Mathematics and War

Bearbeitet von
Bernhelm Booss-Bavnbek, Jens Høyrup

1. Auflage 2003. Taschenbuch. vIII, 420 S. Paperback
ISBN 978 3 7643 1634 1
Format (B x L): 17 x 24,4 cm
Gewicht: 1630 g

The Brains behind the Enigma Code Breaking before the Second World War

Elisabeth Rakus-Andersson*

The German Enigma encoding machine and the contributions of famous cryptologists who broke it are still topics that fascinate both scientists and the general public. After the monarchy of Kaiser Wilhelm II fell, the Weimar republic came into being, and the idea of equipping the armed forces with machine ciphers already found realization in 1926. The German cipher machine, called Enigma, alarmed the general staffs of neighbouring countries, especially Poland and France. This work describes the efforts of cryptanalysts who solved the mystery of Enigma during the 1930s before the beginning of the war.

1 Introduction

In the late 1920s, everything indicated that the small Reichswehr would be converted into a modern million-man army. All the German political parties that came to power voted on the same program, which had as the main assumption to take away from Poland some districts regarded by the German government as "lost territories". The military build-up program of the German army forces had to involve the development of secret intelligence operations [Kozaczuk 1984, Garliński 1999]. These operations always belonged to two categories, namely, cryptography ("secret writing") and cryptology (the study of secret writing, especially for purposes of decryptment – "the breaking" or "reading" of secret correspondence by the third party).

Cryptology deals basically with ciphers, which either transpose (shift) or substitute letters for the original letters in a message, and with codes, which replace entire words and phrases by arbitrary symbols commonly consisting of letters and numbers [Kahn 1967, Kozaczuk 1984].

Rather early the German army commanders realized that they should introduce a cryptography device that was both secure and could satisfy the requirements of speed and convenience. In spring of 1918, the German Navy contemplated the use of cipher machines. The inventor Hugo Koch designed the "Enigma" machine in Holland in 1919 and sold the patent later to Dr. Arthur Scherbius. Scherbius could improve Koch's design and hoped to win the market for this machine in the busi-

* Blekinge Institute of Technology, Department of Health, Science and Mathematics, S-37179 Karlskrona, Sweden. E-mail: Elisabeth.Andersson@bth.se

ness world, but his best customer would be the German government, especially the armed forces [Kozaczuk 1984, Garliński 1999]. In 1926 the navy, and in 1928 the army, introduced cipher machines that at first were modified versions of the civilian model "Enigma" [Kozaczuk 1984, Gaj 1989]. Two years later, in 1930, a military version of the device was constructed. In 1933–34, the Germans adopted Enigma as a basic, unitary cipher system for the armed forces as well as military intelligence (the Abwehr), S.S. formations, the Nazi Party security and Political Intelligence Service (S.D.).

Cryptologists could easily recognize an Enigma cipher by its perfect spread of letters. There were no correlates with natural languages, and the statistical calculations of frequencies of the letters were completely useless.

It was not strange that the Polish authorities were the most engaged of all countries in solving the German coding system. The other German neighbours, such as France or England, were not threatened by German actions to the same degree as Poland. The Polish cryptologists found the solution of the Enigma secret before the war began, and this story shows the historical background of progress made by Polish mathematicians.

2 The Cryptology Course in Poznań

The general staffs of the neighbouring countries were alarmed by the German machine cipher, and cryptologists, who received some messages from the monitoring stations (placed in Poland in Warsaw, Poznań, Starogard and Krzesławice) set to work on breaking the code [Kozaczuk 1967].

There were few persons skilful at cryptology in Poland at this time. At the General Staff's Cipher Bureau in Warsaw, specialists were trained and distinguished from the clerks who enciphered and deciphered messages. The German ciphers and codes monitored by the Poles were only partially intercepted, which gave a reason for educating the cryptologists and equipping them with all necessary knowledge about the ciphers.

The need for organizing the course in cryptology was justified by the actual political situation. In the first days of January 1929, the students at Poznań University's Mathematics Institute were preparing for their final examinations in mathematics, where the examiner was Prof. Zdzisław Krygowski. He had already prepared a list of those third- and fourth-year mathematics students who knew German and had marks of at least "good" in their course work. Afterwards the selected students were asked to assemble at the Institute, where two officers from the Polish General Staff in Warsaw, Major Franciszek Pokorny and Lieutenant Maksymilian Ciężki informed them that a cryptology course was organized and invited them to participate in it [Kozaczuk 1984, Gaj 1989, Sebag-Montefiore 2000]. The students who chose the course were pledged to secrecy concerning both the existence of the course and their participation in it. The lessons were held twice a week in the evenings and conducted by Cipher Bureau cryptologists commuting from Warsaw.

After several weeks of the course, the lecturer presented authentic Reichswehr ciphergrams for the students to solve. This system had already been broken and the Germans called it Double Dice [Kozaczuk 1984, Garliński 1999]. A couple of hours later, three students: Marian Rejewski, Henryk Zygalski and Jerzy Różycki (Fig. 1, 2, 3) presented their solutions. These three students, as the best ones, continued working on cryptology in the underground basements of the Command Post in Poznań.

Figure 1.
Marian Rejewsk in 1944.[1]

Figure 2.
Jerzy Różycki in 1933.[1]

Figure 3.
Henryk Zygalski in 1941.[1]

This work was a kind of laboratory that gave a broad opportunity for experimentation. The mentioned team of skilled students, engaged in cryptology work, did not read long dispatches but tried to work out methods of breaking German cipher keys, which were changed periodically. Radio intercepts were delivered by courier from Warsaw and from the nearest monitoring station in Poznań while the solutions were sent to Warsaw by airplane.

Solutions of some non-mechanical military German ciphers became a matter of routine. The cryptologists learned to exploit the mistakes made by the German cipher clerks as well as certain regularities they discovered. One of these was a rule that a cipher text must contain at least fifty letters. Thus every message sent by the Germans had the letter X added to enlarge the text to fifty signs.

