Anna BOROWSKA
Bialystok University of Technology

THE ENIGMA M3 - THE CONTRIBUTION OF POLISH MATHEMATICIANS IN THE VICTORY OVER THE THIRD REICH

Abstract: *The subject of this paper is the Enigma M3 and its cipher, used by the German military and government services just before and during the Second World War. Section 1 contains an overview of codes used before cipher machines were introduced. Section 2 contains a full description of the M3 (including the introduced changes), elements of the cipher key, and instructions for preparing messages. Section 3 provides the mathematical model of the Enigma M3 cipher as well as an example of a message that could have been sent before September 15, 1938. Section 4 defines the size of the cipher key space, on which the security of messages was dependent. The following section presents the history of cryptanalysis of the M3 cipher, which from 1932 to 1940 was the task of three Polish mathematicians, namely Marian Rejewski, Jerzy Różycki, and Henryk Zygalski.*

Key words: *M3 Enigma machine, cryptanalysis, Zygalski's sheets method, cryptologic bomb method, catalogue method*

Operation Enigma is described by historians as «the greatest secret of the Second World War after the atomic bomb[1]*» The fact that the Enigma cipher was broken by Polish mathematicians already in December 1932 was first revealed by W. Kozaczuk*[2] in 1967. Regular access to secret reports, orders, and other encrypted messages of the Armed Forces of the Third Reich sent from strategic-level radio networks, Hitler's headquarters, the Operational and Tactical Commands of Wehrmacht, SS, SD, diplomacy and other resorts in 1939–1945 contributed significantly to the definite victory of the Allies over Nazi Germany[3].

[1] D. Kahn, "Enigma Unwrapped", *New York Times Book Review*, 29.XII.1974.
[2] W. Kozaczuk, *The Battle of Secrets. The Intelligence Services of Poland and the German Reich 1922–1939*, Warsaw 1967.
[3] K. Gaj, *The Enigma Cipher. The Method of Breaking*, Warsaw 1989, p. 7.

1. Development of ciphers before the Second World War

The origins of cryptography can be traced back to the ancient times when shorthand, among other methods, was used to hide secret messages by means of various techniques, e.g. by masking the secret message in irrelevant text. Methods for disguising information, which are still known, were Caesar cipher and the scytale method. Throughout centuries, two types of cipher were used for disguising messages, i.e. substitution ciphers and transposition ciphers. Substitution ciphers consist in replacing individual letters or groups of letters with other individual letters or groups of letters. These are monoalphabetic (e.g. affine cipher), homophonic, and poly-alphabetic (e.g. Hill cipher, Vigenère cipher) ciphers. Transposition ciphers consist in changing the order of letters in a text. In the 19th century, electromechanical machines, the telegraph, and the radio began to be used for encryption and decryption[4]. These devices considerably improved the development of cipher studies. Among the more well-known ciphering machines are the German Enigma, the Japanese Purple, the German Lorenza, the American SIGABA, the British Typex, and the Polish Lacida. These machines were used mainly for protection of military and diplomatic information, but similar devices were used commercially as well[5].

2. Construction of the M3 Enigma machine

The Enigma M3 is a combination of two systems, electrical and mechanical. Its simplified scheme and an example electric circuit is shown in fig. 1(B). and a rotating mechanism. Its main elements are a 26-character alphabetic keyboard (2),

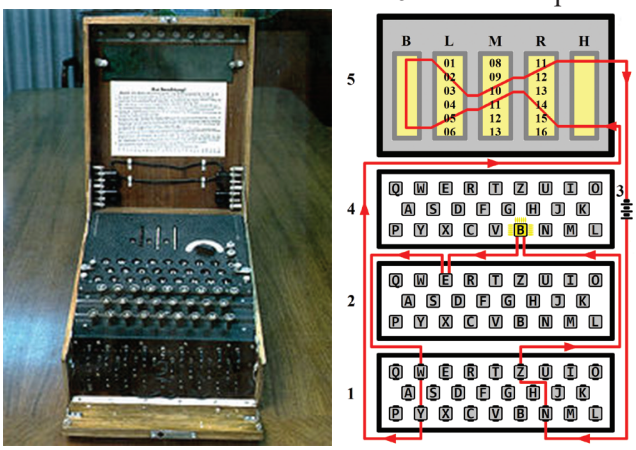

Fig. 1. (A) The Enigma M3[6], (B) The diagram presents how the M3 Enigma works[7]

a set of 26 light bulbs (4), a set of 3 movable ciphering drums (L, M, R) on a common axle, stationary drums (H), i.e. the entry wheel (B) and the reflector (B),

