The Enigma
History and Mathematics

by

Stephanie Faint

A thesis

presented to the University of Waterloo

in fulfilment of the

thesis requirement for the degree of

Master of Mathematics

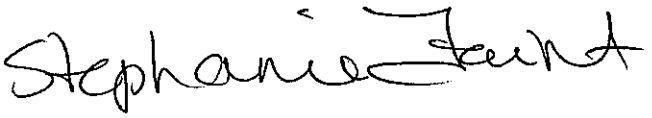
in

Pure Mathematics

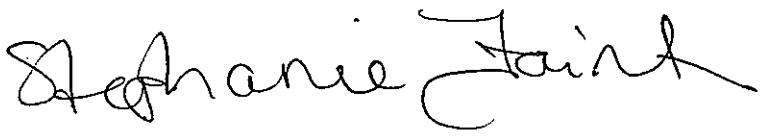
Waterloo, Ontario, Canada, 1999

I hereby declare that I am the sole author of this thesis.

I authorize the University of Waterloo to lend this thesis to other institutions or individuals for the purpose of scholarly research.



I further authorize the University of Waterloo to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.



The University of Waterloo requires the signatures of all persons using or photocopying this thesis. Please sign below, and give address and date.

Abstract

In this thesis we look at the solution to the German code machine, the Enigma machine. This solution was originally found by Polish cryptologists. We look at the solution from a historical perspective, but most importantly, from a mathematical point of view. Although there are no complete records of the Polish solution, we try to reconstruct what was done, sometimes filling in blanks, and sometimes finding a more mathematical way than was originally found. We also look at whether the solution would have been possible without the help of information obtained from a German spy.

Acknowledgements

I would like to thank all of the people who helped me write this thesis, and who encouraged me to keep going with it. In particular, I would like to thank my friends and fellow grad students for their support, especially Nico Spronk and Philippe Larocque for their help with latex. I would also like to thank Kathryn Hare for being so supportive, and always believing in me. Finally, I would like to thank my supervisor, John Lawrence, for not pushing, and for having the patience to let me work at my own pace.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

The Enigma Machine was a German code machine from World War II. It was used by all sections of the German military, in sometimes differing forms, both before and during the war. The Germans believed that it was completely unbreakable, and though they sometimes changed the setup of the machine to foil any such attempt, they never really thought that anyone could do it.

The Polish cryptographers who solved the Enigma machine code were some of the first cryptographers who were mathematicians, not just able to work with languages. They, among others, were chosen to take a class at their university in Poznań, and eventually they became the core of Poland's decryptment team. Their skills with math enabled them to solve the Enigma using Algebra, mostly Group Theory.

One of the biggest controversies surrounding this issue is whether the solution of the Enigma code would have been possible without the help of a German spy. He supplied the French, and through them, the Poles, with information that was

critical in the solution of the Enigma. What remains a mystery is if another method could have been found to decrypt the code, and whether it would have been found in time, particularly without the computing tools of today.

Chapter 2

The History

2.1 Before The Enigma

It all started in January 1929, when Professor Zdzisław Krygowski of the Mathematics Institute of Poland's Poznań University chose a group of third and fourth year students to be given the chance to participate in a cryptology course. The students were chosen based on their academic record, and their ability to speak German. The course was organized by two members of the Polish General Staff in Warsaw, Major Franciszek Pokorny and Lieutenant Maksymilian Ciężki, and conducted by Cipher Bureau cryptologists from Warsaw. About twenty students decided to take the class, held in the evenings, twice a week, and were consequently sworn to secrecy. [5, page 1]

The class was started because of the need for more cryptologists in Poland. The Polish believed (correctly) that the German army was about to be greatly expanded.

The Germans were also advertising that they "[intended] to take away from Poland the 'lost territories' in the east: Pomerania, western Poland, Upper Silesia". [5, page 2] In order to keep up with military developments, it was necessary to monitor German military radio stations, and to decrypt the messages collected from this venture. Unfortunately, there were only about five people in Poland at the time who specialized in cryptology, and thus much of the radio traffic was going undeciphered. Thus many more trained specialists were needed.

Poznań was chosen as the location for the class because of the students. They were mostly from western Poland and had, because of the recent occupations by Prussia and Germany of that area, attended German-language schools. This, combined with their knowledge of Mathematics, made them ideal candidates to increase the number of cryptologists.

The course included not only instruction, but also real-life examples, which became more difficult as the course progressed. These were used to test the students, to see if they were capable of learning this kind of applied, high pressure mathematics. Many found that they were not, and dropped the course either because they didn't have the talent or the ability for learning the material, and others because they couldn't keep up with the pace of the course. Among the few who were able to stay with the course were Marian Rejewski, Henryk Zygalski, and Jerzy Różycki. These three were to later form the basis for the Polish contributions to the solution of the Enigma.

Between 1929 and 1930, the three students had gone their separate ways, but in

the fall of 1930 they were all working for the Cipher Bureau in an underground laboratory in Poznań. It had been organized so that students could keep up with their classes, but still spend their free time deciphering intercepted German radiograms. They were not only able to work at any time of the day or night, but also the lab was "literally but a few paces" [5, page 6] from the Mathematics Institute. They were also given total seclusion and security, with passes being required at the entrance.

The goal of this lab was not to do the deciphering itself, but to "[work] out methods of breaking the German cipher keys." [5, page 6] The codes at first were relatively straightforward to solve, but eventually became extremely difficult, unlike anything they had seen before. These difficult codes were later known to be the work of the Enigma machine. When attempting to break the codes, they, in addition to using the usual mathematical methods, "[exploited] mistakes made by the German cipher clerks". [5, page 6] These included the padding out of short messages with the letter X in order to make fifty letters [5, page 6], and later, for the Enigma codes, the use of repeated letters, letters physically consecutive on the German typewriter keyboard, and letters located consecutively in the alphabet as message keys [1, pages 17 - 18](see Section 4.2).

In the summer of 1932, the Cipher Bureau branch at Poznań was closed, and the students, now specialists, currently working there were moved to the main Cipher Bureau branch in Warsaw, where they continued working on the non-Enigma codes. The core of this team was Rejewski, Zygalski, and Różycki. They each had diverse characteristics which contributed to their eventual successes: Marian Rejewski's

penetrating mind and skill in formulating questions and advancing far-reaching hypotheses from scarce information were supported by the precision, energy, and perseverance of Henryk Zygalski, while Jerzy Różycki contributed elements of vivid imagination and intuition. [5, page 9]

These traits, along with their training and experience, enabled them, with some external assistance, to do what no other group would be able to do for some years: solve the Enigma code.

2.2 The Enigma In Poland

The Enigma Machine first went into service with the German army on July 15, 1928. [4, page 41] Because the codes seemed more like gibberish than encrypted communications, the Poles at first thought that they were broadcast only to confuse and waste the time of the people monitoring and attempting to decrypt the German radio traffic. [5, page 6] As these new codes became more and more frequent, eventually almost replacing all other codes, this possibility grew increasingly unlikely.

The Enigma codes were different from those encountered previously in that the distribution of letters appeared to be too regular, and there were no repetitions of groupings of letters. Because of this, "the usual statistical and linguistic methods would be useless." [5, page 12] Thus, a new technique for code breaking had to be developed.

This task fell at first to Rejewski. In the winter of 1932, he was asked to work on

his own, in the afternoons when the others of his group would not be around, on the Enigma code. His first important discovery was that it was a machine code. The second was the significance of the first six letters of any message. This led to the first step in solving the Enigma: finding the message key.

Once these first discoveries were made, Rejewski was supplied with a commercial Enigma machine. This machine was not identical to the military one, but had enough similarities, such as the reversing drum, that it gave Rejewski a feel for what he was trying to do. He was also required to extend his time working on the Enigma from just two hours in the afternoon to seven hours, and he was given a separate room for this work. [5, page 233]

At this point, Rejewski's work, now with algebraic equations involving several unknowns, came to a halt. He found that without further information, it would be very difficult to continue. Fortuitously, help came at just the right time.

2.3 The Spy

Thought by many, but not all, to be the biggest single break in the solution of the Enigma, was the intelligence supplied by a German working in the Reichswehr's Cryptographic Agency. In October 1932, the man contacted a French intelligence officer and offered information in exchange for payment. At first it was thought that this man was an impostor, but upon receiving some of the proffered documentation, and verifying its authenticity, they realized that they had a genuine source of much needed data. This "newly recruited agent received the pseudonym 'Asche'", [5,

page 17] and supplied important documentation on both the Enigma code, and others currently in use by the Germans.

At this same time, the chief of French radio intelligence, Captain Gustave Bertrand, decided that "of the possible allies, the Poles had the best chance of success" [5, page 16] in the matter of the Enigma. Because of this, the information on the Enigma obtained by Asche was shared with the Poles. The first meeting between the two took place from December 7th to 11th in Warsaw. At the meeting, Bertrand, and his equivalent in the Polish Cipher Bureau, Major Gwido Langer, decided to distribute the tasks necessary to break the Enigma.

> The French were to concentrate on furnishing intelligence from Germany that might facilitate the breaking of the machine cipher, [and] the Poles on the theoretical studies of Enigma intercepts. Procedures were set up for exchange of German radio intercepts, radiogoniometric data, and other intelligence. It was also decided to establish closer ties with the corresponding unit of the Czechoslovak General Staff, thereby creating a triple entente of cryptological services. [5, pages 18 - 19]

Thus, the cooperative efforts that eventually allowed the solution to the Enigma to be used in practice, and to affect the war effort, were begun.

The documents received from Asche and passed on to the Poles included "operating instructions for the cipher machine, keying instructions and obsolete tables of daily keys for September and October 1932" [5, page 19] although other documents may have been passed on as well. These documents, especially the tables of daily keys, were pivotal in Rejewski's solution of the Enigma (see Section 4.3.2) although may not have actually been necessary (see Chapter 5). The operating instructions also helped, by alerting the Poles to the existence of the plugboard.

It is evident that the information Asche provided was very helpful to Marian Rejewski in his solution of the Enigma. What remains to be shown is whether this information was completely necessary: that is, could the Enigma have been solved without it, and if so, could it have been solved as quickly? This issue will be addressed in Chapter 5.

2.4 The Breakthrough

Once the information for the spy was utilized, the final step in the solution of the Enigma was not long to come. The chief breakthrough came in the final days of December 1932. The practical reading of messages began during the second ten days of January. Success, once again, could not have been more timely. Just under way in Germany was the Nazi campaign that on the thirtieth of January 1933 would deliver power into Hitler's hands. Neither the French, nor the British, as it later turned out, despite their long-standing traditions of black chambers with experienced cryptological teams and large financial outlays, managed to solve the German cipher system. [5, page 21]

By the end of 1932, Rejewski had almost succeeded in solving the Enigma, and actually had a solution that he believed to be correct, until an application of it proved that there must be an error. Until this time, he had been assuming that the entry drum was the same as that in the commercial Enigma machine, that "the letters of the alphabet were represented on the circumference of the entry [drum] in the same order in which they appeared on a German typewriter keyboard" [5, page

20]. Since this was the only unfounded assumption made to this point, it must be the mistake, and thus another assumption must be made. Rejewski's wild guess, that the letters were in alphabetical order on the entry drum, turned out to be correct, and thus they were able to read the Enigma code.

2.5 Mechanizing the Process

After the final breakthrough, other steps could be taken to facilitate the reading of coded messages. These included the building of doubles of the military Enigma, and the invention of several devices: the cyclometer, the clock, the bomb, and some special perforated sheets.