The discovery of such rules made it easier to solve the cipher problems. But strange things began to happen, namely, the enciphered information was sent without any stable rules at all, and all the doubts disappeared – this was a complicated machine cipher inaccessible for standard methods of breaking.

[1] From [Garliński 1999]

3 The Enigma

The Poznań cipher office was closed in the summer of 1932. The main purpose for the course in cryptology and for the primary work with reading German messages, which were monitored by the Polish radio network, was to find talented students and train them in working on the new German machine cipher [Hodges 1983, Kozaczuk 1984].

The fact that the Polish authorities turned to mathematicians could have been partially explained by the great development of the Polish mathematical school at that time. Marian Rejewski, who had spent a year in Göttingen for studies, felt that the famous German school of mathematics belonged to the past. Among those professors he had met in Germany were no such outstanding persons as Poland's Stefan Banach and Wacław Sierpiński whose work had such great importance for twentieth-century mathematics [Kuratowski 1980]. The achievements made in mathematics in Poland at the beginning of the twentieth-century instilled a strong belief in the power of the subject. The members of the Polish government, who represented Poland as a new state with rather poor resources after World War I, realized that all intellectual possibilities should have been utilized in the service of the country.

On 1 September 1932, Marian Rejewski, Jerzy Różycki and Henryk Zygalski began working as regular employees at the Cipher Bureau in the general staff building (the "Saxon Palace") in Warsaw [Kozaczuk 1976, 1984, Bauer 2002]. The efforts undertaken during the years 1928–1930 to solve the new machine cryptosystem led nowhere. However, the three mathematicians got a different problem to solve during their first weeks in the General Cipher Bureau, namely, to break the four-letter German naval code [Kozaczuk 1984].

From a dozen short messages, one was selected for closer study. It consisted of only six groups, each of four letters. After thorough analysis the mathematicians noticed that the letter Y occurred at the beginning of a large number of code groups. In German, many question expressions (Wer?, Wo?, Wohin?, Wann?, Welcher?) begin with the same letter, and this regularity could have been present in the code. Next, they noticed that, following this six-group message, another station sent on the same wavelength a short signal consisting of only four signs. By assuming that the first message was a question, they guessed that the second might be an answer. Such a short reply could be a number, maybe a year. The question-answer system was recognized with a possibility that the answer could be a date, e.g., a year. The solution of this six-word signal led to the gradual reconstruction of the entire German naval code used in the second half of 1932. Even after fifty years, Marian Rejewski remembered that YOPY meant "when", YWIN – "where", BAUG – "and", and KEZL – "cancel the final letter".

The Polish mathematicians could read most of the messages in navy code even if the Germans tried to make them difficult. They transposed the alphabetical order, omitted certain letters of the alphabet, or from time to time remitted false code groups.

Even if the effects concerning the navy code were very apparent, the Enigma remained unsolved. The attempts were made to solve the mystery included the mathematicians' efforts as well as the predictions of clairvoyants. One of the preliminary findings was formulated as: "If we write two cipher texts with identical beginnings one below the other, identical letters in the same places will occur in the average twice as often as when we place texts with different beginnings in the same manner".

The work on Enigma required great concentration and at least eighty intercepts per day. Marian Rejewski obtained a commercial Enigma machine used by business firms. The machine resembled a typewriter, with an additional panel built into the lid. The panel contained twenty-six little circular glass windows having, like the keyboard, the letters of the alphabet. A number of glow lamps were built in the panel underside. Inside the machine was a set of three rotors, or rotating drums, and a reversing drum, all sitting on the common axle. The machine had also a stationary drum, called the entry ring. With every stroke of a key one or more rotors rotated, and at the same time the corresponding glow lamp lit up and illuminated the letter in the window above it. The machine was designed in a way that allowed finding the association between the plain text and the cipher. If one struck the key with the letter coming from the clear text, then a corresponding cipher letter would appear in the window. Conversely, when another person tapped out a cipher text, the letters illuminated in turn would spell the plain text. In order to conduct a secret dialog, both parties had to possess the same device set [Kozaczuk 1984].

The commercial Enigma only provided the general insight into the construction of the machine. It was easy to guess that the military version of Enigma would probably have a different wiring system and additional components. The cryptologists had to continue studying the system from the mathematical side. They needed group theory [Kozaczuk 1984, Freedman 2000], especially the properties of permutation groups, which were very useful when working on the military Enigma.

4 International Cooperation

France and Czechoslovakia, like Poland, were threatened by German expansionism. They also were natural allies for Poland in collecting knowledge about German devices and war plans. In 1932, a man in France initiated contacts with the Polish General Staff. Captain Gustave Bertrand, chief of French radio intelligence established a direct cooperation with the Poles, especially for work resulting in solutions of the Enigma problem [Bertrand 1973, Kozaczuk 1984].

In October 1932, French military intelligence made a great contribution to solving the Enigma mystery, thanks to a special opportunity. A French intelligence officer Captain Henri Navarre reported that a man came to him and introduced himself as an employee of the Reichswehr cryptography agency [Bertrand 1973, Garliński 1999, Sebag-Montefiore 2000, Bauer 2002]. Moreover, he offered his services in return for money. Captain Bertrand, who was responsible for techni-

cal and scientific intelligence and ciphers, checked carefully all the information collected about the German agent and decided to investigate the first documents, which the man delivered. The samples were recognized as authentic. The newly recruited agent Hans-Thilo Schmidt received the pseudonym "Asche". The documents delivered by "Asche" were both original and of great importance. During the long cooperation with Captain Bertrand, who met the German collaborator regularly, "Asche" left the following reports [Kozaczuk 1977, 1979, 1984]:

- Materials of the organization of the Reichswehr Cryptographic Agency;
- Various codes used in the German armed forces: A, B, C, D, E and code "Black";
- Documents concerning keys to manual ciphers used by civil staff and army signals service for quick contact between civil and military authorities;
- Documents on machine ciphers: operating instructions for Enigma, keying instructions and monthly tables of army keys for December 1931, 1932, 1933 and the first half of 1934;
- Materials on an earlier Enigma model from 1930 and a document including one cipher text and a corresponding plain text.