[4] J. Pieprzyk, T. Hardjono, J. Seberry, *Fundamentals of Computer Security*, Gliwice 2003, pp. 18–19; D. R. Stinson, *Cryptography. Theory and Practice*, Warsaw 1995, pp. 3–20.
[5] K. Gaj, op. cit., p. 8.
[6] Wikipedia, *Enigma*, http://pl.wikipedia.org/wiki/Enigma (07.01.2017).
[7] K. Gaj, op. cit., p. 51.

a plugboard (1), a battery (3),

Pressing any key (e.g. «E») results in completing an electric circuit. Then, current flows through various components in the present configuration, through the connection under the pressed key, the plugboard, and successively through the entry wheel (H), the three drums R, L, M, to the reflector (B). The reflector returns the signal via drums L, M, and R (but using a different route). Then the current flows through the entry wheel, to the plugboard, and finally to the appropriate bulb (representing a letter different from «E»), causing it to light[8].

All movable drums are disc-shaped (fig. 2(B)). Inside each of them there is a rotor. On the right side of the rotor (on the rim) there are 26 brass spring pins and on the left side there are 26 flat electrical contacts. The contacts and the pins (on both sides) represent the 26 letters of the alphabet. Inside the rotor there are 26 insulated wires, which connect in an established way (different for each of the drum type) the contacts on one side of the drum with the pins on the other. As the drums are arranged side-by-side on a common axle, the pins of a drum touch the electrical contacts of the neighbouring drum, forming 26 fragments of an electric circuit[9]. A movable ring with numbers corresponding to the 26 letters of the alphabet engraved on its external surface is imposed to each of the rotors. One position on the rim of the rotor is defined as the so-called zero position. The ring setting is represented by the letter on the ring (or number, in the military version) opposite to the said position. The individual types of ciphering drums also differ from their so-called turnover positions. The turnover positions of the five types of drums (denoted by I, II, III, IV and V) used in Land and Air Forces were as follows: I-Q, II-E, III-V, IV-J, V-Z[10].

Three different drums were assembled in position L, M and R in the M3. Until December 15, 1938, 3 drums from the set {I, II, III} were selected. They gave 3!=6 various settings. Later, two drums, IV and V, were added. Still, three different drums were selected, but from the set {I, II, III, IV and V}. Five drums gave 60 different settings.

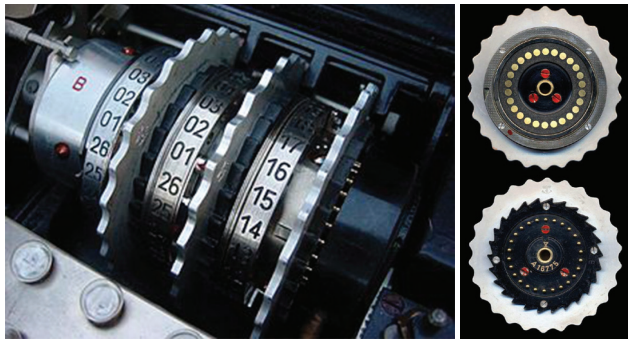

Fig. 2. (A) Assembled set of the drums. Three movable drums between two stationary drums(the entry wheel and the reflector), (B) Left and right side of the ciphering drum[11].

[8] Ibidem, p. 51.
[9] Ibidem, p. 48.
[10] Ibidem, p. 53.
[11] Wikipedia, *Enigma*, http://pl.wikipedia.org/wiki/Enigma, (07.01.2017).

The output contacts of cipher drums I, II, III, IV and V[12].

	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
I	E K M F L G D Q V Z N T O W Y H X U S P A I B R C J
II	A J D K S I R U X B L H W T M C Q G Z N P Y F V O E
III	B D F H J L C P R T X V Z N Y E I W G A K M U S Q O
IV	E S O V P Z J A Y Q U I R H X L N F T G K D C M W B
V	V Z B R G I T Y U P S D N H L X A W M J Q P F E C K

The connections of the entry wheel of the Enigma M3 are represented by the identity permutation[13]. The reflector (reversal drum) pairs the outputs of the last rotor, redirecting the current back through the drums using a different path.

