ZUZANA BUCHOWSKA

Department of Polish-AngloSaxon Cultural Relations
School of English
Adam Mickiewicz University, Poznań
zuzana@ifa.amu.edu.pl

ENIGMA: THE TRUE STORY*

Enigma: Bliżej prawdy (Enigma: Closer to the Truth) was written by cryptologist Marek Grajek. The book was published in 2007 and it talks about the deciphering of encrypted radio communication of the German army in the interwar period and during World War II, which had quite a significant impact on the outcome of the War. The messages were ciphered by a German-produced machine called Enigma, hence the title of the book. As the author states in the preface to his work, the popularity of the matter has led to the emergence of a new discipline – enigmology, which combines the fields of history, mathematics, cryptology, and military studies. There have been many publications dealing with the issue, beginning with General Gustave Bertrand's recollections entitled *Enigma ou la plus grande enigme de la querre 1939-1945* published in 1973.[1] Yet, Grajek's book is unique, as it describes the process of the breaking of the Enigma cipher by three Polish cryptologists: Marian Rejewski, Jerzy Różycki and Henryk Zygalski. Although their success has been mentioned in various publications, it was always done in the context of the influence that it had on the outcome of the War. Grajek, on the other hand, focuses on the theoretical and practical breakthrough which led to the deciphering of the code. Furthermore, as the author claims, his work gives an objective view on the later contribution of the French, British and American cryptologists and engineers to the deciphering of the German codes. Grajek's work is also valuable because

* M. Grajek, *Enigma: Bliżej prawdy* (Enigma: Closer to the Truth), Rebis, Poznań 2007. Pp. 691.

[1] G. Bertrand, *Enigma ou la plus grande énigme de la guerre 1939–1945* (Enigma: The Greatest Enigma of the War 1939–1945), Plon, Paris 1973.

he is the first author who has consulted the families of the Polish cryptologists, whose knowledge gives a new insight into many matters.

The author begins the book with information on events which led to the success of the Polish cryptologists. The first chapter focuses on the history of machine cryptography in Europe and on the creation of Enigma as well as its technical details. The author emphasizes the sophistication of the machine in contrast to its predecessors. What follows is a description of Polish deciphering activity, or rather its lack during World War I and the following formation of cryptographic groups in the Polish army. Grajek then moves on to show how the Mathematics Department was formed at the Adam Mickiewicz University in Poznań, and the great influence that Professor Zdzisław Krygowski had on the development of the curriculum of theoretical mathematics and cryptology there. This information is important, as Rejewski, Różycki and Zygalski were students at that very department. Grajek also points to the fact that at that time, the people who were thought to be predisposed to be cryptologists and thus were employed by different armies, were graduates in foreign, especially classical languages. The Polish cryptologists were probably the first mathematicians to be employed to deal with the matter.

What follows is a description of the process of the decrypting of the Enigma cipher. It is described in the context of important historical and political changes that influenced the team's work, such as Hitler's ascension to power. The author also emphasizes the collaboration of the Polish army with the French intelligence services and German agents, who submitted information that helped decipher the codes. The breakthrough – the moment in which Rejewski broke the Enigma cipher – took place between Christmas and New Year's Day of 1932. However, the Polish did not tell the French about their success. Grajek emphasizes the fact that for the first time in history the code of a ciphering device was broken by means of theoretical mathematics, namely the theory of permutations.

Although this was definitely a breakthrough, it was not the end of the team's struggles, as the Germans kept introducing changes to the different elements of the machine, such as the wiring of its ciphering drums. Nevertheless, for several years the cryptologists managed to invent new ways and devices to cope with these changes, for instance the cyclometer. Unfortunately, in December 1938 the German army introduced major changes to the coding of the messages of the most important army units and the Poles were unable to decipher any of them.

Before Germany's attack on Poland, Polish, French and British intelligence officers met to discuss the breaking of the Enigma cipher. Although cautious at first, the Polish finally shared their success with their partners. This resulted in intensive work, especially on the part of the British, to break new codes, both by means of the methods already developed by the Polish cryptologists, as well as the development of new ones. As the War broke out, Rejewski, Różycki and Zygalski escaped to Romania and then to France, where they con-

tinued their work. They also visited the United Kingdom on several occasions, although France was unwilling to let them go there at first.

Grajek then describes the events of the War in correlation to the successes and failures of the British, French and Polish cryptologists. He stresses such events as the Battle of England, the capitulation of France, the Mediterranean campaign during which the deciphering of Enigma codes played a crucial role, the tough beginnings of the cooperation between American and British cryptologists, and the Battle of the Atlantic.

The author also emphasizes the achievements of the British cryptologists in developing new devices which served to break new German codes, such as Herivel's square, which gave an insight into the habits of German operators of Enigma and allowed to deduce the daily keys to the codes. The author also devotes a whole chapter to the Turing and Turing-Welchman *bombs*, which were deciphering machines, whose prototype was constructed by Rejewski before the War.

The volume of the book is substantial, with almost seven-hundred pages and twenty-one chapters. Despite the technical and mathematical nature of the matter, it reads well and the author is able to explain rather complex mathematical theories and their applications in a way which is understandable even to readers without detailed knowledge of the field. Moreover, he uses a number of boxes and tables which serve to explain the mathematical predicaments in more detail. This allows the readers who are more interested in the mathematical side of the issue to gain a closer perspective.

In the preface, the author states the reasons for writing the book. He asserts that his main aim was to do justice to the Polish cryptologists. Though, to his mind, there is no respectable historian that would question their role, unjust myths about the breaking of the cipher are omnipresent. It is so, despite the fact that Polish historians and politicians have frequently asked for and received acknowledgment of the Polish cryptologists' work by the French and British. However, the author is convinced that unlike mass culture, official documents and celebrations do not speak to the minds of the general public. Grajek believes that his book will make people aware of the contribution of Marian Rejewski, Jerzy Różycki and Henryk Zygalski to the breaking of the Enigma cipher. Judging by the publicity that the book has gained so far in Poland, it is likely that he will achieve his goal. It would be even more feasible, if the book were translated into English, allowing a wider, international audience to become acquainted with the this history of the deciphering of Enigma.