Unfortunately, "Asche" never had an opportunity to get into his hands the most important materials such as the dossier of Enigma, containing the scheme of the machine's wiring.

After receiving the first materials, which threw a new light on the Enigma mystery, Captain Bertrand contacted the Polish Cipher Bureau and arranged to visit Warsaw [Bertrand 1973, Kozaczuk 1984]. The materials he came with awoke a great interest among the cryptologists, because they constituted the first written papers referring to Enigma. Even if the Polish cryptologists had worked on the Enigma cipher since 1927, they had only intercepts as the base of their investigations.

Bertrand described his first meeting with the Poles on 7–11 December 1932 in Warsaw as "historic", and he did not exaggerate when he used this word [Bertrand 1973]. The meeting gave rise to a long and friendly cooperation between Polish and French intelligence specialists. During the Warsaw meeting in December 1932, a number of tasks were decided between Bertrand and his Polish colleagues. The head of the Polish Cipher Bureau, which had been reorganized a year earlier, was Major Gwido Langer. The French were to concentrate on delivering intelligence reports from Germany to help in the code breaking, while the Poles were responsible for theoretical studies of Enigma intercepts. It was also decided to establish closer connections with the intelligence unit in Czechoslovakia in order to create a triple entente of cryptological services. Captain Bertrand (Fig. 4) was to use the pseudonym "Bolek", Major Langer – "Luc", and the Czechoslovak officer – "Raoul". In the later 1930s, the B-L-R triangle was active on the Bolek–Luc line, due to the deteriorated Polish–Czech relations prevailing at that time [Kozaczuk 1976].

It is worth emphasizing that the principle of very strict secrecy was introduced into the Polish–French contacts, and even the three Polish cryptologists – Rejewski, Zygalski and Różycki – did not know anything about the origin of delivered

Figure 4.
General Gustave Bertrand in 1940.[2]

materials. These played an important role in the studies on Enigma in conjunction with the mathematical analysis, which had already been carried out on the intercepts.

The instructions brought by Bertrand gave a general idea of the military Enigma's appearance and operating principles, but said nothing about its inner structure. The electrical connections within the rotors, the variable contacts and other components were still unknown. If one of the last mentioned elements had been missing, then the entire effort would have given no results.

5 Breaking the Enigma System

The precise mathematical analysis was combined with intuitive reconstruction of individual parts. As the following example shows, even knowledge about the German mentality helped in solving the posed problem. Rejewski had found that in the commercial Enigma the letters of the alphabet were represented on the circumference of the entry ring in the same order in which they appeared on the German typewriter keyboard. It was assumed that the military model had its entry ring organized in the same way as the commercial model, but that assertion was wrong. Further, in January 1933 he came to the conclusion that the wiring on the entry ring in the military Enigma was in alphabetical order. The hypothesis was proved to be correct and helped to designate the connections in one of the rotors. The belief in German Ordnung ("order") made the work faster and simpler [Rejewski 1980-2].

[2] From [Kozaczuk 1984].

Solution of the Enigma system involved two distinct matters:
The theoretical reconstruction of the cipher machine was done. The most important task was to determine the Enigma's wiring. The cryptologists first discovered functions of the reflector, or "reversing drum". Afterwards, they reconstructed all the connections in the machine, which had a system of rotors as essential components. Even a special commutator was built into the system. The Poles were able to construct exact replicas of Enigma.

Secondly, the cryptologists developed methods for reconstructing the Enigma keys on the basis of intercepts that were supplied daily by monitoring stations.

The main code break came in the last days of December 1932. The practical reading of messages began during the second ten days of January 1933.

At the beginning of February 1933, the Cipher Bureau ordered the AVA Radio Manufacturing Company in Warsaw to build fifteen replicas of the military Enigma [Kozaczuk 1984]. The machines had to be made of the same components and with identical wiring, to work in the same way as the original military machine known to the German cipher staff as E-Eins [Sebag-Montefiore 2000]. The AVA copy model had typing keys instead of caps, and the upper part of the machine was changed as well. The illuminated windows were covered with cellophane on which the letters were written in the appropriate order.

The first attempt to produce a replica of Enigma was a failure. The cipher text going through the machine resembled some exotic language, but not German. The mathematicians discovered soon that the producers had forgotten about the capital letters, which slipped over the keys only for reading signals. This altered the order of internal connections. The mistake was corrected soon and AVA kept building more copies [Kozaczuk 1984].

A few weeks after the first copies of Enigma were constructed, the cryptologists received a series of German military signals, which indicated a correspondence between the district number 1 in Königsberg and number 2 in Stettin. The messages were unreadable and all the methods to translate them became useless. This cipher was sent on another Enigma machine called Enigma II. Later, it was discovered that it was the ordinary Enigma equipped with eight rotors and an automatic writing device. It had been used only for sending the highest military commands and had been evaluated as unreliable. After several weeks this version of Enigma was withdrawn from use.

Recovery of the settings (starting positions of rotors) and keys to the messages in the various Enigma nets happened by the method of elimination. The connections in the commutator were found by using the lattice method. During the first months after the Enigma solution, further elements of the key were obtained manually, by turning the metal rotors as many as 17576 ways. For top secrecy, the mathematicians did the job by themselves without any help from their assistants. One must add that the Germans changed the connections of the commutator regularly and more and more often, which forced an additional effort in finding the new conditions. The situation was improved when Rejewski invented a cyclometer, which had two sets of Enigma rotors linked together electrically. The cyclometer enabled the cryptologists to create a catalogue of possible settings of the rotors. After that, the comparison of intercepts with the catalogue made it possible to recover the keys faster [Hodges 1983, Kozaczuk 1984].