Marian Rejewski contributed the cyclometer, which "enabled the cryptologist to set up a catalogue of possible settings of the rotors" which "gave much faster recovery of the [daily] keys." [5, page 29] The clock, a device "which made it possible in certain cases to determine which rotor was at the far right side on a given day in a given Enigma net" [5, page 29], was from Jerzy Różycki. In 1938, the bomb was invented by all three Polish cryptologists. It was a device made from six Enigmas, and could find, within two hours, the daily keys, with almost no effort, after initial startup, from the cryptologists. At the same time, the final invention, almost completely that of Henryk Zygalski, was "a special series of [twenty-six] perforated paper sheets with a capacity of fifty-one holes by fifty-one" was used to "[break] the doubly enciphered individual message keys" [5, page 54].

2.6 Leaving Poland

On the first of September, 1939, the invasion of Poland by the Germans began. By the fifth, Poland's situation had deteriorated so much that the Cipher Bureau was ordered to destroy some files, pack up the apparatus and remaining files, and load the material and themselves on a train headed to Warsaw's Wilno Station, where they would then get on a train headed to Brześć, the new location of the supreme headquarters. Once they reached that destination, a new one was proposed, and Bureau personnel now headed south, by truck, after convincing the stage master that "the heavy green crates [containing important decryption equipment that could not fall into enemy hands] were more important than the luggage of civilian dignitaries" [5, page 71]. Along the way, their evacuation orders became more specific, and they headed for Rumania. On September 17th, the cryptologists and other personnel, with the one truck and the little equipment that remained after lack of fuel had gradually whittled down the number of vehicles that could keep moving, crossed into Rumania.

At this point, military and civilian personnel were sent in different directions. Rejewski, Różycki, and Zygalski, fearing that they could be identified by German informers in the camp they were being sent to, ignored their orders. They headed past the camp, and straight to a railroad station, where they purchased tickets, and headed south as quickly as possible, this time to Bucharest. There, the war was much less evident, and they were able to contact the military attaché at the Polish Embassy. While military personnel and government dignitaries were much more important than three apparent civilians, the attaché found time to speak with

them, and suggested that they go to the French or British Embassy.

The three cryptologists first went to the British Embassy, but when they were told they would have to wait, tried the French. As soon as they explained why they were there, and mentioned the name "Bolek", the pseudonym of the French radio-intelligence chief Gustave Bertrand, Paris was contacted and the staff of the Embassy was instructed "to assist the Polish cryptologists in leaving at once for France." [5, page 73] Bertrand had been waiting to contact the Poles since their departure from Warsaw. In less than two days, the cryptologists were supplied passports, transit visas, and were on their way to France.

2.7 In France

After reaching Paris, Rejewski, Różycki, and Zygalski spent a few days on formalities and meeting with Bertrand's organization. At this time, Bertrand himself was in Rumania, attempting "to secure the release from internment camps of officer and civilian workers of the Polish" [5, page 75] Cipher Bureau. He returned shortly after, followed by the Cipher Bureau personnel.

At this time, the French government and military were irritated by the Polish ambassador and military attaché. This was at least partly because the Poles were openly opposed to France's lack of initiative in the conflict. Instead of attacking the Germans, France decided to wait for the Germans at the Maginot Line. Although several high ranking officers disagreed with this policy, Bertrand included, they were "regarded as pessimists" and forced "to follow the rapid advances of the

German armies through Poland on a scrupulously maintained situation map." [5, page 76]

On October 20, 1939, the Polish cryptographers "resumed their interrupted struggle with the German ciphers." [5, page 81] Although the French were not actively engaged in war with the Germans, they still realized the importance of military intelligence, and allowed Major Bertrand free reign with his cipher bureau. As of November, the now joined French and Polish cipher bureaus moved from Paris to Gretz-Armainvillers, to a chateau with the code name of Bruno, which, for the duration of the war, "became the chief headquarters and foundation of all Allied radio intelligence." [5, page 83]

The Poles had managed to bring two Enigma machines out of Poland, and these, as well as one they had given the French at the Warsaw conference, were at their disposal. They were also able to obtain the perforated sheets that were now being manufactured in Britain, in exchange for German Navy and Air Force signals. With this and other equipment, they began to reconstruct their solution to the wartime Enigma system, for which most documentation had been lost on the way out of Poland.

The constant use of the Enigma machines was wearing the machines out. Bertrand thus ordered forty copies to be made, and the subsequent dismantling of one of the machines to copy slowed down the reading of signals. Unfortunately, the manufacturing proceeded very slowly, and six months later, no new machines had yet been received. "It was only after the fall of France in June 1940 and the opening

of underground work in the free zone of the south that four machine were finally assembled from parts produced in occupied France." [5, page 85]

When they first arrived at Bruno, Rejewski, Różycki, and Zygalski often worked sixteen or seventeen hour days. They were needed to break the daily keys, which normally changed shortly after midnight, so often worked from 3pm until 6 or 7 in the morning. They were also required to decipher complete messages as they did not immediately "have experienced decipherers to help them." [5, page 86] At times, Marian Rejewski was exempted from night duty "to work on the theoretical and mathematical aspects of cipher breaking" [5, page 87], and producing a secret handbook to be used in training new workers.

Work continued in France much like this until Germany attacked France on the 10th of May, 1940. At this point, the Polish cryptologists were moved back to Paris. This attack was a surprise for the French "not because of lack of warning to the Allies, but because of a lack of belief by the French High Command" [5, page 105]. This was not the only such occasion on which the cryptologists were ignored. On June 3rd, 1940, Paris was bombed, but though more than sufficient warning had been given, nothing was done to counter the attack.

2.8 After the Occupation of France

As the Germans grew closer to Paris, plans were made to move the staff of Bruno out of harms way. They were slowly moved through the south of France, until an armistice was signed between France and Germany. Bertrand, however, was not

in favour of working with the Germans, and immediately moved his staff to North Africa. Their final destination was Algeria.

Once things had calmed down in France, but before the new regime had completely taken control, Bertrand started making arrangements for continuing with decryption. He felt that the best location to do this would be inside France. The occupation posed a problem, while at the same time working in their favour as many more messages could be intercepted, including those "supplied by members of the resistance movement working in the French postal system." [5, page 113]. It was decided that the cryptologists would continue working in the unoccupied part of France.

When they returned to France, however, it was discovered that, "in the interim, the Germans had once again changed the procedure for transmitting message keys." [5, page 270] After this point, the Polish cryptologists ceased to work on the Enigma code, and left that work to those better positioned and with more resources, the British. The Poles instead worked on deciphering other codes, where their experience and skills could be of some use.

In November, 1942, the Allies landed in North Africa, and the Germans moved into the unoccupied zone of France. [5, page 270] Then, says Marian Rejewski,

> Major Bertrand quickly evacuated us all to the Côte d'Azur in order to organize our transfer in small groups across the Pyrenees into Spain, and on to Great Britain. However, not all the expeditions turned out happily. In crossing the Spanish border, Lieutenant Colonel Langer, Major Ciężki, and engineer Palluth fell into the hands of the Germans. Palluth died on 19 April 1944 in a forced-labour camp when he was struck by a fragment of an Allied bomb dropped during an air raid on the camp. Lieutenant

> Colonel Langer, Major Ciężki were put into prisoner-of-war camps, from which they were liberated by the Allies only in May 1945. Jerzy Różycki had died earlier, on 9 January 1942, in the wreck of a ship that was carrying him across the Mediterranean. Thus, only Henryk Zygalski and I reached Great Britain. There, inducted into the Polish Army, we worked for a time at solving German Ciphers (but not the Enigma Cipher) until, under the terms of the pertinent Soviet-British agreement, our small unit was disbanded. [5, page 270]

After the war, Zygalski became a lecturer at the Battersea Technical College in England. Rejewski, not in good health, held administrative jobs in the business sector, until retirement. Neither cryptologist received much in the way of recognition until thirty years later, when Gustave Bertrand, among others, made public their accomplishments. Marian Rejewski "gave unstintingly of his time to all who wished to know ... about his achievements and those of his colleagues." [5, page 225] Henryk Zygalski died near Plymouth in 1978, and Rejewski in February 1980, at his home in Warsaw.

After their deaths, the cryptologists became the heroes of a Polish movie, *Sekret Enigmy*, and a television series. They also became the subjects of a stamp, the first to recognize the achievements of cryptologists.

2.9 Contributions of the British and the French

Often the British are credited with the complete solution of the Enigma. While we know that the Polish actually found the solutions to the earlier incarnations of the Enigma, the British contributions should not be ignored. Because so much of the British military was based in their Air Force and Navy, their communication and

decryption services were heavily emphasized. Thus, these services had access to more qualified personnel, technical resources, and money, than those of any other country. [5, page 95]

Although they never managed to solve the Enigma on their own, they were able to take the solution and find better ways to utilize it, and to change it to keep up with the German changes. They could put money and manufacturing into making more Enigma copies, as well as the other tools the Poles had developed. They were also able to create better tools, even going so far as to invent one of the earliest computers in the process. In summary, the British were able to turn the solution into a viable and efficient system of decryption.

The French contribution also cannot be overlooked. They gave the Poles a place to work and resources to call upon, as well as a measure of security, after they were forced out of Poland. They also acted as a conduit for relations between the Poles and the other Allied countries. The most important contribution of the French to the Enigma effort, however, was the information they received from the spy, Asche, and passed on to the Poles.

Thus we can see that although the Polish actually initially solved the Enigma, they should not be alone in getting credit for it. Without the assistance of the French, they would not have been able to find a solution as quickly, if at all. Without the British, the solution would have been of much less use, and would not have been able to stay current with the many changes the Germans were making to their encryption processes.

Chapter 3

The Machine

3.1 The Invention

The Enigma code machine was invented in 1918 by Arthur Scherbius, an electrical engineer [4, page 31]. It was initially rejected by both the German navy and Foreign Office, so Scherbius turned to the commercial market. The Enigma began production in 1923, but remained unprofitable until the end of 1924 [4, page 38]. The navy, however, were now looking for a new code system, as it had been discovered "that the British had been reading coded German naval messages for much of World War I" [4, page 38]. After looking into a variety of machines, they decided on Scherbius' Enigma. In 1925, production of the naval Enigma began [4, page 40] and by 1926, the navy had enough to put them into service. In 1928 the army began using a slightly altered version. [4, page 41]

We shall deal mostly with the army Enigma, as that is the machine that the Polish

solved. It was a little less complicated than the naval machine, although it eventually attained some of the other machine's characteristics. They both contained much of the same parts, most significantly the rotors, which were the basis of the new encryption method.

3.2 A Description

The Enigma machine looked, from the outside, like a combination of a typewriter and a cash register (see Figure B.1 on page 72). It consisted of a keyboard, a plugboard, an entry rotor or drum, three moving rotors, a reflector or reversing drum, and a lampboard. A current would flow from the keyboard, through the plugboard, the entry drum, and the three rotors, be turned by the reflector, and go back through the rotors, entry drum, and plugboard, and light up the lampboard.

3.2.1 The Keyboard and Lampboard

The keyboard and the lampboard were the input and output mechanisms of the Enigma machine. The keyboard was a standard typewriter keyboard on which the encrypter would type his message. The lampboard was a set of 26 lights located above the keyboard. When an input letter was encoded, the output letter would light up on the lampboard. A printer was originally used, but that made the machine much too big and cumbersome.

3.2.2 The Plugboard

The plugboard "consisted of a plate with twenty-six sockets, each representing a letter, that could be connected to one another by short cables with jacks on the end." [4, page 41] (see Figure B.1 on page 72) The plugboard was connected to both the keyboard and the lampboard so that the current (and thus the code) traveled through the plugboard at the beginning and end of the encryption, making decryption by the same method possible. When the Enigma was first put into use, six pairs of letters were always connected, but as the war continued, this number was increased, and a range of numbers of connections was available.