The real internal connections of reflectors UKW A (until November 2, 1937) and UKW B (onwards)[14]:

UKWA(AI)(BM)(CE)(DT)(FG)(HR)(JY)(KS)(JQ)(NZ)(OX)(PW)(UV)

UKWB(AY)(BR)(CU)(DH)(EQ)(FS)(GL)(IP)(JX)(KN)(MO)(TZ)(VW)

Pressing any Enigma key results in the right drum rotating by 1/26 of the full angle before the circuit is closed. When it reaches the turnover position, the middle drum also rotates by 1/26 of the full angle, and when the middle drum reaches its turnover position, the left and middle drums rotate[15]. In this way, each subsequent letter is ciphered at a different drum position.

The position of each movable drum is represented by the letter (or number, in the military version) engraved on the ring and visible through the window set in the metal cover of the machine. The fundamental position of the drum (i.e. the rotor position) is the difference between the position of the drum and the ring setting.

The plugboard consists of 26 pairs of sockets and plugs (one pair for each of the letters). Connecting the socket of one pair with the plug of another (and inversely) with a cable, causes that two letters of the alphabet are changed both before and after the signal passes through the ciphering drums[16].

In order to encrypt plaintext by means of the Enigma, the machine must be set according to the daily key and the plaintext must be typed on the keyboard. After pressing any key, e.g. «E», a certain another letter is lighted up. Cyphertext is obtained by recording the sequence of highlighted letters.

The machine's settings for a given month were delivered to each of the units that were using the Enigma in the form of daily key tablets. A daily key (until September 15, 1938) consisted of the following elements: a selection of three

[12] K. Gaj, op. cit., p. 64–65.
[13] Ibidem, p. 96.
[14] Ibidem, p. 67.
[15] Ibidem, p. 53–54.
[16] J. Garliński, *Enigma. Mystery of the Second World War*, Lublin 1989, p. 236.

drums, their order on the axle, ring settings, plug connections, and the initial drum settings[17].

«Since September 15, 1938, the Germans changed the manner of announcing message settings. Starting with this date, the operator was forced to choose his own arbitrary three letters, which he placed in the headline of the message without ciphering (these letters played a role of the initial drum settings). Next, he set the drums to these letters and chose three other letters as the message settings. These letters after two-time coding, were placed at the beginning of the message and then the drums were set to the message settings and the actual ciphering of the message began[18]».

In order to decrypt plaintext encrypted by means of the Enigma, the machine must be set exactly as it was set during encryption and then the cyphertext must be typed in. The structure of the cipher guarantees that the text consisting of the sequence of letters highlighting during entering is indeed the initial message.

The section above is an overview mainly based on publications[19].

3. Mathematical description of the Enigma M3

How the Enigma cipher works can be explained on the basis of the mathematical concept of permutation. If X = {1, 2, …, n} is an n-element set, then a one-to-one transformation of the set X into itself is called a permutation[20] of X.

Let **P** = {A, B, ..., Z} denote a set of possible plaintexts. The Enigma M3 used by the German Land Forces encrypts plaintext T with a polyalphabetic cipher, transforming any letter p from the set according to the following permutation[21]:

$$L = SH(Q^{z}RQ^{-z})(Q^{y}MQ^{-y})(Q^{x}LQ^{-x})B(Q^{x}L^{-1}Q^{-x})(Q^{y}M^{-1}Q^{-y})(Q^{z}R^{-1}Q^{-z})H^{-1}S^{-1}$$

S is a permutation describing the plugboard transformation (S consists of transpositions and 1-cycles only). B is a permutation describing the reflector transformation (B consists of 13 transpositions). L, M, R are permutations describing transformations of the three cipher drums. H is a transformation of the entry wheel (H is the identity permutation). Q = (A, B, C, D, …, W, X, Y, Z) is a cycle of length 26. Variables x, y, z are positions of rotors (left, middle and right) before any key is pressed (x, y, z are numbers from 0 to 25 corresponding to the letters from the set P).

A message generated with the use of the software written by the author that could have been created in the period before September 15, 1938 is shown below.

