To what extent was the contribution of three Polish mathematicians – Marian Rejewski, Henryk Zygalski, and Jerzy Różycki – crucial for breaking the Enigma machine?

History Internal Assessment

Word count: 2035

May 2024

Table of Contents

Section 1: Identification and evaluation of sources

The following pages shall focus on the research question: “To what extent was the contribution of three Polish mathematicians – Marian Rejewski, Henryk Zygalski, and Jerzy Różycki – crucial for breaking the Enigma machine?.” The breaking of Enigma provided valuable intelligence on German troop movements, strategies, and plans and hence was essential in the overall victory of the Allies.

The 2015 thesis "All the King’s Men: British Codebreaking Operations: 1938-43" by an American historian Andrew J. Avery[1] explores the contributions of different nations to Enigma codebreaking. It is relevant to the investigation as it evaluates the Polish input in comparison to that of others. The article "Enigma Relay" by a Polish historian-cryptologist Marek Grajek[2] provides a comprehensive examination of Polish cryptographic efforts dating back to the 1920s. It is relevant to the investigation since it offers a broader perspective on Polish breakthroughs.

A value of the origin of the thesis is that the historian Andre J. Avery specializes in 20th Century Great Britain with the emphasis on British military[3]. Moreover, during his research, he specifically travelled to the United Kingdom to use the resources of the National Archives at Kew, the British Library, and the Bletchley Park Trust[4]. A value of the purpose is that Avery’s work is intended for professional historians, suggesting that it is an objective and critical review of the subject. A value of the content is that Avery provides numerous numbers and statistics concerning messages decrypted and machines constructed by both the

[1] Avery, Andrew J., "All the King’s Men: British Codebreaking Operations: 1938-43" (2015). Electronic Theses and Dissertations. Paper 2475. https://dc.etsu.edu/etd/2475 [Accessed 09.10.2023]
[2] [2] Grajek, Marek (2016) “Enigma Relay”. Pilsudki Institute of London, UK. Available at: https://www.pilsudski.org.uk/en/aktualnosci.php?news=212&wid=22&wai=&year= [Accessed 09.10.2023]
[3] Avery, Andrew J. (n.d). Education. [LinkedIn]. Available from: https://www.linkedin.com/in/andrew-j-avery-97948791/ [Accessed 09.10.2023]
[4] *Ibid*

Polish and British team. A limitation of the origin is that Avery does not speak Polish, meaning he cannot read Polish-written sources and relies on English sources that may favor an English perspective. A limitation of the purpose is that Avery's thesis, intended for an American audience, may reflect their potential lack of interest in the Polish input. A limitation of the content is that Avery's occasional use of the first voice blurs the distinction between personal opinion or academic discourse.

A value of the origin of the article is that Marek Grajek is a cryptologist with a background in history and several books on the history of cryptology[5]. A value of the content is that Grajek aims at describing a wider context for Polish cryptologic efforts, spanning from the 1920s to several years after the World War II. In addition, Grajek meticulously examines the specific accomplishments of Polish mathematicians and delves into the implications of these achievements. A limitation of the origin is that the article was written for the Piłsudski Institute of London, an organization focused on collecting information about Poland[6], which might introduce a bias toward exaggerating Polish achievements. A limitation of the purpose is that Grajek's article was meant for a Polish, non-professional audience, potentially creating subjective and oversimplified narrative. A limitation of the content is Grajek's language, which glorifies Polish advancements and underlines the tragedies faced by Polish mathematicians, potentially creating a biased narrative compared to their British counterparts.

[5] International Conference on Cryptologic History. (2021). Marek Grajek. [online] Available at: https://www.cryptologichistory.org/speakers/marek-grajek [Accessed 09.10.2023]
[6] The Piłsudski Institute of London (n.d.). Mission Statement,. [online] Available at: https://www.pilsudski.org.uk/en/aktualnosci.php?news=84&wid=14 [Accessed 09.10.2023]

Section 2: Investigation

The Enigma machine was a device employed by the German military command to encode strategic messages both before and during World War II[7], which provided a strategic advantage to the Germans as their plans remained unknown to the Allies. Therefore, the breaking of Enigma was of utmost importance to the Allies as shown by the examples of the Battle of Britain, the Battle of the Atlantic and the protection of British convoys[8]. Although many emphasize the role of the Brits, particularly Alan Turing, in this endeavor, it was Polish mathematicians that laid the groundwork for later discoveries. Therefore, the following discussion shall analyze the role that three Polish mathematicians – Marian Rejewski, Henryk Zygalski, and Jerzy Różycki – played in the breaking of Enigma in the context of Polish efforts, the construction of the bombe, and the capture of the Enigma codebook.