3.2.3 The Entry Drum

The entry drum was essentially the connection from the plugboard to the moving rotors. It was stationary, and was actually eventually discovered to take each letter to itself. It was, therefore, not a factor in the final Enigma solution.

3.2.4 The Rotors

The rotors were the most significant part of the Enigma machine. They were what set it apart from all other codes before this time. They allow the Enigma machine to be more than a simple substitution code. The three rotors were placed side by side in the machine. The order of the rotors, and their initial rotation, were changed periodically, making the Enigma even harder to solve.

An Enigma rotor is a disk somewhat smaller than a hockey puck. It has 26 electrical

contacts evenly spaced around its circumference, usually made of brass. Inside, each contact on one side of the rotor is connected to a contact on the other side, in a random manner (See Figure B.2 on page 73). Every machine was supplied with a set of rotors with identical connections. These connections, which we will call the rotor configuration, are the building blocks of the Enigma code. [4, page 31-32]

The three rotors are placed in the machine in a previously specified way. Each time a letter is input, the first rotor turns one position. Each time the first rotor passes a specific letter or position, the second rotor turns one position, and each time the second rotor passes a specific letter or position, the third rotor turns one position. This 'turnover' position of a rotor was determined by the rotor's ring, a band around the circumference of the rotor, with the alphabet printed on it, which could be rotated around the wheel, and then locked in place. This allowed the encryptors to vary the position of turnover. [4, page 37]

3.2.5 The Reflector

After going through all the rotors, the current passes through the reflector, or reversing drum. The reflector was a stationary drum that, like the rotors, had 26 connections on one side, but instead of sending the current through to the other side, it was output back through the same side. This was accomplished by attaching the wiring from one contact to another on the same side, effectively reversing the flow of the current (see Figure B.3 on page 74). The current would then follow a path back through the machine to the lampboard. This reversing action allowed the same machine to be used for encryption and decryption of messages, as each

letter followed a sort of 'symmetric' path. [4, page 37-38] This, combined with the fact that the rotors were traversed once in either direction, meant that, if the rotors did not rotate, or if we were always looking at the same point of their rotation from a given starting point, the action of the Enigma machine could be represented by a permutation that was a product of thirteen disjoint transpositions.

Chapter 4

The Solution

4.1 Daily Key

The daily key was a document received by the Enigma cipher clerks, on a monthly basis, that dictated the settings of the Enigma machine. These settings, at different times during and before the war, were changed at various intervals, sometimes more than once a day, and sometimes less. The name "daily key" was maintained as this was the most common interval of change. These settings were the plugboard settings, the choice of rotors, their initial positions and orders, and the ring settings on the rotors.

4.2 Message Key

4.2.1 What Was It

The message key was the six character prefix sent with any Enigma communication. It consisted of two successive encryptions of a sequence of three letters, chosen by the Enigma operator. The encryption of these letters was performed with the Enigma machine starting at the initial daily settings. The sequence was encrytped twice so that any mistakes during transmission might be found. For the Germans, the message key was how each cipher clerk let the intended message recipient know how the rotor positions were to be changed from the initial daily settings at the start of the message body. This change was necessary to make the Enigma code more than a complicated substitution cipher that changed daily, but that would be relatively simple to solve each day [5, page 251]. To the Polish, the message key was one of the most important secrets of the Enigma cipher.

4.2.2 Mistakes

Each day, the operators were given rotor settings and orders in the daily key, but the actual positions of the rotors at the beginning of the message was left to their discretion. This meant that, at least at the start of the Enigma's use, some very obvious keys were chosen. These included strings such as 'aaa' and 'qwe' (the first three letters on the German keyboard) as well as many other patterns, both alphabetic, and having to do with the position of the letters on the keyboard. As Rejewski and the others were by this time experienced cryptographers, they were

well aware of the human inclination for making 'random' selections in some kind of pattern, and were able to use this to guess likely combinations of letters. As at least one of the German operators was likely to make one of these choices on any given day, all the decrypters had to do was match it to the message. Thus this inability of humans to do anything completely randomly was one of the factors that led to the solution of the Enigma.

Another such factor was something that the Germans thought would make the solution more difficult: the double encrypting of the message key. Ironically, this double encipherment led almost directly to the solution of the rotor connections, and, additionally, was unable to stop the message keys from being solved [5, page 254].

4.2.3 How it was Used in the Solution

The three letters sent encoded at the beginning of each coded message led to one of the significant breaks in the Enigma solution. They were able to use the fact that the three letters were encoded twice to find permutations of the letters of the alphabet that helped them to find the configuration of the rotors. We shall see that these permutations represented the actions of the Enigma machine starting at the daily setting, and that they were products of thirteen disjoint transpositions (see Section 3.2.5 on page 21). For simplicity of notation, we'll call these permutations A, B, C, D, E, and F. Also note that throughout this paper, a product of permutations will be viewed as a composition of functions. That is, we start from the left to the right when looking at a product of permutations.

On any given day, there could be hundreds of messages sent, many of them intercepted by the Poles. Once it was discovered what the first six letters were, the next step was collecting enough of these preambles to find complete permutations. For example, a set of preambles might be

ajk gdi

grt pcn

psb ekf

eso ahf

From this small example, we take the first letter of each of the blocks of three letters in the first line, the a and the g. Then we would look for a preamble starting with g. From that we would get a p in the second block. Continuing, we get e and a again. This gives the cycle (agpe), which is part of the product AD. Continuing in this fashion, with the first and fourth letters of other permutations, gives us all of AD. The second and fifth letters give us BE, and the third and sixth, CF.

The small example given is very artificial. In practice, there would have to be sixty or more preambles (and thus the same number of messages) to complete all of the permutations. All of these messages would have to be collected on the same day, in order to have the same Enigma settings to work with. This requirement was just one more thing that made the solution of the Enigma difficult.

In all cases, this process gave permutations that contained cycles of equal length in pairs. That is, there were an even number of any length cycle that appeared in the permutation. The following theorem and its proof will explain why.

Theorem 4.1 *Let G be the set of all elements $g \in S_{2n}$ such that g is a product of n disjoint transpositions. Let $\alpha \in S_{2n}$. The equation $XY = \alpha$, $X, Y \in G$ has a solution if and only if the cycle decomposition of α has an even number of (disjoint) cycles of each order.*

If α has $2m_i$ i-cycles so that

$$2n = \sum_{i=1}^{n} i \cdot 2m_i,$$

then the number of solutions is

$$\prod_{i=1}^{n} \frac{i^{m_i} \cdot ((2m_i)!)}{m_i! \cdot 2^{m_i}}$$

Proof: Consider $X, Y \in G$, both with cycle decompositions composed entirely of disjoint transpositions.

Look at the element a_1, and take its transposition in X, say (a_1, b_1).

Then take the transposition (b_1, a_2) in Y, which must exist since Y only has transpositions, and all $2n$ elements possible must be in one of them.

If $a_2 = a_1$, then X contains (a_1, b_1) and Y contains $(b_1, a_2) = (b_1, a_1)$. Since all transpositions in X and Y are disjoint, this is the only occurrence of a_1 and b_1 in X and Y. Thus $XY = \alpha$ would produce $a_1 \to b_1 \to a_1$ and $b_1 \to a_1 \to b_1$, which gives $(a_1)(b_1)$ in $XY = \alpha$, a pair of 1-cycles.

At this point in the process, having placed a_1 and b_1 in their cycle pair, we must choose a new starting element, one not equal to either a_1 or b_1, and begin again.

If $a_2 \neq a_1$, then take (a_2, b_2) in X, which must exist as above. If $b_2 = b_1$, then we have (a_1, b_1) in X and $(a_2, b_2) = (a_2, b_1)$ also in X, which contradicts our assumption of disjoint transpositions.

Then take (b_2, a_3) in Y. Again, this must exist.

If $a_3 = a_2$ then we have $(b_2, a_3) = (b_2, a_2)$ in Y and (b_1, a_2) in Y, which contradicts the disjoint transpositions assumption.

If $a_3 = a_1$, we have $(b_2, a_3) = (b_2, a_1)$, and (b_1, a_2) in Y, and (a_1, b_1) and (a_2, b_2) in X, which gives us $b_2 \rightarrow a_1 \rightarrow b_1$ and $a_2 \rightarrow b_1 \rightarrow a_1$, so we have (b_2, b_1) and (a_2, a_1) in $XY = \alpha$, a pair of 2-cycles. Using the (a_2, b_2) transposition in this process instead of (a_1, b_1) gives us the same result.

If $a_2 \neq a_1$, we continue the process as above, each time adding new elements until we find one repeated, ie $a_k = a_1$. This must happen, as all $2n$ elements in X are in some cycle (transposition) in Y.

Then $(a_1, a_2, \ldots, a_{k-1})$ and $(b_1, b_{k-1}, \ldots, b_2)$ are in α.

Note that in each case two disjoint cycles of the same length are produced.

If the same procedure is repeated on the remaining elements, more pairs of disjoint cycles are produced, as no cycle could contain one of the already used elements.

Thus, if X and Y are as given, an α of the required form is produced.

Now take α such that it is a product of an even number of cycles of each order.

Consider k-cycles, of which there are $2m_k$.

Take two of these, say $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_k)$. Pair these as (a_1, b_1), (a_2, b_2), $\ldots$, (a_{k-1}, b_{k-1}), (a_k, b_k) in X and (b_1, a_2), (b_2, a_3), $\ldots$, (b_{k-1}, a_k), (b_k, a_1) in Y. This is like writing one permutation above the other, and pairing the elements

vertically. Then, as above, the product of these gives $(a_1, a_2, \ldots, a_k)(b_1, b_2, \ldots, b_k)$. Continuing this method on each remaining pair of like-ordered cycles we get a solution (X, Y).

Thus the first part of the theorem is proved.

Again, consider k-cycles. There are $2m_k$ of these. Thus, there are

$$\binom{2m_k}{2}$$

ways to choose one pair,

$$\binom{2m_k - 2}{2}$$

for the next, and so on. Therefore, we have

$$\left(\frac{(2m_k)!}{2!(2m_k-2)!}\right)\left(\frac{(2m_k-2)!}{2!(2m_k-4)!}\right)\cdots\left(\frac{4!}{2!2!}\right)\left(\frac{2!}{0!2!}\right) = \frac{(2m_k)!}{(2!)^{m_k}} = \frac{(2m_k)!}{2^{m_k}}$$

ordered pairs of k-cycles. To look at unordered pairs we need to divide by $m_k!$, the number of permutations of each set of pairs. Thus we have

$$\frac{(2m_k)!}{m_k!2^{m_k}}$$

ways to choose the pairs.

Finally, we can pair the elements of these k-cycles in k different ways for each of the m_k pairs.

Thus we have

$$\frac{k^{m_k}(2m_k)!}{m_k!2^{m_k}}$$

ways to make 2-cycles of the k-cycles.

Finally, taking the product over all cycles, we have

$$\prod_{i=1}^{n} \frac{i^{m_i} \cdot (2m_i)!}{m_i! \cdot 2^{m_i}}$$

solutions to $XY = \alpha$.

■

From this theorem, we can see that AD, BE and CF are products of two permutations, each written as a product of only disjoint transpositions. These are our A, B, ... , F. The proof also tells us how to find A, B, ... , F, by pairing the elements of pairs of equal length cycles.