Other inventions included a clock, devised by Jerzy Różycki, that determined the right position of one of the rotors on a certain day in a given Enigma net.

In late June 1934, the three mathematicians experienced the exciting decryptment of a transmission they could read as "To all commandants of the airfields throughout Germany". The signal ordered "the transportation to Berlin, alive or dead, of Karl Ernst, adjutant to S.A. chief".

Thus 1934 was the year when the cryptology team of the Polish Cipher Bureau broke the ciphers of the German Army (Heer) and the codes of S.D. as well as codes and ciphers of the German Navy. The Kriegsmarine used three kinds of Enigma keys: operational, staff and admirals. The last key was resistant to breaking for a long time [Kozaczuk 1984].

6 Devices as a Reaction for Changes of Enigma Settings

The struggle against the German machine cipher had not ended in 1933, with the solution of Enigma and the building of its copy. In order to read the messages of the German Army, Air Force, and Navy, it was not enough to break the system once. The changes in it had to be detected and the reaction had to follow as well. Since the numbers of intercepts were growing proportionally to the Wehrmacht's expansion, several Polish lieutenants and captains were sent to the Cipher Bureau for training.

By the beginning of 1936, the Germans were using six kinds of keys to Enigma machines which were intended use by the supreme civil authorities: the staffs of the Armed Forces, the Army, S.S. staffs, S.S. operational units, special situations (the key "A"). The precautions and the secrecy concerning Enigma were growing in Germany as the war approached. The Germans carefully kept records of machine starting positions to prevent repetition of the same combinations. From 1 October 1936, they changed the settings every day. The responses to these changes from the Polish side resembled a duel between Poland's Cipher Bureau and Nazi Chi-Dienst (the German Cryptological Service). Three periods could be recognized in this battle [Kozaczuk 1984].

In the first period, 1933–35, little "changes" were made by the Germans, and the apparatus that had been developed by the Poles was sufficient for continuous decryptment.

In the second period from 1936 to November 1938, each change came very fast and to keep pace with them, the Polish cryptologists had to use all their knowledge and experience while they worked with the same tools and resources.

In the third period from the late 1938 to September 1939, a new wartime generation of Enigmas appeared with further complications.

Once the luck was on the Polish side, when German cipher clerks had committed great errors. They had often selected message keys (the first six letters at the beginnings of messages) in a stereotypic manner. For example, they could strike the same letter three times (AAA) or they could strike letters in alphabetical order (ABC). There was another possibility that they could use letters that lay next to each other down or diagonally across the keyboard, which was against regulations.

The cycle principle discovered by Marian Rejewski let him distinguish the proper regular message keys from the chaotic ones, which were introduced by mistake [Rejewski 1980-1, 1980-2, Hodges 1983, Kozaczuk 1984, Gaj 1999, Bauer 2002].

In 1937, important changes were made in the Polish Cipher Bureau. Its German section, B.S.-4, was separated from headquarters and moved out of the city. In the specially constructed new buildings hidden in woods not far from Pyry in the south of Warsaw, working conditions were better than at the cramped quarters in Warsaw. Another purpose in moving the German section with its cryptologists was to better protect the secrecy of their operations. The Abwehr carefully tested all people who were suspected of being traitors, and the secret German agents were present everywhere.

At the Polish B.S.-4, a strict prohibition was introduced against talking to anyone, even to fellows from the Cipher Bureau, about Enigma [Woytak 1979].

The Polish General Staff ordered an experiment to be carried out in January 1938. The test was to show how many of the intercepted Wehrmacht ciphers the cryptologists could read. The results of tests, which were conducted during two weeks, showed that about 75 percent of the messages had been decrypted.

7 French and English Efforts in Breaking Enigma

During these years Captain Bertrand visited the Polish Cipher Bureau many times. Expecting the approach of war it was important to ensure communication in the Warsaw-Paris-Prague triangle. After visiting the new nest of the Polish cryptologists in Pyry, which was called Wicher (Wind), Bertrand went to Prague to speak to representatives of the Czechoslovak General Staff, which even in May 1938 still looked to the future with hope.

In France, Bertrand's services were occupied with non-machine ciphers, leaving Enigma to the Poles [Kozaczuk 1979]. The French cryptologists were able to read the secret radio correspondence from Germany and Italy as well as from other countries. The French intelligence services also spread false information about French codes and ciphers, and in this way the Germans got "the mobilization code" of France's military intelligence while the Italians got the French B.D.G. naval code. During the war, the false information that was transmitted in these codes by the allies caused many damages and defeats for the Fascist countries. In Rotterdam one could buy various codes and ciphers, risking spending a lot of money for nothing, and even Captain Bertrand visited this exchange using the pseudonym Victor Hugo.

After the annexation of Austria by Germany in 1938, the British began to show more interest in intelligence contacts with their future allies. Bertrand was invited to London, where for the first time he met the British cipher experts. He came with Asche's papers that he gave to the British [Bertrand 1973]. The British cryptological service in the 1930s was part of the Foreign Office and contained some military sections. Officially known as the Government Code and Cipher School, or G.C.C.S., it was also called Room 47 of the Foreign Office until 1939 [Calvocoressi

1977, Hodges 1983, Kozaczuk 1984, Gaj 1989, Freedman 2000]. Afterwards it was called Station X or Bletchley Park. The chief of the G.C.C.S., Commander Alastair Denniston, was a professional naval intelligence officer. He successfully worked at breaking German codes and ciphers in the famous Room 40 at the Admiralty during the years 1914–18. The chief cryptologist at G.C.C.S., Alfred Dillwyn Knox, had been a worker of Room 40 during World War I. In the middle of the thirties, G.C.C.S. worked hard on breaking the German machine cipher, but failed to make progress. Knox managed, likely in 1938, to solve the cipher of General Franco's Army based on the commercial version of Enigma, but the military Enigma still was a riddle. The lack of success with the military Enigma in England could be attributed to the shorter time of investigation when compared with the Poles, and less mathematical effort involved in their analysis.