In November 1932, some Enigma-related materials were sold by Hans Thilo Schmidt, who worked at the German Cipher Office and needed money, to the French secret service[9]. Gustav Bertrand, a French military intelligence officer, photographed the sketches and took them to Warsaw[10]. In the meantime, Poland assembled a team of skilled mathematicians, including Marian Rejewski, Henryk Zygalski, and Jerzy Różycki[11]. With materials from Bertrad, the Poles replicated an operational Enigma by January 1933 and had fifteen copies made by the following month[12]. However,

---

[7] Encyclopaedia Britannica (2019). Enigma | German code device | Britannica. In: *Encyclopædia Britannica*. [online] Available at: https://www.britannica.com/topic/Enigma-German-code-device. [Accessed 09.10.2023]

[8] Avery, Andrew J., "All the King's Men: British Codebreaking Operations: 1938-43" (2015). Electronic Theses and Dissertations. Paper 2475. https://dc.etsu.edu/etd/2475 [Accessed 09.10.2023]

[9] Crypto Museum (n.d). History of the Enigma – the rotor-based cipher machine. Available at https://www.cryptomuseum.com/crypto/enigma/hist.htm [Accessed 09.10.2023]

[10] Chris Christensen (2015) Review of IEEE Milestone Award to the Polish Cipher Bureau for "The First Breaking of Enigma Code", Cryptologia, 39:2, 178-193, DOI: 10.1080/01611194.2015.1009751 [Accessed 09.10.2023]

[11] Grajek, Marek (2016) "Enigma Relay". Pilsudki Institute of London, UK. Available at: https://www.pilsudski.org.uk/en/aktualnosci.php?news=212&wid=22&wai=&year= [Accessed 09.10.2023]

[12] University of California San Diego. (n.d.). The Polish Attack on Enimga. [online] Available at: https://mathweb.ucsd.edu/~crypto/students/enigma.html [Accessed 09.10.2023].

they needed the monthly wheel settings for decryption, which they obtained by identifying patterns in the beginning of German radio messages[13]. Additionally, they learned how three Enigma cylinders were wired, reducing variables and thus improving the decryption. By the end of 1937, they had improved Enigma decryption, achieving 100% accuracy[14]. In September 1938, however, the Polish codebreakers faced a problem as the Germans stopped sending message keys at the start of messages. Moreover, the Germans made the Enigma more complex by adding two discs and more circuits to the plugboards, increasing possible combinations significantly[15]. The Poles responded by creating the "bomba,"[16] a series of interconnected Enigma machines to identify initial wheel positions and wiring configurations. Polish team also used perforated paper sheets and “clock method”, pioneered by Zygalski[17] and Różycki[18], respectively, to determine the rotor settings. The former relied on the permutation theory devised by Zygalski which was later even called “the formula that won the Second World War” by a British cryptologist, I. J. Good[19]. Nonetheless, both methods became impractical due to the manual labor required and Enigma advancements. There was also a growing demand for more Enigma machines, with the Polish Cipher Bureau estimating a need for sixty "bomba" setups, each consisting of six Enigmas. Manufacturing over three

[13] Grajek, Marek (2016) “Enigma Relay”. Pilsudki Institute of London, UK. Available at: https://www.pilsudski.org.uk/en/aktualnosci.php?news=212&wid=22&wai=&year= [Accessed 09.10.2023]
[14] Avery, Andrew J., "All the King’s Men: British Codebreaking Operations: 1938-43" (2015). Electronic Theses and Dissertations. Paper 2475. https://dc.etsu.edu/etd/2475 [Accessed 09.10.2023]
[15] Crypto Museum (n.d) “History of the Enigma – the rotor-based cipher machine”. Available at https://www.cryptomuseum.com/crypto/enigma/hist.htm [Accessed 09.10.2023]
[16] Chris Christensen (2015) Review of IEEE Milestone Award to the Polish Cipher Bureau for “The First Breaking of Enigma Code”, Cryptologia, 39:2, 178-193, DOI: 10.1080/01611194.2015.1009751 [Accessed 09.10.2023]
[17] Crypto Museum (n.d) “History of the Enigma – the rotor-based cipher machine”. Available at https://www.cryptomuseum.com/crypto/enigma/hist.htm [Accessed 09.10.2023]
[18] Chris Christensen (2015) Review of IEEE Milestone Award to the Polish Cipher Bureau for “The First Breaking of Enigma Code”, Cryptologia, 39:2, 178-193, DOI: 10.1080/01611194.2015.1009751 [Accessed 09.10.2023]
[19] Grajek, Marek (2016) “Enigma Relay”. Pilsudki Institute of London, UK. Available at: https://www.pilsudski.org.uk/en/aktualnosci.php?news=212&wid=22&wai=&year= [Accessed 09.10.2023]

hundred Enigmas was extremely expensive[20], and the Polish codebreakers were falling behind as the Enigma code became more complex.