4.2.4 Analysis of Theorem 4.1

We can see from this theorem that, while we know how many solutions there are to $XY = \alpha$, this number is not always small, or even reasonable. In fact, with only the 26 letters of the alphabet, there can be a huge number of solutions, sometimes billions of them (see Table A.1). What we need to know is how often this number is small enough to be useful. To find this out, we need to look at the individual cycle decompositions of our permutations, AD, BE, and CF.

First we need to look at the possible types of cycle decompositions of $\alpha \in S_{26}$. There are 101 of these. We then need to take a particular type of cycle decomposition, and find out how many of these there are. Since our permutations are composed of disjoint cycles, each cycle length appearing in an even number, we can come up with a formula for the number of possibilities. The formula for this is:

$$\frac{(2n)!}{\prod_{i=1}^{n} (i^{2m_i} \cdot (2m_i)!)}.$$

Finally, we need to calculate the number of solutions for each of the possible cycle decompositions, using the formula given in the theorem,

$$\prod_{i=1}^{n} \frac{i^{m_i} \cdot (2m_i!)}{m_i! \cdot 2^{m_i}}.$$

This data is collected in Table A.1 on page 63.

Using the values in Table A.1, we can see that there are a total of 2, 927, 671, 399, 386, 587, 378, 671, 616 possible permutations of the type we require. We now want to look at how often there are a small number of solutions to the equation. Table A.2 on page 69 gives these values. We can see that in most cases there will be very few solutions. In 96% of the cases, there will be less than fifty possible solutions for A. This means that most of the time, there were very few cases to look at to find the correct one, and that it would very seldom have been impossible to test all of the possible solutions, even given that that there was no access to computers.

4.2.5 Finding the Right Solution

Now that we've discovered that we would usually have a small number of solutions, we need to discover which of these solutions is the correct one. To do this, we use the known foibles of the encryptors, mentioned earlier, such as using keys like 'aaa' and 'qwe'. This was not always possible given the message data on a given day, but an example will demonstrate how it could have been done. The following example was taken from [1].

For a given day, we collect the message keys (see Table A.3 on page 69). From this table, we can see that there are four keys that have been repeated: AHY OHU, KTR YZH, RHO KHE, and RPS KGO. Since the German message encoders were more likely to use alphabetic or keyboard sequences than any other sequence, we can assume that these represent such sequences. We also need to calculate the three permutations AD, BE, and CF. These are:

$$AD = (XUFBV)(CMSTJ)(AOQ)(RKY)(DG)(EH)(LZ)(PW)(I)(N)$$
$$BE = (UQNAJPGVIWCY)(FTZLKEXDRMOB)(H)(S)$$
$$CF = (CYUVBXD)(EFPGTSO)(HWIR)(JQZL)(AN)(MK)$$

The two pairs of 1-cycles tell us that in the message keys, an I or N in the first position must decipher to the other, and in the second position, an H or S must decipher to the other. Not much of this information is useful, except that H deciphers to S. Thus AHY and RHO come from ?S? (where '?' represents an unknown letter). From the alphabet, we have RST, and from the keyboard, we have WSX,

ASD, and ESZ, as well as the reverses of these as possible keys. If we look again at the permutation AD, we see that R and A come from 3-cycles, which we can match up in the following way:

(AOQ)

(RYK)

This gives us the possibility that A deciphers to R and R deciphers to A, which in turn gives RHO into AS? and AHY into RS?. Looking back at our possible keys, we see that probably RHO deciphers to ASD and AHY deciphers to RST. This allows us to match up the 7-cycles in CF in the following way:

(CYUVBXD)

(STGPFEO)

Using the previous information, we can take RPS to A?C, which is likely to be ABC, and thus we have:

(PGVIWCYUQNAJ)

(BFTZLKEXDRMOB)

in BE. Finally, we can decipher KTR to QA?, which is likely QAZ, and thus we get:

(RHWI)

(ZLJQ)

in CF. This gives us most of the matchings for the theorem, and from here, we should be able to use the rest of the message keys to find the complete matchups.

In this way, we can use the message keys to find the exact permutations A,B, ... , F. You can see that this example is very artificial. However, on a normal day there could be many more messages, and thus more message keys to work with. This gave them more chances of finding repeated keys, and more chances to get keys that gave them more information. This method also relied heavily on the mistakes made by the encryptors, but these mistakes did happen fairly often. They also, over time, came to 'know' the individual encryptors, and what their particular mistakes might be.

4.3 Rotors

4.3.1 The Basic Equations

We now want to try to convert the action of the Enigma into algebraic equations, or operations in permutations. We want to take each part of the machine, the rotors, the plugboard, the reflector, etc., and give each a letter to represent its action. If we use the same letters as Rejewski, we have:

S = plugboard

L = rotor 3

M = rotor 2

N = rotor 1

R = reflector

H = entry drum

(See Figure B.1 on page 72)

Thus the path of a message entry through the Enigma is:

$$SHNMLRL^{-1}M^{-1}N^{-1}H^{-1}S^{-1}$$

which represents its travel from the keyboard through the plugboard, the entry drum, the three rotors and the reversing drum, and back to the lampboard.

Since the Enigma rotated the rotors to create the code, we must take this successive movement into consideration. Thus we must introduce a permutation in S_{26}, called P, into the equation to represent this rotation. We will, for now, only consider the rotation of the first rotor. This is because the second rotor only turns every twenty-six rotations of the first rotor, and thus for a series of six rotations, of the twenty-six starting points of the first rotor, only twenty-one of these will involve a change in the second rotor. The third rotor changes even less frequently.

If we take our permutation A to be the basic or intitial permutation shown above, we have:

$$A = SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S^{-1}$$

$$B = SHP^{2}NP^{-2}MLRL^{-1}M^{-1}P^{2}N^{-1}P^{-2}H^{-1}S^{-1}$$

$$\vdots$$

$$F = SHP^{6}NP^{-6}MLRL^{-1}M^{-1}P^{6}N^{-1}P^{-6}H^{-1}S^{-1}$$

Now we want to solve these equations for N, M, L and R.

4.3.2 The First Rotor

At first it was assumed that the entry drum of the military Enigma was the same as that of the commercial Enigma. Thus the permutation created by this drum was thought to be

$$H = \begin{pmatrix} qwertzuioasdfghjkpyxcvbnml \\ abcdefghijklmnopqrstuvwxyz \end{pmatrix}$$

That is, the rotor took input in the order of the German keyboard, and produced output in alphabetical order. Although this assumption eventually proved to be false, much time and effort was lost in trying to solve the Enigma using it, and work was consequently almost abandoned. [5, page 255]

Although this original assumption was false, we will assume that H is known. At this time, the ninth of December, 1932, Rejewski was given a photocopy of two tables of daily keys for September and October 1932 [5, page 256]. Since these tables also gave the daily plugboard connections, the permutation S was now known for some of the data. Thus we can write

$$A = SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S^{-1}$$

$$\text{as} \quad H^{-1}S^{-1}ASH = PNP^{-1}QPN^{-1}P^{-1} \qquad (Q = MLRL^{-1}M^{-1})$$

where the left hand side is assumed to be known. Similarly, we have

$$H^{-1}S^{-1}BSH = P^2NP^{-2}QP^2N^{-1}P^{-2}$$
$$\vdots$$
$$H^{-1}S^{-1}FSH = P^6NP^{-6}QP^6N^{-1}P^{-6}$$

where again the left sides are assumed to be known. Since P is also a known permutation, we transfer the preceding and succeeding P's from the right hand side to the left hand side, giving

$$P^{-1}H^{-1}S^{-1}ASHP = NP^{-1}QPN^{-1}$$
$$P^{-2}H^{-1}S^{-1}BSHP^2 = NP^{-2}QP^2N^{-1}$$
$$\vdots$$
$$P^{-6}H^{-1}S^{-1}FSHP^6 = NP^{-6}QP^6N^{-1}.$$

Finally, for simplicity, we shall rename the left hand side:

$$U = NP^{-1}QPN^{-1}$$
$$V = NP^{-2}QP^2N^{-1}$$
$$\vdots$$
$$Z = NP^{-6}QP^6N^{-1}.$$

Now we want to look at these equations as successive products. Thus we have:

$$\begin{aligned} UV &= NP^{-1}QPN^{-1}NP^{-2}QP^2N^{-1} \\ &= NP^{-1}(QP^{-1}QP)PN^{-1} \\ VW &= NP^{-2}QP^2N^{-1}NP^{-3}QP^3N^{-1} \\ &= NP^{-2}(QP^{-1}QP)P^2N^{-1} \\ &\vdots \\ YZ &= NP^{-5}QP^5N^{-1}NP^{-6}QP^6N^{-1} \\ &= NP^{-5}(QP^{-1}QP)P^5N^{-1}. \end{aligned}$$

Now, substitution gives us:

$$\begin{aligned} VW &= NP^{-1}N^{-1}(UV)NPN^{-1} \\ WX &= NP^{-1}N^{-1}(VW)NPN^{-1} \\ &\vdots \\ YZ &= NP^{-1}N^{-1}(XY)NPN^{-1}. \end{aligned}$$

From this we can see that VW is transformed from UV by the $NP^{-1}N^{-1}$. Our goal now is to solve for $NP^{-1}N^{-1}$. To do this, we need a theorem.

Theorem 4.2 *Let $\alpha, \beta \in S_n$. The equation $X\alpha X^{-1} = \beta$ has a solution $X \in S_n$ if and only if α and β have the same cycle decompositions.*

Suppose that α (and β) is a product of m_1 1-cycles, m_2 2-cycles, ..., m_n n-cycles

so that

$$n = \sum_{i=1}^{n} i \cdot m_i.$$

Then the number of solutions to $X\alpha X^{-1} = \beta$ *is*

$$\prod_{i=1}^{n} i^{m_i} \cdot (m_i!)$$

Proof: Suppose α and β have the same cycle decompositions. That is, both have m_1 1-cycles, m_2 2-cycles, ..., m_n n-cycles.

Now take each k-cycle in α and map the first element of that k-cycle to an element of a k-cycle in β. For the k-1 elements left in the chosen k-cycles, continue this process by mapping each subsequent element in the k-cycle in α to the subsequent element in the k-cycle in β. Continue this for each cycle in α, not reusing any cycle in β.

ie. if $\alpha = (12)(34)(5678)$ and $\beta = (23)(45)(6781)$ the following are possible mappings:

$$X = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 1 \end{pmatrix}$$

$$\text{or } X' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 3 & 2 & 8 & 1 & 6 & 7 \end{pmatrix}$$

Then $X\alpha X^{-1}(1) = X\alpha(8) = X(5) = 6 = \beta(1)$.

In general, suppose $\alpha : i \to j$ and $X : i \to p, j \to q$. Then $X\alpha X^{-1} : p \to i \to j \to q$. Now show $\beta : p \to q$. Since $X : i \to p$ (and therefore $X^{-1} : i \to p$) and $\alpha : i \to j$, by construction, and since $X : j \to q$, we have $\beta : p \to q$. Thus $X\alpha X^{-1} = \beta$.

Therefore α and β having the same cycle decomposition implies that α and β are conjugate.

Now suppose α and β differ only by replacing elements in cycles, that is, are conjugate. Since no element can be used more than once to replace another, the cycles remain disjoint, and thus α and β have the same cycle decomposition.

Proof of the second part:

Leave α in the given order. How many permutations of β are there that leave cycle groupings as they are in α?

Starting with the 1-cycles, there are m_1 of them. Thus there are $m_1!$ orders to write the cycles in, since all the cycles are disjoint. Finally, there is only on way to write each 1-cycle, so we have a total of $m_1!$ ways to write the 1-cycles.