- ✓ the text: ABCDEFGHIJKLMNOPQRSTUVWXYZ;
- ✓ the daily key settings (the order of drums I, II, III, ring settings ZHL,

[17] Ibidem, p. 237.
[18] M. Rejewski, "How did Polish Mathematicians Decipher the Enigma", *Polish Mathematics Association Yearbooks*, Series 2nd: Mathematical News, vol. 23, 1980, pp. 22–23.
[19] K. Gaj, op. cit.; M. Rejewski, op. cit.; M. Grajek, L. Gralewski, *The Birth of Mathematical Cryptology*, Toruń 2009, M. Rejewski, *Memories of my Work at the Cipher Bureau of the General Staff Second Department 1930–1945*, Poznań 2013.
[20] A. Mostowski, M. Stark, *Elements of Higher Algebra*, Warsaw 1970, pp. 34–39.
[21] K. Gaj, op. cit., p. 93.

initial drum settings YNC, connections of the plugboard (BY)(CX)(EO)(HV)(KR)(PZ));

- ✓ the message key: ASD;
- ✓ the message: LIO IWN YISVIWKOUBZKHEHCCNYKWHTMZI.

4. Security of the Enigma M3 cipher

The security of the Enigma cipher depended on the size of the key space. The size of the key space of the Enigma M3 is expressed by formula

$$K = N_{Do} \cdot N_{Rs} \cdot N_{Ds} \cdot N_{Ps} \cdot N_{Ms},$$

where N_{Do} is the number of possible orders of drums, N_{Rs} is the number of ring settings, N_{Ds} – the number of possible initial drum settings, N_{Ps} – the number of plugboard settings, N_{Ms} is the number of possible message keys.

From[22] January 1, 1939 to November 16, 1939 k = 5 and n = 7–10. For, example for n = 10 we have $K = 60 \cdot 26^3 \cdot 26^3 \cdot 150\,738\,274\,937\,250 \cdot 26^3$ possible keys.

5. History of decryption of the Enigma M3

In 1919, Hugo Koch, a Dutch constructor, designed a cipher machine called Geheimschiffriermachine. He sold his patent to dr Artur Scherbius, a German engineer, who significantly modified the device and started its manufacture (by Scherbius & Ritter). The machine called Enigma was intended to secure commercial secrets in the big industry and trade. Various versions of the same device were used during and before the Second World War, e.g. in Germany, Italy, Spain, or Switzerland. However, the most important users (since 1926) of the machine were the German Armed Forces. The machines manufactured for military purposes differed in construction from the commercial versions. What is more, changes were introduced from time to time both to the method of encryption and the device itself (e.g. on December 15, 1938 two additional rotors were introduced; on September 15, 1939 the method for conveying initial settings of the drums was changed). The reason for the changes was to eliminate successful attempts at breaking the cipher. Nearly until the end of the war, the German command-in-chief treated the Enigma cipher as absolute. On the basis of opinions of experts from special committees, they precluded any effective decryption. The Germans were convinced that even if the enemy came into possession of a military Enigma unit, then not knowing the key, they would be unable to decipher any message. On the other hand, the fact that the Allies could decipher German messages was Ultra secret information.

The Polish military intelligence noticed that the German Land Forces were using a machine cipher already in 1928, but the attempts at deciphering intercepted messages in Poland were fruitless. In 1929, on the request of the General Staff of the Polish Armed Forces, a cryptography course for the best students fluent in German was organized at University in Poznań. On September 1st, 1932 the three

[22] Ibidem, p. 69.

most cryptographically gifted graduates of the course (Marian Rejewski, Jerzy Różycki, and Henryk Zygalski) were employed in the Cipher Bureau (the B.S.-4) in Warsaw. The mathematicians' task was to break the Enigma cipher. It should be emphasized that similar unsuccessful attempts were being made by intelligence services in France and Great Britain.

In December 1932, M. Rejewski finished reconstruction of the internal connections of all Enigma elements. At the beginning of 1933, the three mathematicians first deciphered the latest German messages intercepted by radio. M. Rejewski summarises his and his colleagues' work from that period in the following way[23]: «Thus, the result of the work accomplished during the course of merely a few months can be summarized as follows:

1.Reconstruction of the German military cipher machine Enigma.

2.Finding a method for the daily reconstruction of the message keys.

3. Finding a method for reconstructing the daily keys».

The French intelligence service had an agent in Germany (codename «Asché») employed in the German Cipher Bureau. The documents obtained from the agent were transferred by the French intelligence service to the Polish Cipher Bureau. These materials helped, but were not the decisive factor in the successful breaking of the cipher by M. Rejewski.

