inside Story of Bletchley Park* edited by F.H. Hinsley and Alan Stripp [**9**] are good starting points for understanding the work of the British codebreakers at Bletchley Park.

Two mathematical papers by Rejewski about the solution of Enigma ([14d] and [14e]) appear as appendices to [14]. They are also available on several internet sites.[9] Similar results appear in Rejewski's paper *An Application of the Theory of Permutations in Breaking the Enigma* [**22**]. This paper is also available on several internet sites.

Frank Carter, a mathematician who is now a Bletchley Park volunteer, has written several papers describing the mathematics used by the World War II cryptanalysts. His papers are available as either Bletchley Park Trust reports or on the Bletchley Park website. In particular, two of his papers [**4**] and the technical report "The Polish recovery of the Enigma Rotor wiring" (which is available on the Bletchley Park website and appeared just after this paper was written) discuss the mathematical work of Rejewski.

A complete coverage of cryptology from a mathematician's viewpoint is contained in *Decrypted Secrets: Methods and Maxims of Cryptology* by F.L. Bauer [**2**]. It is hoped that this paper's gentle introduction would encourage readers to examine Bauer's excellent book.

Cryptologia is a quarterly journal devoted to all aspects of cryptology. The journal began publishing in 1977, and its back issues contain many articles about the history and mathematics of Enigma. *Cryptologia* is published by the Taylor & Francis Group.

Mathematicians Did Not Win the War

> *Polish penetration into the secrets of the Enigma began in earnest when Rejewski realized the application of a simple property of permutations—namely, that if G and P are permutations, then the permutation defined by PGP^{-1} has the same*

[9] The paper that is Appendix E also appears in *Cryptologia*, **VI**, number 1, (January 1989), 1–18; and in Cipher Deavours; David Kahn; Louis Kruh; Gregg Mellen; and Brian Winkel; editors, 1989, *Cryptology: Machines, History, & Methods*, Artech House, Boston, 1989, pp. 310–327.

> *cycle structure as the permutation G. No doubt practitioners of group theory should introduce this property of permutations to students as "the theorem that won World War II."* Cipher A. Deavours [**5**, pp. 229 & 232].

To paraphrase many others, no theorem won the war. The war was won by those who served in the various Allied military services, but the information gleaned from Enigma helped the Allies win the war, and the breaking of Enigma began with Polish mathematicians who found patterns in Enigma messages.

Acknowledgments. I thank Northern Kentucky University student Dan Meredith for creating the illustrations and enhancing the photographs for this article. Dman41786@yahoo.com

This paper results from two talks given by the author. One talk was presented at the Pi Mu Epsilon initiation ceremony at Austin Peay State University, December, 2004, and the other was presented at the Mathematical Association of America, Kentucky Section, Spring 2005.