Now we look at the 2-cycles, of which there are m_2. Thus there are $m_2!$ different orders to write the cycles in, since, again, all cycles are disjoint. There are 2 ways to write each cycle as each has two elements. Therefore there are 2^{m_2} ways to write the cycles, not counting order of cycles, which gives us a total of $2^{m_2} \cdot m_2!$ ways to write the 2-cycles.

:Finally, look at the n-cycles. There are m_n n-cycles, which can be written $m_n!$ different orders. There are n ways to write each cycle, and therefore there are n^{m_n}

ways to write each cycle, not counting order of cycles. This gives $n^{m_n} \cdot m_n!$ ways to write the n-cycles.

Thus our final result is:

$$(m_1!)(2^{m_2} \cdot m_2!) \ldots (n^{m_n} \cdot m_n!)$$
$$= \prod_{i=1}^{n} i^{m_i} \cdot m_i!$$

■

So we let UV = α, VW = β and $NP^{-1}N^{-1} = X$. From the theorem we know that there are solutions for $NP^{-1}N^{-1} = X$ and we know how many solutions there are. We can find these solutions by subscribing UV above VW as in the theorem. If we do this in all possible ways, we get all the possible solutions. Doing this for the other combinations, VW and WX, ... , XY and YZ, gives us the other sets of solutions. If we compare these sets, we should find at least one solution common to all the solution sets (there will always be at least one solution as these solutions come from a real code). In fact, we will probably have only to check two of the solution sets to find the solution, as there will usually be only one element common to any two sets. This common solution is our desired value for $NP^{-1}N^{-1} = X$.

At this point, Rejewski's solution seemed to fall apart. Contrary to the theory, there were no matching solutions in the solution sets. This setback almost caused the work to be abandoned, until Rejewski's looked at his original assumptions. He soon realized that he had the entry drum permutation wrong, as it was the only unfounded guess he had made. When he made another hypothesis, that the entry drum was connected in alphabetical order, that is, H was the identity, the solution

was clear.

Now that we have a solution for $NP^{-1}N^{-1} = X$, we want to find N. This is done by subscribing $NP^{-1}N^{-1}$ below P, which we know, in all 26 possible ways (as P, and therefore $NP^{-1}N^{-1}$, is a 26 cycle). This gives us all the ways that rotor N could be put in the machine. Each of the 26 solutions is correct for some setting, but it is difficult to know which is the "base case", the setting of the rotors that emerge in practice only when the rotors are put in the machine with identical settings. What could be done, however, was to choose one of the solutions to be our base case, and to adjust the interpretation of any given settings accordingly.

4.3.3 Analysis of Theorem 4.2

We know that there are a finite number of solutions, and we know that one of them must be in all the solution sets, and thus must be the correct solution. The important questions is, how many solutions are we finding and comparing? To discover this, we must analyze the values given by this theorem, much as we did those we found in Theorem 4.1.

In this case, there are 2436 different cycle decompositions of permutations of 26 elements. Therefore, we will not create a table of all of the values, but merely pick out some values that give us a good idea of what we are looking at. There are a total of about $.4032914611 \cdot 10^{27}$ permutations of 26 elements. The numbers and percentages of these with numbers of solutions less than some specific values are given in Table A.4 on page 70.

From Table A.4 we can see that the results for Theorem 4.2 are not as good as for Theorem 4.1. However, not as much analysis needs to be done with these numbers. All we need to do is find two that are the same, not check each to see if they work. We can find all the solutions for the first equation, and then find the solutions to the second equation until we find a matching one. Thus, on average, we would have to find about 300 solutions to the first equation, and then find 150 (assuming a random distribution) solutions to the second equation. This second number could probably be lowered by looking at the structure of the second equation, and eliminating matchings that would not be similar to anything found in the first equation, although this might not reduce the total time taken.

4.3.4 The Entry Drum

At this point we want to look at something that came up earlier. Although Rejewski finds the permutation of the entry drum by guessing, he does mention that it could have been discovered through deduction [5, page 258]. We want to show how this might have been possible. This method is similar to that of finding the first rotor, but much more complicated, as we know much less about the structure of the machine at this point [2]. The only parts we can assume that we know are the plugboard, the positions (not configurations) of the rotors and the permutations A, B, ... , F.

We start by assuming that the first rotor is the same rotor starting at the same position throughout our analysis, but that the other two rotors have different configurations, X and Y, that don't change with the rotation of the first rotor. Thus

we are using data from two different days. We will call the position the first rotor starts in the base position, and incorporate this into the permutation N so that we don't have to use extra notation. Finally, we know the plugboard configuration. Thus we can write:

$$\begin{aligned} K_1 &= S^{-1}AS = HPNP^{-1}XPN^{-1}P^{-1}H^{-1} \\ K_2 &= S^{-1}BS = HP^2NP^{-2}XP^2N^{-1}P^{-2}H^{-1} \\ &\vdots \\ K_6 &= S^{-1}FS = HP^6NP^{-6}XP^6N^{-1}P^{-6}H^{-1} \end{aligned}$$

and

$$\begin{aligned} K_1^* &= S^{-1}AS = HPNP^{-1}YPN^{-1}P^{-1}H^{-1} \\ K_2^* &= S^{-1}BS = HP^2NP^{-2}YP^2N^{-1}P^{-2}H^{-1} \\ &\vdots \\ K_6^* &= S^{-1}FS = HP^6NP^{-6}YP^6N^{-1}P^{-6}H^{-1} \end{aligned}$$

where K_i are known and X_i and Y_i represent the current positions of the middle rotors and the reversing drum.

We can then take products of the equations K_i and K_i^*, to get:

$$\begin{aligned} K_1K_1^* &= HPNP^{-1}XPN^{-1}P^{-1}H^{-1}HPNP^{-1}YPN^{-1}P^{-1}H^{-1} \\ &= HPNP^{-1}XYPN^{-1}P^{-1}H^{-1} \end{aligned}$$

$$\begin{aligned}
K_2K_2^* &= HP^2NP^{-2}XP^2N^{-1}P^{-2}H^{-1}HP^2NP^{-2}YP^2N^{-1}P^{-2}H^{-1} \\
&= HP^2NP^{-2}XYP^2N^{-1}P^{-2}H^{-1} \\
&\vdots \\
K_6K_6^* &= HP^6NP^{-6}XP^6N^{-1}P^{-6}H^{-1}HP^6NP^{-6}YP^6N^{-1}P^{-6}H^{-1} \\
&= HP^6NP^{-6}XYP^6N^{-1}P^{-6}H^{-1}
\end{aligned}$$

If we now rearrange the equations to isolate XY, we get:

$$\begin{aligned}
XY &= PN^{-1}P^{-1}H^{-1}K_1K_1^*HPNP^{-1} \\
XY &= P^2N^{-1}P^{-2}H^{-1}K_2K_2^*HP^2NP^{-2} \\
&\vdots \\
XY &= P^6N^{-1}P^{-6}H^{-1}K_6K_6^*HP^6NP^{-6}
\end{aligned}$$

We can now do some substitution:

$$\begin{aligned}
K_2K_2^* &= HP^2NP^{-2}PN^{-1}P^{-1}H^{-1}K_1K_1^*HPNP^{-1}P^2N^{-1}P^{-2}H^{-1} \\
&= HP^2NP^{-1}N^{-1}P^{-1}H^{-1}K_1K_1^*HPNPN^{-1}P^{-2}H^{-1} \\
&= HP^1(PNP^{-1}N^{-1})P^{-1}H^{-1}K_1K_1^*HP(NPN^{-1}P^{-1})P^{-1}H^{-1} \\
&\vdots \\
K_6K_6^* &= HP^6NP^{-6}P^5N^{-1}P^{-5}H^{-1}K_5K_5^*HP^5NP^{-5}P^6N^{-1}P^{-6}H^{-1} \\
&= HP^6NP^{-1}N^{-1}P^{-5}H^{-1}K_5K_5^*HP^5NPN^{-1}P^{-6}H^{-1} \\
&= HP^5(P^1NP^{-1}N^{-1})P^{-5}H^{-1}K_5K_5^*HP^5(NPN^{-1}P^{-1})P^{-5}H^{-1}
\end{aligned}$$

Since we know the values of $K_i K_i^*$ for $i = 1, 2, \ldots, 6$ we can solve for

$$\Gamma_i = HP^i(P^1NP^{-1}N^{-1})P^{-i}H^{-1}$$

using Theorem 4.2.

At this point, we must assume that the size of the solution set for the above equation is relatively small so that we can work with all the solutions. We now want to isolate

$$(P^1NP^{-1}N^{-1})$$

by moving the surrounding permutations to the other side:

$$P^{-i}N^{-1}\Gamma_i HP^i = (P^1NP^{-1}N^{-1})$$

We can then equate the permutations containing Γ_i and Γ_{i+1}:

$$P^{-i}N^{-1}\Gamma_i HP^i = P^{-i-1}N^{-1}\Gamma_{i+1}HP^{i+1}$$

and isolate Γ_{i+1}:

$$HPH^{-1}\Gamma_i HP^{-1}H^{-1} = \Gamma_{i+1}$$

Now we can solve for HPH^{-1}, using Theorem 4.2, as both Γ_i and Γ_{i+1} are known. We take the solutions to these equations that are in all five solution sets, and get

a possible set of values for each Φ_i in the equation:

$$HPH^{-1} = \Phi_i$$

With these values, we can solve for H, as P is known, which gives us a set of solutions for H. Since P is a 26-cycle, HPH^{-1} is also a 26-cycle, and there are only 26 solutions, one of which must be the solution of the entry drum, and this one must appear in all 5 of the possible solutions sets. Thus we have deduced the configuration of the entry drum.

4.3.5 The Second Rotor

Given the solution to the first rotor, how were the solutions to the other two found? A couple of items made that easier to do. The Germans, in order to make the code harder to solve, had been changing the order of the rotors quarterly. Also, the data supplied to Rejewski had been for September and October 1932, a period bridging two quarters. Thus, for messages after the change, with a new rotor in the first spot, the same method could be applied again.

4.3.6 The Last Rotor

Now we have 26 choices for each of 2 rotors, and one rotor left to solve. At this point we deviate from the actual methods used by Rejewski. We use a more mathematical method than he did, or at least, than he specified.

To solve the last rotor, we assume that in at least one of the months that data was

supplied for, the unknown rotor was the last rotor in the machine. In this case, we need to use the A permutation that we used for solving the first two rotors, but for several days, rather than all six permutations from one day. We also need to choose days in which the settings of the rotors follow an arithmetic progression.

At this point, we can assume that in our usual equation for permutation A, that we know rotors N and M, and the settings of each of these rotors (from the daily key). We want to adjust this equation so that it is possible to permute each of the rotors. That is, we are no longer assuming that just the first rotor moves. Thus, our equation would look like this:

$$A = SP^xNP^{-x}P^yMP^{-y}P^zLP^{-z}RP^zL^{-1}P^{-z}P^yM^{-1}P^{-y}P^xN^{-1}P^{-x}S^{-1}$$

Since we know the configuration of rotors M and N, and their settings, we can let

$$J^{-1} = SP^xNP^{-x}P^yMP^{-y}$$

and so we can write

$$A = J^{-1}P^zLP^{-z}RP^zL^{-1}P^{-z}J$$

$$\text{which gives} \quad JAJ^{-1} = P^zLP^{-z}RP^zL^{-1}P^{-z} = U$$

where the left hand side is known.

We now have

$$J_n^{-1} U_n J_n = A_n$$

where n represents a given set of settings of rotors N and M. We know what a chosen A_n does to input on a given day, and we know what J does to input, given that we know the settings on that day. To solve for U_n, we need to find, among the daily settings given for the month the L rotor is third, are 4 settings for the L rotor in some arithmetic progression.