From then until 1939, the Polish Armed and Governmental Forces had access (without knowing the source) to credible and reliable secret information about the Third Reich. Messages intercepted in the years 1933–1939 were transferred to three cryptologists (M. Rejewski, H. Zygalski, and J. Różycki) working at the Cipher Bureau, who determined the keys for individual Enigma networks. Then the material was transferred to the chiefs of the Cipher Bureau, who decided on the urgency and order of deciphering of the messages. The deciphered material was transferred by the chief of the Cipher Bureau to the appropriate state and military authorities.

The permutations by means of which messages were encrypted were involutions. Therefore, in order to decrypt the messages it was enough to set the Enigma according to the key and enter the cyphertext. The three cryptologists did not participate in deciphering the messages.

Their duties in the Cipher Bureau consisted of breaking daily keys for individual Enigma networks, detecting changes in the manners of generating messages and changes in the Enigma machine construction as well as designing new ways of breaking daily keys. In February 1933 the Polish General Staff ordered constructing 15 Enigma doubles. By the end of August 1939, AVA manufactured about 17 of these. In 1938 an experiment was performed which showed that a 10-person staff of cryptologists and operators of BS-4 is capable of breaking and deciphering 75% of all intercepted Enigma messages.

Until September 15, 1938, elements of the cipher key such as the order of drums, plugboard connections, and the message key could be recreated with the use of the catalogue of characteristics. Since September 15, 1938 the Germans changed the method of providing message keys. The method of deciphering based on the catalogue of characteristics ceased to be useful. In October 1938,

[23] M. Rejewski, *How did Polish Mathematicians ...*, p. 17.

M. Rejewski designed the cryptologic bomb. With the use of the bomb, the result was achieved within about 2 hours (6 bombs were started simultaneously, one for each setting of the three rotors). When the number of drums was increased to 5, finding the key with the use of the bombs ceased to be viable. An obstacle in using the bomb was also the increased number of plugboard connections. Almost concurrently H. Zygalski designed a different deciphering method, the so-called sheets method. Six sets of perforated sheets were made (one set for each order of 3 drums). Each of 3 sets consisted of 26 sheets. Creating such sheets was a very time-consuming task. About 450 holes were cut out in each of them by hand (using a razor). On December 15, 1938 the Germans introduced 2 additional ciphering drums. At this point, 60 cryptologic bombs were needed instead of 6 as well as 60 sets of Zygalski sheets. The Poles had manufactured only one set of sheets.

In the first months of 1939, the Polish General Staff decided to exchange information with the Allies. On April 9th and 10th, 1939 representatives of three cryptologic services, i.e. Poland, France, and Great Britain, met in Paris. The Poles realized that the Allies had not broken the Enigma cipher. Therefore the Poles did not admit that they had been able to read German encrypted messages. In July 1939 another meeting was held. The war was certain. Poles revealed all of their knowledge and abilities to read Enigma.

After the war broke out, BS-4 was ordered to destroy a part of the documentation and equipment. The Cipher Bureau personnel was evacuated to Romania, then the cryptologists were transported to France. The French-Polish radio-intelligence unit «Bruno» was stationed about 40 kilometres from Paris. The three Polish cryptologists were employed there. The British provided the unit with the whole collection of 60 sets of 26 perforated Zygalski sheets. In May 1940, the Germans once again radically changed the mechanism of using Enigma. The French general G. Bertrand wrote *«inhuman efforts and incessant work day and night were needed, in order to overcome this new obstacle: on 20 May decryption was restarted*[24]*»*. In June, 1940, the Italian Armed Forces attacked France from the Alps. The staff of «Bruno» were evacuated to La Ferté Saint Aubin, then to Vensat. After the defeat of France, 15 Poles and 7 Spaniards («Bruno» staff) were transported to Algeria. From Africa the cryptologists returned to France, where in October 1940 they began to work in the «Cadix» centre (maintaining connection with London). There, the Poles no longer worked with the Enigma – it was the task of the British.

The section above is an overview mainly based on publications[25].

1. *The methods of cryptoanalysis of the Enigma cipher*

The most important methods for breaking the Enigma cipher, designed by the Polish cryptologists were the catalogue of characteristics method (in use until September 15, 1938), the cryptologic bomb method, and the method of perforated Zygalski sheets (in use after September 15, 1938). These methods have

[24] K. Gaj, op. cit., p. 24.

[25] W. Kozaczuk, "Enigma – a Brief History", in: K. Gaj, *The Enigma Cipher. The Method of Breaking*, Warsaw 1989; K. Gaj, op. cit.; M. Rejewski, *How did Polish Mathematicians …*, C. Christensen, "Polish Mathematicians Finding Patterns in Enigma Messages", *Mathematics Magazine*, vol. 80, 2007, pp. 247–273.

been described by many historians[26]. The Reader can find the most reliable data in Rejewski's publications[27]. The author recommends especially the Christenson's publication[28].