The British were rather reserved towards Bertrand's proposals to join forces with the French and Polish intelligence sections.

8 The Bombe as a Response for Further Changes in the Enigma System

The international situation became severe and nobody had doubts anymore that Germany would prepare more and more aggressive plans directed towards their neighbours. Suddenly, on 15 September 1938, two weeks before the Munich conference, the Germans altered the rules for enciphering message keys used by the twenty thousand Enigma machines. Now, the Enigma operator himself could select the basic position, a different one each time when he sent a message.

The Polish mathematicians, who met the difficulties in their work every day, thought of constructing a device that was more efficient than the cyclometer and could take over the long calculations. In October 1938, Marian Rejewski invented the mathematical model of an aggregate, which was left to designers in AVA.

The bombe, as the device for recovering Enigma's daily keys was christened, was a true invention [Hodges 1983, Kozaczuk 1977, 1979, 1984, Sebag-Montefiore 2000, Bauer 2002]. This was an electro-mechanical aggregate based on six Polish Enigmas combined with additional devices and transmissions. An electrically driven system of rotors turned round automatically, creating in each bombe 17567 different combinations of letters within two hours. When the rotors were placed in the sought-for position, a light appeared, the motors stopped automatically, and the cryptologist read the indications. By setting the bombes in action (in November 1938), the daily keys could be recovered within two hours. Almost at the same time, the B.S.-4 worked out a method for breaking the doubly enciphered individual message keys, which were formed according to the changes of the Enigma system introduced in September 1938. The new Polish method was based on using a special series of perforated paper sheets with a capacity of fifty-one holes by fifty-one. Each series consisted of twenty-six sheets. Theoretically, the method was based on so-called females, that is, on manipulating the sheets to match the coinci-

dent places in the pre-programmed system. Designed mainly by Henryk Zygalski, the system was quite independent of the number of connections in the German Enigma's commutator [Hodges 1983, Sebag-Montefiore 2000].

The Germans were cautious and once again changed the Enigma ciphers on 15 December 1938. This time the change involved not operating procedures but components. The Germans introduced two additional rotors per device, raising the number from three to five [Hodges 1983, Kozaczuk 1984, Freedman 2000]. This innovation, combined with the new keying procedure, made the process of decryptment almost impossible to continue with. The costs of further operations with further Enigma breaking seemed to be too high for the Polish government.

9 A Gift for the Allies

At the beginning of 1939 the Polish General Staff decided to broaden its exchange of information on Enigma with possible allies. The constant connection was already established with the French staff, but the French still did not know that Enigma had been solved in 1932 and that the replicas had been created. General Bertrand wrote in his book, published in 1973, that Enigma had been broken in Poland in 1939 [Bertrand 1973]. Since the Polish concept of the solution was kept as a close mystery, the French became impatient and weighed the possibility of arranging a common meeting with French, Polish and British representatives. Bertrand hoped that such a meeting would improve the Polish-British contacts that were rather cool [Bertrand 1973]. At the end of 1938, Bertrand succeeded in organizing the meeting in Paris, where top officers of the cryptological services were present. Before, Bertrand had to make a trip to London in order to persuade Commander Denniston of the need of taking part in the meeting. Denniston did not believe that anything new could be expected in Paris. He had never been in touch with the Polish cryptologists and did not imagine that they could have any achievements with Enigma.

This first meeting with British representatives took place on 9–10 January 1939 in Paris, at the French Military Intelligence offices. Major Bertrand, Captain Henri Braquenié from the air force staff and an army staff officer represented the French. Three British experts and the Poles – Colonel Gwido Langer and Major Maksymilian Ciężki – were the other members of the meeting.

At the Paris meeting it was agreed that the next conferences would be held in Warsaw and London if something new would come to light.

The principle of the highest security about the development of work on Enigma was observed in contacts between Poland and its French and British allies. The Poles did not leave any decrypted messages to their foreign partners up to the summer of 1939. Only summaries about the German armed forces were exchanged. Close contacts in radio intelligence between Poland and France did not mean sharing the secrets of cryptological methods.

But the great moment came. In July 1939, Bertrand received a telegraphed invitation from Gwido Langer (Luc) with words "there is something new..." [Ber-

trand 1973]. During the evening on 24 July, an international meeting was held in Warsaw and Langer informed his French and British colleagues that not only Enigma's secret had been penetrated but also the machine itself had been reconstructed. The French would receive one copy, the British another. The next morning all the participants of the Warsaw meeting drove to the new B.S.-4 place in the Kabackie Woods. A working meeting took place and the reconstructed Enigma was shown. Marian Rejewski said about himself and his colleagues: "We showed and told them everything what we knew about Enigma". Besides Denniston and Knox, who participated in the meeting, there was another person coming from England. It was possible that the Deputy head of the British military intelligence, Colonel Steward Menzies, appeared incognito as a "Professor Sandwich", a mathematician from Oxford [Rejewski 1980-2].

After seeing the Polish Enigma replica, Denniston and Knox wanted to contact London at once to order engineers and electricians to come down. It was unnecessary because Langer told them that it would be a machine each for Paris and London. The two Enigma machines soon arrived in Paris in diplomatic luggage. The perforated sheets with instructions for using were also enclosed. On August 16 Bertrand, accompanied by a British diplomatic courier, took one of the machines to London and at Victoria Station personally handed it to Colonel Menzies [Bertrand 1973, Kozaczuk 1984, Gaj 1989, Freedman 2000, Sebag-Montefiore 2000, Bauer 2002]. A few days later Knox sent greetings to the three Polish mathematicians, which included the words in both Polish and English: "My sincere thanks for your cooperation and patience. A.D. Knox".