To give an example to work through the method with, we will choose a progression of 3. So, given our starting value, z, for the permutation of rotor L, we have these equations:

$$J_{n_0} A_{n_0} J_{n_0}^{-1} = P^z L P^{-z} R P^z L^{-1} P^{-z}$$

$$J_{n_3} A_{n_3} J_{n_3}^{-1} = P^{z+3} L P^{-(z+3)} R P^{z+3} L^{-1} P^{-(z+3)}$$

$$J_{n_6} A_{n_6} J_{n_6}^{-1} = P^{z+6} L P^{-(z+6)} R P^{z+6} L^{-1} P^{-(z+6)}$$

$$J_{n_9} A_{n_9} J_{n_9}^{-1} = P^{z+9} L P^{-(z+9)} R P^{z+9} L^{-1} P^{-(z+9)}$$

We now move the bracketing P's from the right side to the left side, as these are also known:

$$P^{-z} J_{n_0} A_{n_0} J_{n_0}^{-1} P^z = L P^{-z} R P^z L^{-1}$$

$$P^{-(z+3)} J_{n_3} A_{n_3} J_{n_3}^{-1} P^{z+3} = L P^{-(z+3)} R P^{z+3} L^{-1}$$

$$P^{-(z+6)} J_{n_6} A_{n_6} J_{n_6}^{-1} P^{z+6} = L P^{-(z+6)} R P^{z+6} L^{-1}$$

$$P^{-(z+9)} J_{n_9} A_{n_9} J_{n_9}^{-1} P^{z+9} = L P^{-(z+9)} R P^{z+9} L^{-1}$$

Now we can rename the left hand side for simplicity:

$$\Psi_0 = L P^{-z} R P^{z} L^{-1}$$

$$\Psi_3 = L P^{-(z+3)} R P^{z+3} L^{-1}$$

$$\Psi_6 = L P^{-(z+6)} R P^{z+6} L^{-1}$$

$$\Psi_9 = L P^{-(z+9)} R P^{z+9} L^{-1}$$

Next, we take products of successive Ψ_i's:

$$\begin{aligned}
\Psi_0 \Psi_3 &= L P^{-z} R P^{z} L^{-1} L P^{-(z+3)} R P^{z+3} L^{-1} \\
&= L P^{-z} R P^{-3} R P^{z+3} L^{-1} \\
&= L P^{-z} (R P^{-3} R P^{3}) P^{z} L^{-1} \\
\Psi_3 \Psi_6 &= L P^{-(z+3)} R P^{z+3} L^{-1} L P^{-(z+6)} R P^{z+6} L^{-1} \\
&= L P^{-(z+3)} R P^{-3} R P^{z+6} L^{-1} \\
&= L P^{-(z+3)} (R P^{-3} R P^{3}) P^{z+3} L^{-1} \\
\Psi_6 \Psi_9 &= L P^{-(z+6)} R P^{z+6} L^{-1} L P^{-(z+9)} R P^{z+9} L^{-1} \\
&= L P^{-(z+6)} R P^{-3} R P^{z+9} L^{-1} \\
&= L P^{-(z+6)} (R P^{-3} R P^{3}) P^{z+6} L^{-1}
\end{aligned}$$

And finally, substitute:

$$\Psi_3\Psi_6 = LP^{-3}L^{-1}(\Psi_0\Psi_3)LP^3L^{-1}$$
$$\Psi_6\Psi_9 = LP^{-3}L^{-1}(\Psi_3\Psi_6)LP^3L^{-1}$$

Now, just as when we were solving for the other two rotors, we use Theorem ref-prop:absoln to find $LP^{-3}L^{-1}$. Then we use the same method as before to solve for L, given that we know P and therefore P^{-3}. Finally, using the daily setting and our solutions to all three of the rotors, as well as "a sample of plain text and its authentic ciphergram at a stated daily key and message key" which had been supplied with the monthly tables of keys, the reversing drum was easy to discover.

On a last note in the solution of the third rotor, we look at the question: can the value of the arithmetic progression be anything? No. If it is 13, for example, there are only two possible values to choose from: z and x+13, as z+26=z. In this case, our analysis would not have been possible. While 2 has the same characteristic of 13, that is, it divides 26, we are only dealing with 4 settings, while there are 13 different values available from 2. However, in this kind of analysis, it is probably best to avoid numbers not relatively prime to the order of the permutation.

4.4 Finding the Daily Key

Now we want to figure out the other connections in the Enigma machine. That is, the particulars specified in the daily key: the plugboard, the rotor positions and orders, and the ring settings. These are the tools and information that we have

used until this time to find out the rotor configurations. Now, given the discovered configurations, we want to find the data that was known previously.

We start by looking at the equations

$$\begin{aligned} A &= SQ_1S^{-1} \\ B &= SQ_2S^{-1} \\ &\vdots \\ F &= SQ_6S^{-1} \end{aligned}$$

where

$$Q_i = P^{x_i}NP^{-x_i}P^{y_i}MP^{-y_i}P^{z_i}LP^{-z_i}RP^{z_i}L^{-1}P^{-z_i}P^{y_i}M^{-1}P^{-y_i}P^{x_i}N^{-1}P^{-x_i}$$

We then want to take products of these equations to get the permutations AD, BE, and CF:

$$\begin{aligned} AD &= SQ_1S^{-1}SQ_4S^{-1} = SQ_1Q_4S^{-1} \\ BE &= SQ_2S^{-1}SQ_5S^{-1} = SQ_2Q_5S^{-1} \\ CF &= SQ_3S^{-1}SQ_6S^{-1} = SQ_3Q_6S^{-1} \end{aligned}$$

We know that the permutations A, B, ... , F and their corresponding Q_i's have the same cycle decompositions, and that their products must also have the same decompositions. We also know that since they are composed of disjoint cycles of 26 elements, there are 101 different possibilities for each decomposition. There are

three equations we are looking at, each with 101 possibilities, and thus $101^3 = 1,030,301$ possible decomposition combinations for AD, BE, and CF. In addition, we know that there are $3! = 6$ different orders for the three rotors, and 26 different positions for each of the three rotors, and thus $6 \cdot 26^3 = 105,456$ different complete settings for the rotors. Thus, there is an average of less than 1 rotor setting for each cycle decomposition combination. While this does not mean that we have at most one rotor setting to test, it does suggest that we would not have to test very many, and that many of the decomposition combinations would not even be possible.

Using this information, we want to make a catalogue of all rotor settings, filed by cycle decomposition combination. At the beginning of the Enigma's use, it was known that the plugboard switched exactly six letters and thus S and S^{-1} consisted of six transpositions. It is also true that the plugboard did not change the cycle decomposition, just the individual permutations. Therefore, it would be quite simple to go through the catalogue and pick those permutations that differed from A by the switching of six letters. From these, it sufficed to try the given settings of rotors and inferred settings of the plugboard on the machine and see which gave intelligible output. Another factor that would help with this testing was the fact that most messages "began with the letters ANX from the word 'an' (German for 'to') and 'x' to separate the words." [5, page 261] This meant that in many cases as few as three letters would have to be checked.

Thus, with a little bit of manual labour, a few calculations, and some luck, it was relatively easy to find the daily settings of the Enigma machine. This meant that the three Polish cryptographers could spend most of their time improving the

methods they already had, and finding new ways to deal with any changes made to the German methods.

4.5 The German Changes

As the Germans grew closer to starting their offensive, and as the subsequent war progressed, an increasing number of changes were made to the way messages were encoded on the Enigma machine. These changes meant that Rejewski was constantly working at solving the Enigma, and made all the cryptologists look for better and more efficient ways to find the daily key, decrypt messages, and keep up with all the changes.

Until December 1st, 1936, there were always exactly six plugboard transpositions. After that time, this number changed to between five and eight transpositions. Not satisfied with the security afforded by this, the Germans increased the number to between seven and ten transpositions on January 1st, 1939 [5, page 268]. This change, however, can be easily dealt with using the catalogue method described in Section 4.4. They would still have to look up the permutation combinations, but instead of looking for a solution with exactly six switches, they would have to consider more of the choices. The catalogue method we describe is a combination of two methods we know the Polish used, their smaller catalogue and the cyclometer. Although not identical to either of these, it accomplishes essentially the same thing and works in a similar way, using the same mathematical principles and Enigma characteristics.

At the beginning, the rotor order was changed once a quarter. On February 1st, 1936, the frequency of change increased to monthly, and eight months later, to daily. [5, page 262] This made knowing the rotor positions very important, and a method was devised to find this more quickly. This method was called the "clock method", and used "the unequal frequency of occurrence of letters in the German language" [5, page 262].

> If we subscribe beneath each other, letter by letter, two texts in German, ..., then within the compass of twenty-six letters, there will be, on average, two columns with identical letters, and this feature will be preserved, as well, when we encipher both texts with the same key. However, if we encipher each text using a different key to the machine cipher, then the twenty-six letters will include, on average, only one column with identical letters. ... Within the compass of twenty-six letters, this phenomenon does not occur in a perceptible way, but when we have messages of say, two hundred sixty letters each, then in general we can tell by this procedure whether they were enciphered using the same or different keys. We make use of this in the following way:
> If we have a sufficient quantity of cipher material, we usually find between ten and twenty pairs of messages such that in each pair the first two letters of the keys are the same and only the third letters if the keys differ. We now subscribe the two messages of a pair beneath each other in such a way that the letters enciphered using the same setting of the drums will appear beneath each other. *A priory*, though, there are two possible ways of subscribing the messages beneath each other, depending on the position of drum N at which the rotation of the middle, the M, drum takes place. These positions are known and are different for each of the three drums.... It suffices, with each of the two possible ways of subscribing the messages beneath each other, to count the number of columns with identical letters, in order to find out which of the ways of subscribing the messages is the right one, and thereby to determine which of the three drums is at the right hand side. [5, pages 262 - 263]

This method was the only method that used characteristics of language, rather than of the Enigma machine.

At the beginning, there were only three rotors to choose from, so it was necessary

merely to figure out in what order they were placed in the Enigma machine. Later, (on December 15th, 1938) however, this number was increased to five, although only three were actually used at any one time. This increased the number of possible rotor orders from six to sixty. To deal with this, the cryptologists had to find the configuration of the new rotors, and figure out which rotors were being used. They assumed that the first, or N, rotor, was a known rotor, that is, one of the original three. They also assumed that the other two rotors consisted of a known and an unknown rotor, and then proceeded exactly as had been done when solving for the third rotor. They would then be able to use a greatly expanded catalogue to find the daily keys. [5, page 268]

On November 1, 1937, the Germans changed the reversing drum. Fortunately, they had discussed this change over the Enigma net prior to that day, so the Poles were prepared for it. Thus, all they had to do was solve the new reflector as they had done the previous one.

Chapter 5

The Spy: Was he really necessary?

As mentioned in Section 2.3 on page 7, there is some controversy as to whether the data obtained from the spy, Asche, was really necessary to the solution of the Enigma. In this chapter, while we will not attempt to give a definitive answer, we will try to shed some light on some of the factors involved.

One of the most significant factors in this decision is whether it would have been possible to find two days with the same rotor settings. To look at this possibility, we need to use the "birthday paradox", which says that in a group of 23 people, there is a 50% chance that two will have the same birthday. We tailor this to our situation using the following estimate, given in [6, page 237 - 238].

