Foreign Intelligence Agency

Serving Poland in the shadows

Enigma was an electromechanical encryption machine that used both the electrical properties and mechanical components for polyalphabetic encryption. Its most important components were the encryption rotors, rotating on a single axis.

The decisive factor in the Enigma’s creation was the purchase of patent rights to another rotary encryption machine developed nine years earlier by Dutch engineer Hugo Koch by Artur Scherbius, a German engineer, the designer of his own rotary encryption machine and co-founder of the Scherbius & Ritterwas electrical equipment factory, in 1928. This transaction brought revolutionary changes in the encryption equipment market and in the field of cryptology. The Enigma quickly gained the recognition of buyers, which resulted in numerous orders, thanks to which it found its way to mass production.

The commercial success and effectiveness of the Enigma, which at that time was mainly used to encrypt German commercial correspondence, also attracted the interest of the German army and intelligence services, which, after a painful defeat during World War I, were working on the creation of an “ideal” encryption device. After modifying its construction and principles of operation, these institutions introduced it to use in their cipher communication. It affected its neighbouring countries, which since then had lost the ability to decipher German messages.

British and French cryptologists repeatedly tried to break the German code, but their efforts ended in failure each time. Discouraged by the constant failures, they finally stopped further attempts, considering the Enigma to be a machine which is impossible to be worked out.

Beginning of work on breaking German ciphers

At the beginning of work on breaking German ciphers, Poles, unlike other nations, were afraid of Germany’s expansive policy, and were motivated to work on this country’s cipher system and, above all, they believed that thanks to their ingenuity, intelligence and effort it would be possible to break the key used in it. For centuries it had been widely believed that the best specialists in this field are linguists and people with linguistic skills. However, Polish experts decided to apply non-standard methods of work, based on the knowledge and mathematical skills of selected graduates of Polish universities who knew German. At the beginning of 1929, in search for talented candidates for a secret cryptology course, the intelligence of the Second Republic of Poland addressed Professor Zdzisław Krygowski, a lecturer at the Institute of Mathematics at the University

of Poznań, for help in their selection (it was no coincidence that a university located in the Prussian partition was selected, where knowledge of German was common). The students indicated by him – 20 mathematicians – participated in classes conducted by Major Franciszek Pokorny, Lieutenant Maksymilian Ciężki and engineer Antoni Palluth. Out of this group, only three mathematicians were engaged by the Cipher Bureau of the Second Division of the General Staff of the Polish Army. The most talented scientist was Marian Rejewski, a fairly short, modest and prudent young man, described by his friends as a “shy four-eyes”. The other two were his university friends, Henryk Zygalski and Jerzy Różycki. At the same time, Gwido Langer, a modern technology enthusiast, came to Warsaw from Vilnius, first as the head of the radio intelligence unit and then as the head of the Cipher Bureau, transforming it into a well-functioning structure. Thanks to him, the person who played an important role in the activities of the German section of the Cipher Bureau was Antoni Palluth, who purchased a civilian copy of the Enigma, allowing research on the device.

The photos show a copy of the Enigma used during World War II. The device is currently stored in the Foreign Intelligence Agency.

First successes of Polish cryptologists

A breakthrough in the work on the Enigma was possible thanks to the close cooperation between the Polish and French intelligence services. The French handed over to Warsaw copies of materials concerning the military version of the Enigma, received from the German cipher Hans Thilo Schmidt, who worked for them. In return, Poles were to share with Paris the possible effects of using the information provided. This data allowed them to construct an exact copy of the Enigma. However, it was still not enough to read the German messages. Finally, thanks to the materials brought to Warsaw on December 8, 1932 by Captain Gustav Bertrand, Gwido Langer’s counterpart serving in French intelligence, Polish cryptologists managed to decrypt the cryptograms for the first time, using the Enigma, in the Saxon Palace in Warsaw, where the headquarters of the Cipher Bureau was then located, just before the New Year,

on December 31, 1932. The success came just in time, as political changes took place in Germany at the beginning of 1933, as a result of which Adolf Hitler gained power. In this context, improving and increasing the effectiveness of the work of cryptologists from the German section, who had only one copy of the reconstructed Enigma at their disposal, became particularly important. For this reason, the second division of the General Staff commissioned the “AVA” Radio Engineering Plant in Warsaw, headed by Leonard and Ludomir Danielewicz as well as Edward Fokczyński and Antoni Palluth (amateur radio enthusiasts), to develop further models of this device. A dozen or so copies of the Enigma were created, used by the Cipher Bureau as early as in 1934.