10 The Mathematical Solution of Enigma

The applications of mathematics to cryptology expanded rapidly with the introduction of cipher machines. The use of permutation theory, combined with other methods of cryptological analysis, contributed to the breaking in Poland in 1932/33 of the German machine cipher, Enigma. The description of some examples, giving insight into Enigma decrypment, is based on two available reports written by Marian Rejewski, which can be found in the Sikorski Historical Institute in London and the military Historical Institute in Warsaw respectively. Other sources of information are Rejewski's publications which appeared in 1980 [Rejewski 1980-1, 1980-2, Kozaczuk 1984].

Description of the machine

Enigma was a device that was used for the mechanical encipherment of plain texts.

It had a twenty-six-letter keyboard and, behind it, a panel with twenty-six letters illuminated by glow lamps, which were placed under them. The main ciphering components were the three cipher drums or rotors and a fourth stationary reflector or reversing drum. All the rotors sat on the common axle. The reversing drum could be moved towards or away from the rotors with a lever. The machine

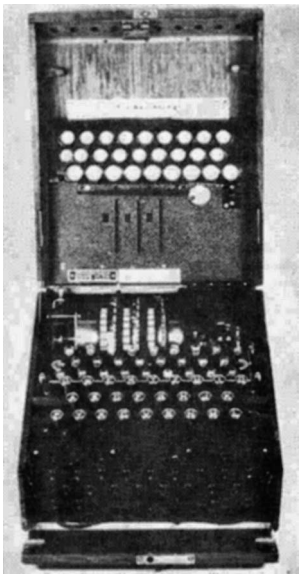

Figure 5.
General view of the military model Enigma.[3]

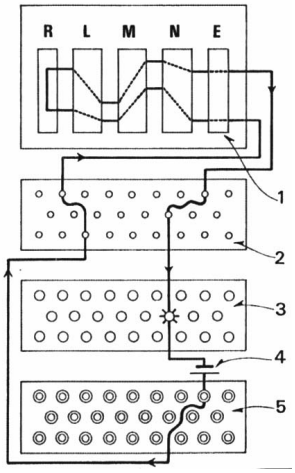

Figure 6.
The path of electric current through Enigma's components. 1: rotors (E: entry ring, L, M, N: main rotors, R: reversing drum), 2: commutator, 3: lamps, 4: battery, 5: keyboard.[4]

was also equipped with a stationary entry ring, which constituted the link between the commutator and the right rotor [Rejewski 1980-1, 1980-2, Deavours 1981].

The three rotors had the letters of the alphabet placed about their rims. The letters were visible in the little windows in the lid. Each rotor had twenty-six fixed contacts on one face and twenty-six spring-loaded contacts on the other. The reversing drum had only spring-loaded contacts connected in pairs on one face. The connections in four rotors constituted the most important part of the ciphering system and the secret of Enigma. Even the organization of connections in the entry ring was a great mystery, and the discovery of that secret by Rejewski at the beginning of 1933 constituted one of the greatest contributions in the work on the machine. The entry ring had the letters connected up in alphabetical order. These connections did not cause any relevant action of the entry ring.

The commutator was in front of the keyboard. Six pairs of plugs connected with wires made possible the interchange of twelve among the twenty-six letters of the alphabet.

The depression of an Enigma key caused the right-hand rotor to rotate through one twenty-sixth of the whole circumference. At the same time, the circuit was closed and current ran from the depressed key through the commutator, the entry ring, all three rotors that moved by rotating a bit, the reversing drum, and back through the rotors, and once again through the commutator. A glow lamp lit under one of the letters, which was always different from the depressed key (Fig. 6). Conversely, if someone struck the key, which was lightened before, a previously depressed letter would appear in the windows with light. The Enigma was constructed both for writing plain texts in order to obtain cipher and, conversely, to transform ciphers into clear messages. When one depressed the successive letters of a plain text, the letters of the bulbs that lit formed the cipher.

[3,4] From [Garliński 1999]

Encipherment procedure

Sending a message, the German clerk first set the rotors in the basic position established for that day and changed the letters in the commutator by placing the plugs in the appropriate sockets. Then he selected the individual key for that message, three letters he enciphered twice. In this way he obtained six letters, which were placed at the opening of the message. Next, he set the rotors to the selected individual key and began to encipher the message. The individual keys for a given day thus had two characteristics: the unknown basic position, and an unknown key for the message, which was enciphered twice. We realize that the first sign meant the same thing as the fourth one, the second was identified with the fifth and the third was compared to the sixth. Let us denote these pairs by AD, BE and CF [Rejewski 1980-1, 1980-2, Bauer 2002]. If we have about eighty messages per day, then all the letters of the alphabet can occur in the keys on the six places. We know from the machine's description that, when we strike a given key, for example "x", the lamp "y" is to be lit. Then, conversely, striking the "y" key will cause the "x" lamp to light. It is thus concluded that the permutations A through F consist of transpositions. Every pair of letters included in the same transposition has one letter coming from the plain text, while the other represents the cipher being associated with the first letter. For instance, the unknown permutation A is expected to be a set of pairs of the type:

$$A = (as)(br)(cw)(di)(ev) \ldots (zu).$$

If the encipherer strikes in the first place the unknown key "x" and obtains the letter "a", and by striking in the fourth place the same key "x" obtaining the letter "b", then, by striking in the first place the "a" key, he would obtain the letter "x", and by striking in the fourth place the "x" key, he would obtain the letter "b". Thus, there occurs a successive action, first of "a" on "x", and then of "x" on "b". The execution of such operations is called the composition of permutations. If we write the letters "ab" next to each other we will produce a fragment of the permutation AD, which is a product of unknown permutations A and D.