We start with an estimate of the probability of no collisions, that is, that no setting appears more than once in k days. We know that the choice on the first day is arbitrary. Given that there are n possible choices, the probability that there were no collisions by the second day is $1 - \frac{1}{n}$, and $1 - \frac{k-1}{n}$ on the kth day. Thus our

estimate is

$$\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\ldots\left(1-\frac{k-1}{n}\right)=\prod_{i=1}^{k-1}\left(1-\frac{i}{n}\right).$$

When x is a small number, as ours is, we know that $1-x\approx e^{-x}$. The estimate is obtained from the first two terms of the series expansion:

$$e^{-x}=1-x+\frac{x^2}{2!}-\frac{x^3}{3!}\ldots.$$

Thus we get

$$\prod_{i=1}^{k-1}\left(1-\frac{i}{n}\right)\approx\prod_{i=1}^{k-1}e^{\frac{-i}{n}}=e^{\frac{-k(k-1)}{n}}.$$

Now we have that the probability of at least one collision is

$$1-e^{\frac{-k(k-1)}{n}}.$$

If we want this probability to be ϵ, we can solve for k as a function of n and ϵ:

$$\begin{aligned}
e^{\frac{-k(k-1)}{n}} &\approx 1-\epsilon \\
\frac{-k(k-1)}{n} &\approx \ln(1-\epsilon) \\
k^2-k &\approx n\ln\frac{1}{1-\epsilon}.
\end{aligned}$$

Ignoring the $-k$ term, we estimate

$$k \approx \sqrt{n \ln \frac{1}{1-\epsilon}}.$$

We finally take $\epsilon = 0.5$ and our estimate is:

$$k \approx 1.17\sqrt{n}.$$

With our $n = 6 \cdot 26^3$, k is approximately 380.

Thus, after 380 days, it would be reasonable to expect two days with the same rotor positions. The problem that arose at this point would be recognizing that two settings were the same, given only the encrypted data of the two days. The method of comparing frequencies of pairs of letters used previously would be of some help, but would not be a guarantee of identical settings. It would only eliminate settings that were probably not the same. Comparing the cycle decompositions would also help, and a combination of these two checks could give a fairly good estimate of when a match was found.

Finally, given that we have found two days with identical settings, we must solve the equations:

$$\begin{aligned} A_i &= S_i HPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S_i^{-1} &&= S_i \Delta_1 S_i^{-1} \\ B_i &= S_i HP^2NP^{-2}MLRL^{-1}M^{-1}P^2N^{-1}P^{-2}H^{-1}S_i^{-1} &&= S_i \Delta_2 S_i^{-1} \\ &\vdots \end{aligned}$$

$$F_i = S_i H P^6 N P^{-6} M L R L^{-1} M^{-1} P^6 N^{-1} P^{-6} H^{-1} S_i^{-1} \qquad = S_i \Delta_6 S_i^{-1}$$

where $i = 1, 2$, $\Delta_j = HP^jNP^{-j}MLRL^{-1}M^{-1}P^jN^{-1}P^{-j}H^{-1}$, and A_i, B_i, ... F_i are known. Isolating the Δ_j's in one set of equations, we can write

$$\begin{aligned}
\Delta_1 &= S_1^{-1} A_1 S_1 \\
\Delta_2 &= S_1^{-1} B_1 S_1 \\
&\vdots \\
\Delta_6 &= S_1^{-1} F_1 S_1
\end{aligned}$$

Then substituting for Δ_j we get

$$\begin{aligned}
A_2 &= S_2 S_1^{-1} A_1 S_1 S_2^{-1} \\
B_2 &= S_2 S_1^{-1} B_1 S_1 S_2^{-1} \\
&\vdots \\
F_2 &= S_2 S_1^{-1} F_1 S_1 S_2^{-1}
\end{aligned}$$

Now, using Theorem 4.2, we can solve for $S_2 S_1^{-1}$.

At this point, we run into a problem: how to solve for S_2 and S_1^{-1}, and thus for S_1. At first glance, it looks like an application of Theorem 4.1, but upon closer inspection, we see that it cannot be. Theorem 4.1 requires that S_2 and S_1^{-1} be products of disjoint transpositions. This is not, however, the case. Both are products of six disjoint transpositions, and fourteen 1-cycles. Thus we have to look

for some other method.

What other method might we use to solve this? For a group of 26 elements, there are

$$\frac{\binom{20}{14,6}\binom{26}{2,2,2,2,2,2}}{20!} = 100,391,791,500$$

possible such permutations, and without further analysis, there is no way to tell which would be the correct ones. It would also require further work to find out how many permutations S_1 and S_2 existed for each product so that it could be known that all had been found. Then testing would have to occur on each of these permutation combinations to find the rotor settings given that choice of permutations. With the limited resources available, this compounding of the task may have made the solution virtually impossible. If you also take into consideration that they probably did not know, without the spy's data, that there were six transpositions, this solution just grows more difficult.

The other main barrier in the solution of the Enigma was the time factor. The Poles knew that invasion was relatively imminent, and they did not want to be wasting the time of one of their most valuable people on something that might not be possible to solve. Several times, even after the information was received from the spy, work was almost stopped on the Enigma. If Asche had never existed, the work would likely have ended in order to use Rejewski's time more profitably than on a seemingly unsolvable code.

Thus we can see that there were many roadblocks on the way to the solution. The chances of finding two days with the same rotor setting were very slim, and the difficulty recognizing such an occurrence only added to the problem. Solving the permutation equations would also have been difficult, especially having been made hundreds or thousands of times harder by having to try each of the possible plugboard solutions. Finally, the time constraints would have made all of this even more impossible, particularly with out the aid of any sort of computing device. Today, it may not be so difficult, as programs could be written, and computer time dedicated to this solution, but with three, and sometimes only one man working on the problem, the obstacles were most likely insurmountable.

Appendix A

Tables

Table A.1: Number of Possible Permutations and Solutions for each Cycle Decomposition in Theorem 4.1

Cycle Decomposition	Permutations	Solutions
1, 12	700158786678134784000000	12
13	119317000333315276800000	13
1, 2, 10	126028581602064261120000	20
2, 11	208311705127378944000000	22
1, 3, 9	69151485104013312000000	27
3, 10	112025405868501565440000	30
1, 4, 8	49229914688306352000000	32
1, 1, 11	69437235042459648000000	33
1, 5, 7	41152189910878126080000	35

Cycle Decomposition	Permutations	Solutions
4, 9	77795420742014976000000	36
5, 8	63014290801032130560000	40
6, 7	57155819320664064000000	42
1, 2, 3, 7	14288954830166016000000	42
2, 3, 8	21879962083691712000000	48
1, 2, 4, 6	10939981041845856000000	48
1, 1, 2, 9	12965903457002496000000	54
2, 4, 7	16075074183936768000000	56
2, 5, 6	14003175733562695680000	60
1, 3, 4, 5	7001587866781347840000	60
3, 4, 6	972442759275187200000	72
1, 1, 3, 8	729332069456390400000	72
1, 1, 4, 7	535835806131225600000	84
1, 1, 5, 6	466772524452089856000	90
1, 2, 2, 8	410249289069219600000	96
1, 6, 6	648295172850124800000	108
2, 2, 9	648295172850124800000	108
1, 1, 2, 3, 6	162073793212531200000	108
1, 1, 2, 4, 5	131279772502150272000	120
1, 1, 1, 10	2800635146712539136000	150
1, 2, 5, 5	1680381088027523481600	150

Cycle Decomposition	Permutations	Solutions
1, 3, 3, 6	1440655939666944000000	162
1, 2, 2, 3, 5	583465655565112320000	180
3, 3, 7	2116882197061632000000	189
2, 2, 3, 6	810368966062656000000	216
1, 2, 3, 3, 4	405184483031328000000	216
3, 5, 5	1493672078246687539200	255
4, 4, 5	1312797725021502720000	240
2, 2, 4, 5	656398862510751360000	240
1, 1, 1, 2, 8	546999052092292800000	240
1, 1, 2, 2, 7	446529838442688000000	252
2, 3, 3, 5	518636138280099840000	270
2, 3, 4, 4	455832543410244000000	288
1, 1, 1, 3, 7	317532329559244800000	315
1, 1, 1, 4, 6	243110689818796800000	360
1, 1, 3, 3, 5	17287871276003328000	405
1, 1, 3, 4, 4	151944181136748000000	432
1, 1, 2, 2, 3, 4	75972090568374000000	432
1, 1, 1, 2, 3, 5	77795420742014976000	450
1, 2, 2, 4, 4	85468601889420750000	576
1, 2, 2, 2, 6	60777672454699200000	720
2, 2, 2, 7	89305967688537600000	840

Cycle Decomposition	Permutations	Solutions
1, 1, 1, 1, 9	61742397414297600000	945
1, 4, 4, 4	68374881511536600000	960
1, 1, 1, 2, 2, 6	20259224151566400000	1080
1, 1, 1, 5, 5	37341801956167188480	1125
2, 2, 2, 3, 4	15194418113674800000	1440
1, 1, 1, 2, 4, 4	11395813585256100000	1440
1, 1, 1, 1, 2, 7	12757995384076800000	1470
3, 3, 3, 4	24010932327782400000	1620
1, 1, 1, 3, 3, 4	9004099622918400000	1620
1, 1, 2, 2, 2, 5	7293320694563904000	1800
1, 1, 1, 1, 3, 6	7717799676787200000	1890
1, 1, 1, 1, 4, 5	6251417738197632000	2100
1, 1, 2, 3, 3, 3	4001822054630400000	2430
1, 1, 1, 1, 2, 3, 4	2170631159096400000	2520
1, 2, 2, 2, 3, 3	2251024905729600000	3240
2, 2, 3, 3, 3	2000911027315200000	4860
1, 1, 1, 2, 2, 3, 3	750341635243200000	4860
1, 1, 1, 1, 2, 2, 5	520951478183136000	6300
1, 2, 2, 2, 2, 4	610490013495862500	6720
1, 1, 1, 2, 2, 2, 4	379860452841870000	7200
1, 1, 1, 1, 1, 8	868252463638560000	7560

Cycle Decomposition	Permutations	Solutions
2, 2, 2, 2, 5	781427217274704000	8400
1, 3, 3, 3, 3	762251819929600000	8505
2, 2, 2, 2, 2, 3	6029530997490000	90720
1, 1, 1, 1, 1, 1, 7	8591242682880000	72765
1, 1, 1, 1, 1, 2, 6	192944991919680000	11340
1, 1, 1, 1, 1, 3, 5	123484794828595200	14175
1, 1, 1, 1, 1, 4, 4	18088592992470000	45360
1, 1, 1, 1, 3, 3, 3	19056295498240000	42525
1, 1, 2, 2, 2, 2, 3	90442964962350000	15120
1, 2, 2, 2, 2, 2, 2	102776096548125	665280
1, 1, 1, 1, 1, 1, 1, 6	64250746560000	810810
1, 1, 1, 1, 1, 1, 2, 5	2104854457305600	103950
1, 1, 1, 1, 1, 1, 3, 4	1461704484240000	124740
1, 1, 1, 1, 1, 2, 2, 4	9044296496235000	45360
1, 1, 1, 1, 1, 2, 3, 3	7146110811840000	51030
1, 1, 1, 1, 2, 2, 2, 3	12059061994980000	37800
1, 1, 1, 2, 2, 2, 2, 2	150738274937250	453600
1, 1, 1, 1, 1, 1, 1, 1, 5	385504479360	10135125
1, 1, 1, 1, 1, 1, 1, 2, 4	18070522470000	1081080
1, 1, 1, 1, 1, 1, 1, 3, 3	2379657280000	3648645
1, 1, 1, 1, 1, 1, 2, 2, 3	121808707020000	374220