Development of decryption techniques

Germans systematically modified the design and operation principles of the Enigma device. Every modification resulted in a response from Polish cryptologists who came up with inventive and efficient methods of breaking the code and decrypting messages. Their work resulted in, among other things, a device constructed in 1936 called a cyclometer which enabled the cryptologists to obtain the current Enigma code within minutes. Consequently, in September 1938, when German specialists kept introducing subsequent innovations concerning Enigma design and operation, M. Rejewski and his friends created a device called Rejewski’s bomb which allowed them to break Enigma codes automatically. What was unique about the bomb was the fact that it was based on exceptional mathematical concepts, such as the theory of cycles. In order to help to determine the sequence of enigma coding rotors perforated paper sheets were used, designed by H. Zygalski and called Zygalski’s sheets.

On the brink of the World War II

On 25-27 July 1939 the second meeting with the

representatives of the British and French intelligence services took place in Warsaw.

The first meeting was organised in January 1939 in Paris and was devoted to possibilities of breaking the Enigma cipher. It was then agreed that the next meeting was to be held only if any of the involved parties obtained new information regarding the encryption device. At that time, none of the Polish representatives revealed the information that Poles had been reading German Enigma encrypted wires for six years. However, the situation in Europe had been changing so dramatically from January till July 1939 that Poland decided to share this secret with the Allies and give them one copy of the Enigma device as well as a set of "Zygalski's sheets" and "Rejewski's Bombs".

During the second meeting in July 1939 France was represented by Major Gustave Bertrand and Captain Henri Braquenié. The representaives of the British intelligence were, among others, Commander Alastair Denniston, the head of the Government Code and Cypher School in Bletchley Park, Alfred Dillwyn "Dilly" Knox, the top British cryptologist and Prof. Humphrey Sandwich, a radio monitoring intelligence specialist.

On July 25th 1939 the representatives of the French and British intelligence were invited to the Polish decryption facility in Pyry. The guests received Enigma decrypting devices manufactured by "AVA" company. During their visit the allies were familiarised with methods of obtaining keys to encrypting devices. Additionally, Lt Col G. Langer demonstrated how to perform a decryption of a German secret wire sent from the SS Command. On this particular day the Poles decided to share with the allies the secret that had been protected for many years. Both delegations were also presented with a copy of the Enigma device together with materials necessary for operating the machine. Having learnt about the results of Polish cryptologists' work, the French and the British were astonished by their level of advancement which was unattainable for the allies at that time. The devices were shipped to the recipients by sea, which was considered the safest option at that time. On the basis of the information obtained from the Poles, the British immediately launched a project aimed at creating a cryptographic facility in Bletchley Park. The scientists who began their studies concerning the German coding system started arriving there as early as August 1939. One of them was Alan Turing, a mathematical genius, whose work concentrated on

developing his own methods of decryption. Over time the cryptologists from Bletchley Park managed to take almost full control over German codes and were able to decode the wires sent between all types of German armed forces and they often could read them sooner than the rightful recipient.

The text is based on AW own archives as well as available publications, including:

J. Garliński, *Enigma. Tajemnica drugiej wojny światowej,* Londyn 1980.

B. Johnson, *Sekrety drugiej wojny światowej. Wojna mózgów. Tajne badania naukowe i ich zastosowanie w czasie drugiej wojny światowej,* trans. M.Wasilewski, Poznań 1997.

W. Kozaczuk, *W kręgu Enigmy,* Warszawa 1979.

Marian Rejewski 1905-1980. Życie Enigmą pisane, ed. S.Ciechanowski et al*.,* Bydgoszcz 2005.

Further reading:

M. Baldwin, *Wprowadzenie do ENIGMY. Wykład wygłoszony z okazji 65. rocznicy spotkania kryptologów polskich i alianckich w Lesie Kabackim (Pyry k. Warszawy),* 1939; Zdzisław J. Kapera translated and provided an introduction of the lecture, Kraków-Mogilany 2004.

M. Grajek, *Odnaleziony raport – czego nowego dewiedzieliśmy się o historii złamania Enigmy?,*[w:] *Enigma bez tajemnic. 85. rocznica sukcesu polskich kryptologów,* ed. idem. Toruń 2020, p. 41-57.

Z.J. Kapera, *Stan badań nad polską Enigmą 1932-1942,* [w:] *Wkład polskiego wywiadu w zwycięstwo aliantów w II wojnie światowej. Akta konferencji naukowej zorganizowanej w Krakowie w dn. 20-22.10.2002 r. przez Polską Akademię Umiejętności, Muzeum Armii Krajowej, Towarzystwo Obrony Zachodnich Kresów Polski i Instytut Historii Uniwersytetu Jagiellońskiego*, red. idem, Kraków 2004, p. 13-26.

M. Rejewski, *Jak matematycy polscy rozszyfrowali Enigmę*, "Wiadomości Matematyczne" R.XXIII 1980, p. 1-28.

M. Rejewski, *Wspomnienia z mej pracy w Biurze Szyfrów Oddziału II Sztabu Głównego 1930-1945*, Poznań 2013.

Sztafeta Enigmy. Odnaleziony raport polskich kryptologów, editing, elaboration and texts translation by M.Grajek, Warszawa

2019.