REFERENCES

1. A.A. Albert, Some Mathematical Aspects of Cryptography (address to the AMS on November 22, 1941), *A. A. Albert Collected Mathematical Papers*, AMS, 1993, pp. 903–920.
2. F.L Bauer, *Decrypted Secrets: Methods and Maxims of Cryptology, Second Edition*, Springer-Verlag, Berlin, 2000.
3. Stephen Budiansky, *Battle of Wits: The complete story of codebreaking in World War II*, The Free Press, New York, 2000.
4. Frank Carter, The first breaking of Enigma: Some of the pioneering techniques developed by the Polish Cipher Bureau, *The Bletchley Park Trust Reports*, number 10, 1999.
5. Cipher A. Deavours, Afterward to How Polish Mathematicians Deciphered the Enigma by Marian Rejewski, *Annals of the History of Computing*, **3**, Number 3, (July 1981), 229–232.
6. David Hamer, Enigma: Actions Involved in the "Double-Stepping" of the Middle Rotor, *Cryptologia*, **XXI**, number 1 (January 1997), 47–50.
7. Robert Harris, *Enigma*, Ballatine Books, New York, 1995.
8. Peter Hilton, Enigma, *Notices of the American Mathematical Society*, **43**, number 6, (June 1996), 681–682.
9. F.H. Hinsley and Alan Stripp, editors, *Codebreakers: The Inside Story of Bletchley Park*, Oxford University Press, Oxford, 1994.
10. Andrew Hodges, *Alan Turing: The Enigma*, Vintage, London, 1992.
11. David Kahn, The Polish Enigma Conference and Some Excursions, *Cryptologia*, **XXIX**, number 2 (April 2005), 121–126.
12. David Kahn, *The Codebreakers: The story of secret writing, revised and updated*, Scribner, New York, 1996.
13. David Kahn, *Seizing the Enigma: The race to break the German U-boat codes 1939–1943*, Barnes and Noble, New York, 1991.
14. Wladyslaw Kozaczuk, *Enigma: How the German machine cipher was broken, and how it was read by the Allies in World War Two*, translated by Christopher Kasparek, University Publications of America, 1984. [14b] Appendix B, A conversation with Marian Rejewski by Richard Woytak. [14d] Appendix D, How the Polish mathematicians broke Enigma by Marian Rejewski. [14e] Appendix E, The mathematical solution of the Engima cipher by Marian Rejewski.
15. Wladyslaw Kozaczuk and Jerzy Straszak, *Enigma: How the Poles Broke the Nazi Code*, Hippocrene Books, New York, 2004.
16. Alex Kuhl, Rejewski's Catalog, *Cryptologia*, to appear.
17. Solomon Kullback, *Statistical Methods in Cryptanalysis*, Aegean Park Press, Walnut Creek, CA, 1976.
18. John Lawrence, The versatility of Rejewski's method: Solving for the wiring of the second rotor, *Cryptologia*, **XXVIII**, number 2 (April 2004), 149–152.
19. John Lawrence, A Study of Rejewski's Equations, *Cryptologia*, **XXIX**, number 3 (July 2005), 233–247.
20. John Lawrence, Factoring for the Plugboard—Was Rejewski's Proposed Solution for Breaking the Enigma Feasible?, *Cryptologia*, **XXVIX**, number 4 (October 2005), 343–366.
21. Jim Reeds, Review of The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography, *Notices of the American Mathematical Society*, **47**, number 3, (March 2000), 369–372.
22. M. Rejewski, An Application of the Theory of Permutations in Breaking the Enigma Cipher, *Applicaciones Mathematicae* **16**, number 4, (1980), 543–559.
23. Frank Rowlett, *The Story of Magic: Memoirs of an American cryptologic pioneer*, Aegean Park Press, Walnut Creek, CA, 1998.

24. Hugh Sebag-Montefiore, *Enigma: The Battle for the Code*, Phoenix, London, 2000.
25. Simon Singh, *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography*, Doubleday, New York, 1999.
26. Abraham Sinkov, *Elementary Cryptanalysis: A mathematical approach*, Mathematical Association of America, 1968.
27. Gordon Welchman, *The Hut 6 Story*, M and M Baldwin, Cleobury Mortimer, Shropshire, England, 1998.
28. Brian J. Winkel, Cipher A. Deavours, David Kahn, Louis Kruh, editors, *The German Enigma Machine: Beginnings, Success, and Ultimate Failure*, Artech House, Boston, 2005.
29. F.W. Winterbotham, *The Ultra Secret*, Dell, New York, 1974.

Why Richard Cory[1] Offed Himself or One Reason to Take a Course in Probability

A hypochondriac at heart, he thought
(Though symptom free) he had a dire disease,
And after fruitless weeks of worry, sought
Some test to take to set his mind at ease.

He forthwith found one that would do the trick,
And accurate (at oh point nine) to tell
Those having the disease that they were sick,
And just the same, the well that they were well.

One crucial point he failed to note was this:
That of a hundred like him, only one
Had the disease, and this slip made him miss
The implication when the test was done

And positive! Therefore, consumed with dread,
And now convinced his blackest fears were right
(By faulty logic fatally misled[2]),
He shattered silence that calm summer night.

J. D. Memory
Professor of Physics, Emeritus
North Carolina State University
jmemory@nc.rr.com

[1] "Richard Cory" is a frequently anthologized poem by E. A. Robinson

[2] An example of the False Positive Fallacy: On average, of 1000 Corys, ten would have the disease, yielding nine true positives and one false negative. Of the remaining 990, there would be 99 false positives and 891 true negatives. The false positives outnumber the true positives by a factor of eleven. So if D denotes having the disease and P denotes testing positive, we learn from the poem that $\Pr(P \mid D) = 0.9$, whereas $\Pr(D \mid P) = 9/108$, or about 0.083. Richard Cory shot himself "that calm summer night," because he confused $\Pr(P \mid D)$ with $\Pr(D \mid P)$.