The cryptologists wrote out separately the six first letters of all the messages from a given day, more precisely, their twice enciphered keys. They chose the arbitrary key and wrote down its first letter, and next to it the fourth. Then they looked for the key, which had as its first letter the fourth letter of the previous key and they wrote the first letter of the second key beside the fourth letter of the first key. They continued seeking for such a key (the third one) that began with the fourth letter of the second key and so on. After a number of steps they returned to the first letter in the first word.

Let us consider the following example. Let

dmq vbn
von puy
puc fmq

designate the chosen openings, that is, the doubly enciphered keys of three of some eighty messages available for a given day. From the first and the fourth letters we can see that "*d*" becomes "*v*", "*v*" becomes "*p*", "*p*" becomes "*f*". In this way we obtain a fragment of a permutation *AD* "*dvpf*". Similarly, from the second and the fifth letters we notice that "*o*" becomes "*u*", "*u*" becomes "*m*" and "*m*" becomes "*b*". We obtain a fragment of the permutation *BE* as "*oumb*". And lastly, we get "*c*" which becomes "*q*", "*q*" which becomes "*n*" and "*n*" which becomes "*y*". Hence, the permutation *CF* begins with "*cqny*". The openings of other messages would permit the complete assembly of the set of permutations *AD*, *BE* and *CF* to appear. For example, *AB*, deciphered from the daily openings was a permutation:

$$AD = \begin{matrix} d\ v\ p & & o\ e\ i\ j & & t\ b\ c\ r\ w\ a\ s \\ \downarrow\ \downarrow\ \downarrow & \ldots & \downarrow\ \downarrow\ \downarrow\ \downarrow & \ldots & \downarrow\ \downarrow\ \downarrow\ \downarrow\ \downarrow\ \downarrow\ \downarrow \\ v\ p\ f & & d\ i\ j\ m & & e\ c\ b\ w\ r\ a\ s \end{matrix} = (dvpfkxgzyo)(eijmunqlht)(bc)(rw)(a)(s)$$

while

$$BE = (blfqveoum)(hjpswizrn)(axt)(cgy)(d)(k)$$

and

$$CF = (abviktjgfcqny)(duzrehlxwpsmo).$$

The set of permutations for *AD*, *BE* and *CF* was called "the characteristic set for a given day". We remember that the permutations contain the enciphered letters without any close connections with the plain text. We wish to separate the permutations *A* through *F*, which, instead, present the associations between the clear text and the cipher.

In the solutions, some theorems were involved. Let us quote the most important of them.

Theorem 1
If two permutations X and Y of the same degree comprise disjunctive transpositions, then their product XY will include disjunctive cycles of the same lengths in even numbers.

We may also prove the converse theorem.

Theorem 2
If a permutation includes disjunctive cycles of the same lengths in even numbers, then the permutation may be regarded as a product XY of two permutations X and Y, composed of disjunctive transpositions.

Analysing the permutation *AD* we can evaluate its contents as two cycles of the length 10, two cycles of the length 2 and two cycles of the length 1.

It may also be shown that:

Theorem 3
Letters entering into one and the same transposition of permutation X or Y, enter always into two different cycles of the same length, which belong to the permutation XY.

The theorems quoted above helped to determine the connections between the plain text and the corresponding cipher. Let us assume that the German clerks had some habits when they arbitrarily created the openings of messages. Suppose, e.g., that the encipherer liked to select three identical letters, such as "*aaa*", "*bbb*" and the like. Since in product *AD* the letters "*a*" and "*s*" form single-letter cycles, then "*a*" and "*s*" should belong to the same transposition (*as*). It means that the plain letter "*a*" has the representing cipher letter "*s*".

Suppose that the enciphered message keys from a given day begin with the letter "*s*":

sug smf
sjm spo
syx scw.

Only the last key starting with "*syx*" could arise from the plain text "*aaa*", for the transposition (*as*) has one representative in the cycle (*a*) and the other in (*s*) – both belonging to *AD*. By analysing the transposition (*ay*), representing the second place of the key, we realize that "*a*" belongs to the cycle (*axt*) while *y* is placed in (*cgy*). Both cycles come from the permutation *BE*. At last, the pair (*ax*) tracing the third position in the key has "*a*" in (*abviktjgfcqny*) and "*x*" in (*duzrehlxwpsmo*). The cycles are parts of the permutation *CF*. Even the strict analysis of the second part in the third message key proves that "*scw*" are ciphers of "*aaa*" according to the rule of double ciphering.

By using the sets *AD*, *BE* and *EF*, when collecting them during a few days, the mathematicians managed to construct the internal connections of the machine.

The set of equations

The unknown permutations *A* through *F* were also found as solutions of the equation set. After a key has been depressed, the current first passes through a series of the machine's components to light a lamp with the letter at last. Each of these components causes a permutation of the alphabet. We denote the permutation caused by the commutator by the letter *S*, the permutations created by the rotors (from right to left) have initials *N*, *M*, *L*, and the permutation caused by the reversing drum is called *R*. Since the letters of the entry ring were linked in alphabetical order, then the permutation *H*, associated with the ring, would be the identity without any relevance. The path of the current will be represented by the product of permutations $SNMLRL^{-1}M^{-1}N^{-1}S^{-1}$, where the sign "–1" denotes an inverse permutation. We also keep in mind that the depression of the key causes a movement of the first right rotor that rotates a bit equal to one twenty-sixth of the circumfer-

ence. This movement creates the next permutation in which each letter is assigned to the next one. We denote the last permutation by P and write it down as

$$P = \begin{array}{cccccc} a & b & c & & z \\ \downarrow & \downarrow & \downarrow & \ldots & \downarrow \\ b & c & d & & a \end{array} = (abcdef \ldots xyz)$$