Cycle Decomposition	Permutations	Solutions
1, 1, 1, 1, 1, 2, 2, 2, 2	10767019638375	1587600
1, 1, 1, 1, 1, 1, 1, 1, 1, 4	1968466500	137837700
1, 1, 1, 1, 1, 1, 1, 1, 2, 3	133855722000	12162150
1, 1, 1, 1, 1, 1, 1, 2, 2, 2	100391791500	16216200
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 3	9209200	1964187225
1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 2	164038875	413513100
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2	44850	27498621150
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1	1	7905853580625

Table A.2: Percent of Solution Numbers Within Given Bounds for XY = α

No. of Solutions	No. Less Than	Percent Less Than
50	2813739736174304515200000	96.10845455
100	2894931801899428949280000	98.88171886
200	2919453261040612010937600	99.71929439
1000	2927504583673253964802800	99.99430213
2000	2927649559078766757995280	99.99925401
10000	2927670908460732334159780	99.99998323

Table A.3: A Set of Message Keys

AAT	OJS	JTZ	CZL	ROV	KBB
AHY	OHU	KIC	YWY	RPS	KGO
AHY	OHU	KTR	YZH	RPS	KGO
AUQ	OQZ	KTR	YZH	RQM	KNK
ASZ	OLO	LEA	ZXN	SGM	TVK
BKX	VED	LFB	ZRX	SVR	TIH
CFS	MTO	LFE	ZTF	SXO	TDE
CXP	MDG	LNI	ZAR	TGS	JVO
DJU	GVP	LUC	ZQY	THG	JHT
DUI	GQR	MPM	SGK	TLN	JKA
ECS	HYO	ONA	QAN	TLW	JKI
ETH	HZW	OPS	QGO	TMJ	JOQ
FHV	BIW	OSM	QSK	TOQ	JBZ
FVI	BIR	OXQ	QDZ	TOW	JBI
GVP	DGB	PDN	WRA	UOD	FBC
GZK	DLM	PIL	WWJ	WAL	PJJ
HVM	EIK	QDR	ARH	WWD	PCC
IVP	IIG	QYL	AUJ	XRQ	UMZ
JHD	CHC	RHO	KHE	ZHR	LHH
JSF	CSP	RHO	KHE	ZWS	LCO

Table A.4: Percent of Solution Numbers Within Given Bounds for $X\alpha X^{-1} = \beta$

No. of Solutions	No. Less Than	Percent Less Than
50	57213885045335786127360000	14.18673356
100	87168883973322306355200000	21.61436390
150	12808102836763978039296000	31.75892394
200	16215823550414576664576000	40.20869548
286	20133746766748026187776000	49.92356326
500	25287218369115760189440000	62.70209218
750-	29200233582263039746867200	72.40479008
1000	31715056462213489578393600	78.64053549
2400	36335831997314150287257600	90.09819325

Appendix B

Figures

Figure B.1: The Enigma Machine

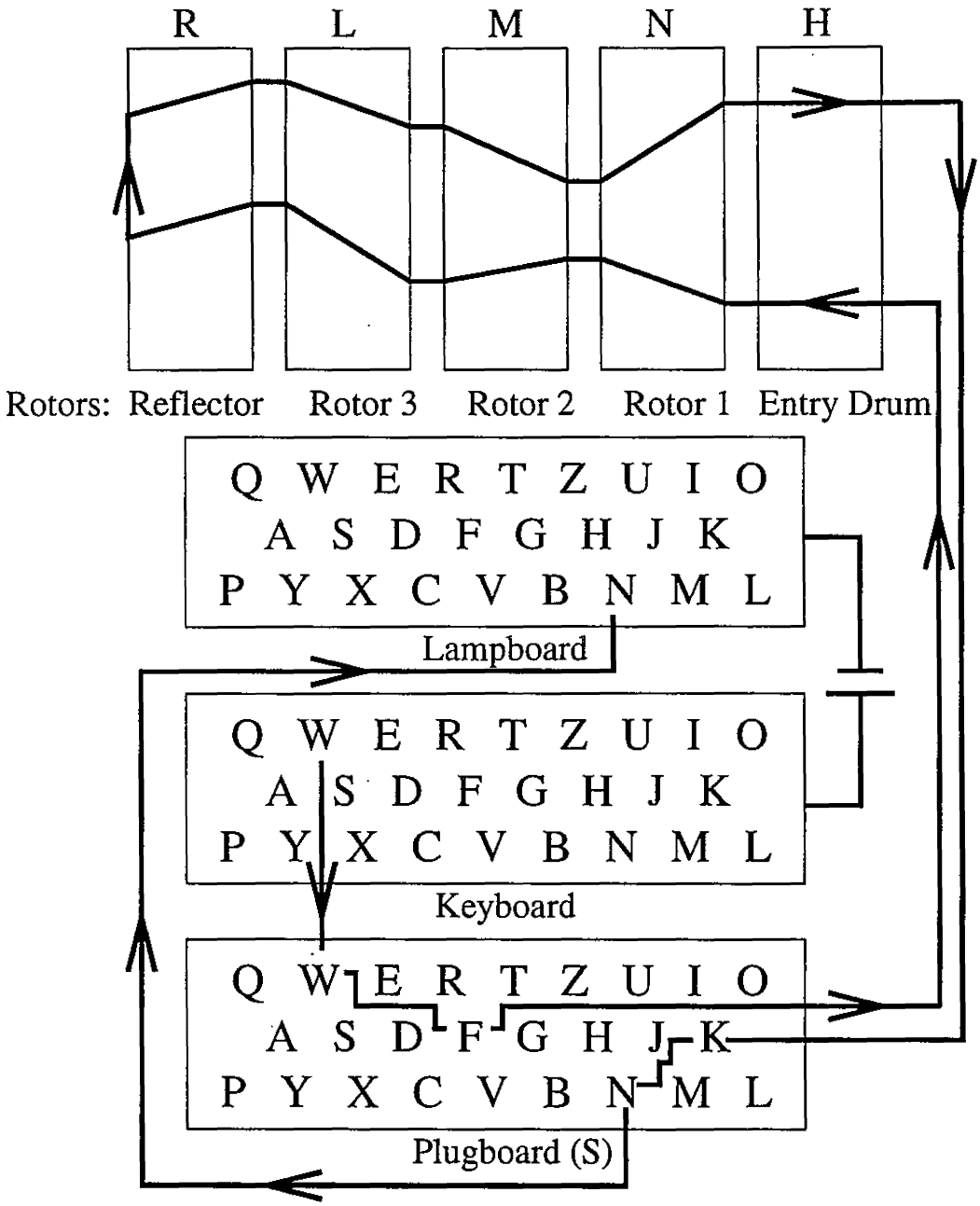


Figure B.2: A Rotor

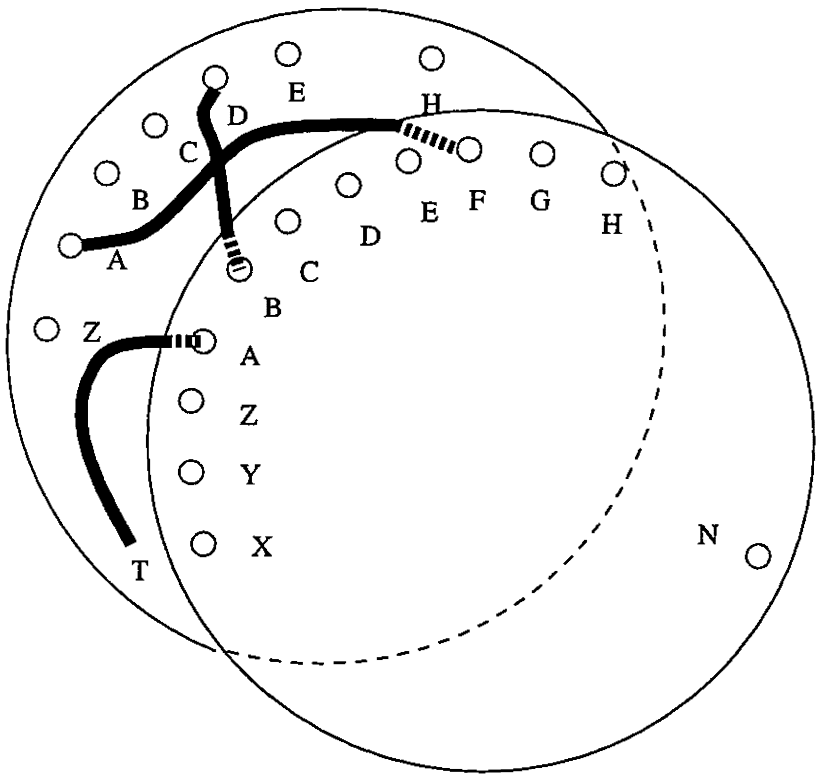
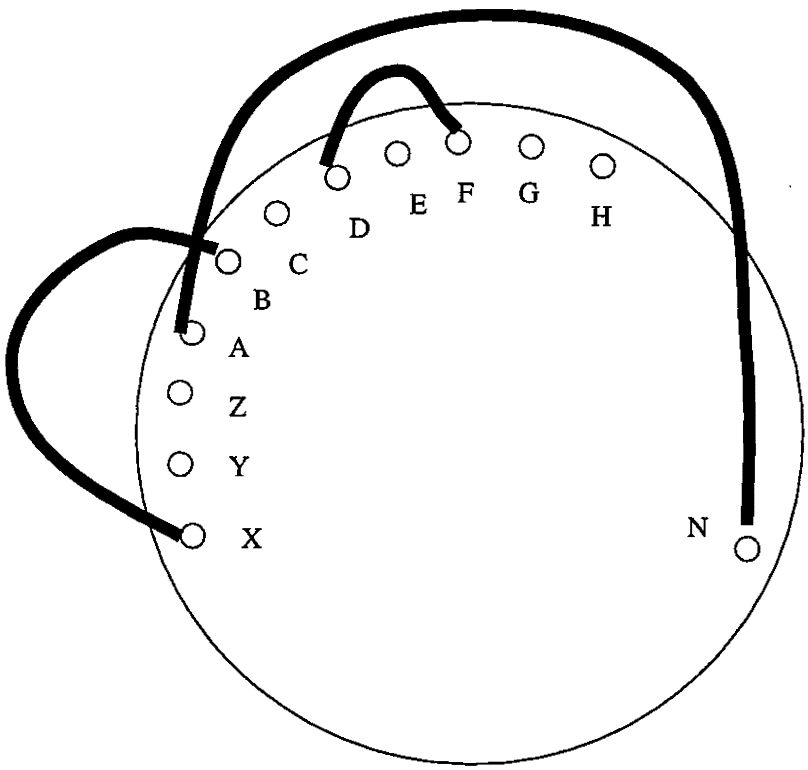


Figure B.3: Inside the Reflector



Bibliography

[1] C. A. Deavours. *Breakthrough '32: The Polish Solution of the Enigma.* Aegean Park Press, Laguna Hills, California, 1988.

[2] Józef Garliński. *Enigma War.* Scribner & Sons, New York, 1980.

[3] I. N. Herstein. *Topics in Algebra.* John Wiley & Sons, second edition, 1975.

[4] David Kahn. *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943.* Houghton Mifflin Company, Boston, Massachusetts, 1991.

[5] Wladyslaw Kozaczuk. *Enigma: How the German Cipher Was Broken, and How It Was Read by the Allies in World War II.* University Publications of America, Inc., 1979. English-language translation by Christopher Kasparek, 1984.

[6] Douglas R. Stinson. *Cryptography: Theory and Practice.* CRC Press, Inc., Boca Raton, Florida, 1995.