The first in-depth mathematical and cryptologic analysis of the Enigma cipher was carried out by K. Gaj in his book[29]. The author of this paper also recommends reading the articles[30], in which a full reconstruction of the three aforementioned methods are presented.

References

1. Borowska A., "The Cryptanalysis of the Enigma Cipher. The Catalogue Method. Part 1", *Simulation in Research and Development*, vol. 6, no. 1, 2015.
2. Borowska A., "The Cryptanalysis of the Enigma Cipher. The Catalogue Method. Part 2", *Simulation in Research and Development*, vol. 6, no. 1, 2015.
3. Borowska A., "The Cryptanalysis of the Enigma Cipher", *Advances in Computer Science Research*, vol. 10, 2013.
4. Borowska A., Rzeszutko E., "The Cryptanalysis of the Enigma Cipher. The Plugboard and the Cryptologic Bomb", *Computer Science*, vol. 15, No 4, 2014.
5. Christensen C., "Polish Mathematicians Finding Patterns in Enigma Messages", *Mathematics Magazine*, vol. 80, 2007.
6. Garliński J., *Enigma. Mystery of the Second World War*, Lublin 1989.
7. Gaj K., The *Enigma Cipher. The Method of Breaking*, *Communication and Connection Publishing House*, Warsaw 1989.
8. Grajek M., *Enigma. Closer to the Truth*, Poznań 2007.
9. Grajek M., Gralewski L., *The Birth of Mathematical Cryptology*, Toruń 2009.
10. Gralewski L., *Breaking of Enigma. History of Marian Rejewski*, Adam Marszałek Publishing House, Toruń 2005.
11. Kahn D., "Enigma Unwrapped", *New York Times Book Review*, 29.XII.1974.
12. Kozaczuk W., "Enigma – a Brief History", [w:] K. Gaj, *The Enigma Cipher.*

[26] M. Rejewski, *How did Polish Mathematicians ...*; idem*, Memories of my work ...*; K. Gaj, op. cit., C. Christensen, op. cit., M. Grajek, L. Gralewski, op. cit.; L. Gralewski, *Breaking of Enigma. History of Marian Rejewski*, Toruń 2005., M. Grajek, *Enigma. Enigma. Closer to the Truth*, Poznań 2007.
[27] M. Rejewski, *How did Polish Mathematicians ...*, idem, *Memories of my work ...*
[28] C. Christensen, *Polish Mathematicians Finding Patterns ...*.
[29] K. Gaj, op. cit.
[30] A. Borowska, "The Cryptanalysis of the Enigma Cipher. The Catalogue Method. Part 1", *Simulation in Research and Development,* vol. 6, no. 1, 2015, pp. 5–22, eadem, "The Cryptanalysis of the Enigma Cipher. The Catalogue Method. Part 2", *Simulation in Research and Development*, vol. 6, no. 1, 2015, pp. 23–33, eadem, "The Cryptanalysis of the Enigma Cipher", *Advances in Computer Science Research*, vol. 10, 2013, pp. 19–38, A. Borowska, E. Rzeszutko, "The Cryptanalysis of the Enigma Cipher. The Plugboard and the Cryptologic Bomb", *Computer Science*, 2014, vol. 15, no 4, pp. 365–388.

The Method of Breaking, Warsaw 1989.

13. Kozaczuk W., *The Battle of Secrets. The Intelligence Services of Poland and the German Reich 1922–1939*, Warsaw 1967.
14. Mostowski A., Stark M., *Elements of Higher Algebra*, Warsaw 1970.
15. Pieprzyk J., Hardjono T., Seberry J., *Fundamentals of Computer Security*, Gliwice 2003.
16. Rejewski M., "How did Polish Mathematicians Decipher the Enigma", *Polish Mathematics Association Yearbooks*, Series 2nd: *Mathematical News*, vol. 23, 1980.
17. Rejewski M., *Memories of my work at the Cipher Bureau of the General Staff Second Department 1930–1945*, Poznań 2013.
18. Stinson D. R., *Cryptography. Theory and Practice*, Warsaw 1995.
19. Wikipedia, *Enigma*, http://pl.wikipedia.org/wiki/Enigma, (07.01.2017).