The unknown permutations A–F are represented in the form

$$A = SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}S^{-1}$$
$$B = SP^{2}NP^{-2}MLRL^{-1}M^{-1}P^{2}N^{-1}P^{-2}S^{-1}$$
$$\ldots$$
$$F = SP^{6}NP^{-6}MLRL^{-1}M^{-1}P^{6}N^{-1}P^{-6}S^{-1}$$

and the AD, BE and CF products have the presentations

$$AD = SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{3}NP^{-4}MLRL^{-1}M^{-1}P^{4}N^{-1}P^{-4}S^{-1}$$
$$BE = SP^{2}NP^{-2}MLRL^{-1}M^{-1}P^{2}N^{-1}P^{3}NP^{-5}MLRL^{-1}M^{-1}P^{5}N^{-1}P^{-5}S^{-1}$$
$$CF = SP^{3}NP^{-3}MLRL^{-1}M^{-1}P^{3}N^{-1}P^{3}NP^{-6}MLRL^{-1}M^{-1}P^{6}N^{-1}P^{-6}S^{-1}.$$

In the set of equations derived above, only the permutation P and its powers are known. By discovering the connections in the drums it was possible to reconstruct the associated pairs "plain text-cipher" in the permutations A–F, which gave a possibility to read the messages during only one day.

The material above, shown as an excerpt from the large documentation of the Enigma description, allows us to understand better the machine construction as well as to realize that enormous efforts were undertaken to break the Enigma's code.

Epilogue

As the title suggests, the first part of the Enigma story, based only on the collected facts, ended in July 1939. After some weeks the war broke up. The British code-breakers at Bletchley Park received an Enigma machine and rotors I to V from the Polish Cipher Bureau on 24 July, 1939. The British recovered rotors VI and VII from the crew of U-33 on 12 February 1940, while rotor VIII was captured in August 1940. In May and June 1940, using clear text and cipher text captured from Schiff 26, Hut 8, a section at Bletchley Park had solved some April Enigma traffic with the aid of the first British bombe. Both the bombe, which was Alan Turing's great device, and further investigations during the war leading to the construction of the computer prototype, constitute a great amount of information, which ought to be discussed separately in another paper.

At the beginning of the war, the three Polish cryptologists were forced to leave the country and to escape, at first to Romania and France and then to England. In 1946, Rejewski returned to Poland from England, where he spent the last years

Figure 7. Leading Polish army officers were present at a ceremony in 2001 when a memorial plaque was unveiled at the tomb of the cryptologist Marian Rejewski (1905–1980). The photo shows some generals, together with Rejewski's daughter and the President of the Polish Mathematical Society. Not many mathematicians have experienced similar honours in life or posthumously.
As a mathematics student, Rejewski had been recruited in 1929 by the Cipher Bureau of the General Staff of the Polish Army. Rejewski then created a mathematical method for breaking the German Enigma code of that time. Long before their competitors, the Polish Cipher Bureau officers realized the potential of mathematics in cryptological research.

of the war. He had worked as a clerk until he retired. In 1980 he died in Warsaw. Zygalski decided to stay in England. He had taught mathematics at the Battersee Technical College before he died in 1978. Różycki was killed during the catastrophe of a French ship in 1942.

The early Polish contributions in the Enigma solution enabled the British codebreakers to make great progress in the further development of methods breaking the Enigma code already in 1940. There is no doubt that the successful effort to break Enigma shortened the war and spared many human lives.

References

Bauer F. L. (2002): *Decrypted Secrets. Methods and Maxims of Cryptology.* Springer Verlag, Berlin-Heidelberg-New York 2002.

Bertrand G. (1973): *Enigma ou la plus grande énigme de la guerre 1939–1945*, Libraire Plon, Paris 1973.

Calvocoressi P. (1977): The secrets of enigma. *The Listener* **20**, (1977), p. 27.

Deavours C. A. (1981): Comments to "How Polish Mathematicians Deciphered the Enigma" by Marian Rejewski. *Annals of the History of Computing* **3** (1981), pp. 229–234.

Freedman, M. (2000): *Unravelling Enigma. Winning the Code War at Station X*. Published by Led Cooper, Barnsley 2000.

Gaj K. (1989): Szyfr Enigmy – metody złamania. Wydawnictwo Komunikacji i Łączności, Warsaw 1989.

Garlinski J. (1999): Enigma – tajemnice drugiej wojny światowej. Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 1999.

Hodges A. (1983): *Alan Turing: The Enigma*. Simon and Schuster, New York 1983.

Kahn, D. (1967): *The Codebreakers*, Macmillan, New York 1967.

Kozaczuk W. (1967): Bitwa o tajemnice. Książka i Wiedza, Warsaw 1967.

Kozaczuk W. (1976): Złamany szyfr. Wydawnictwo Ministerstwa Obrony Narodowej, Warsaw 1976.

Kozaczuk W. (1977): Wojna w eterze. Wydawnictwa Radia i Telewizji, Warsaw 1977.

Kozaczuk W. (1979): W kręgu Enigmy. Książka i Wiedza, Warsaw 1979.

Kozaczuk W. (1984): *Enigma: how the German machine cipher was broken, and how it was read by the Allies in World War Two*. University Publications of America 1984 (Translation of W kręgu Enigmy).

Kuratowski K. (1980): *A Half-Century of Polish Mathematics: Remembrances and Reflections*. Pergamon Press, Oxford 1980.

Rejewski M. (1980-1): An application of the theory of permutations in breaking the Enigma cipher. *Zastos Mat*. (*Applicationes Mathematicae)* **16** (1980), no. 4, pp. 543–559.

Rejewski M. (1980-2): Jak matematycy polscy rozszyfrowali Enigmę. *Wiadomości Matematyczne* **23** (1980), pp. 1–28.

Sebag-Montefiore H. (2000): *Enigma – The Battle for the Code*, Weidenfelt & Nicolson, London 2000.

Woytak R. (1979): *On the Border of War and Peace: Polish Intelligence and Diplomacy in 1937–1939 and the Origins of the Ultra Secret*, Columbia University Press, New York 1979.