Therefore, when Germany conquered Poland (1939) and France (1940)[21], the efforts were redirected to Bletchley Park where The Government Code & Cypher School (GC&CS) was already operating since 1919, though not on such a huge scale[22]. The GC&CS recruited prominent mathematicians where the two most significant were Alan Turing and Gordon Welchman[23]. Turing's strategy for breaking the Enigma code differed significantly from the Polish method. He sought an electro-mechanical device called the bombe, which relied on the correlation between a section of anticipated plaintext (referred to as a "crib," thus giving rise to the term "the cribbing method"), such as "weather forecast," and the corresponding ciphertext[24]. On the other hand, the Polish "bomba" focused on finding keys through the analysis of message beginnings[25]. More specifically, the bombe systematically tested all possible Enigma wheel settings, which amounted to 17,576 combinations or even 158,900,000,000,000 when accounting for various plugboard settings, wheel configurations, and rotor choices[26], that would fit the chosen crib[27]. In this way, the Polish failure benefited the British. Turing had the advantage of bypassing this initial

[20] Chris Christensen (2015) Review of IEEE Milestone Award to the Polish Cipher Bureau for "The First Breaking of Enigma Code", Cryptologia, 39:2, 178-193, DOI: 10.1080/01611194.2015.1009751 [Accessed 09.10.2023]
[21] Crypto Museum (n.d) "History of the Enigma – the rotor-based cipher machine". Available at https://www.cryptomuseum.com/crypto/enigma/hist.htm [Accessed 09.10.2023]
[22] Government Communication Headquarters. (2019). Our origins & WWI. [online] Available at: https://www.gchq.gov.uk/section/history/our-origins-and-wwi. [Accessed 09.10.2023]
[23] The National Museum of Computing. (n.d.). Bombe History. [online] Available at: https://www.tnmoc.org/bh-6-enter-turing-and-welchman [Accessed 09.10.2023]
[24] *Ibid*
[25] Grajek, Marek. (2016). Enigma Relay. Pilsudki Institute of London, UK. Available at: https://www.pilsudski.org.uk/en/aktualnosci.php?news=212&wid=22&wai=&year= [Accessed 09.10.2023]
[26] Ellsbury, Graham. (n.d.). The Turing Bombe. [online] Available at: http://www.ellsbury.com/bombe1.htm. [Accessed 09.10.2023]
[27] The National Museum of Computing. (n.d.). Bombe History. [online] Available at: https://www.tnmoc.org/bh-6-enter-turing-and-welchman [Accessed 09.10.2023]

stage and picking up where the Poles had left off[28]. However, the introduction of the bombe initially led to confusion and uncertainty among the British codebreakers. As the historian A. P. Mahon noted, "unfortunately the bombe was an expensive apparatus and it was far from certain that it would work, or even if the bombe itself worked, that it would enable us to break enigma"[29]. To resolve the issue, Welchman added a “diagonal board”, which eliminated the problems with the unreliability of the bombe and improved the efficiency of the codebreaking process by decreasing the number of plausible starting keys in fewer runs, using variations found in the crib method[30]. Another contribution by Welchman was the proposal of establishing five departments, forming a chain of different organizations to systematically solve the code: The Registration Room, The Intercept Control Rooms, and the Machine Room[31]. This stresses a significant difference between the British and Polish codebreaking operations. The British, with government support, had access to the financial resources needed to develop and expand their codebreaking facilities. In contrast, the Poles had achieved remarkable progress, but lacked the financial means and personnel to continue their work at the same pace[32]. The British's superior financial backing allowed them to make substantial advancements and construct 73 operating bombes by 1943[33].

However, the codebreakers at Bletchley Park faced different challenges when dealing with the naval code compared to their work on the Luftwaffe code. The German Navy utilized four rotors and had eight different rotor choices at their

[28] Avery, Andrew J., "All the King’s Men: British Codebreaking Operations: 1938-43" (2015). Electronic Theses and Dissertations. Paper 2475. https://dc.etsu.edu/etd/2475 [Accessed 09.10.2023]
[29] Mahon, A. P. (2009). Naval Enigma: The History of Hut Eight, 1939-1945. Great Britain: Military Press.
[30] Avery, Andrew J., "All the King’s Men: British Codebreaking Operations: 1938-43" (2015). Electronic Theses and Dissertations. Paper 2475. https://dc.etsu.edu/etd/2475 [Accessed 09.10.2023]
[31] Mahon, A. P. (2009). Naval Enigma: The History of Hut Eight, 1939-1945. Great Britain: Military Press.
[32] Avery, Andrew J., "All the King’s Men: British Codebreaking Operations: 1938-43" (2015). Electronic Theses and Dissertations. Paper 2475. https://dc.etsu.edu/etd/2475 [Accessed 09.10.2023]
[33] *Ibid*

disposal, significantly increasing the number of potential combinations[34]. Consequently, the British needed to find ways to expedite the bombe's operation. After abandoning two other plans of capturing the plans due to technical difficulties and ethical consideration, it was decided that the Royal Navy should focus on capturing trawlers and fetching plans from them[35]. One such attempt proved successful – the München trawler was seized in 1941 and the codebooks for May and June were obtained[36]. With the captured materials in hand, the British were finally able to decrypt current messages. In 1942, they decrypted 148,196 naval messages in ten months, averaging around 14,819 messages decrypted per month[37]. The following year, in 1943, they managed to decrypt an astounding 370,861 naval messages over the course of twelve months, leading to a monthly average of approximately 30,905 messages decrypted[38].

In conclusion, the Polish efforts in the breaking of the Enigma were essential in the 1930s, before the war started. Later, as the Enigma was gradually progressing, the Poles could not keep up financially to improve their methods and lost on their importance in the codebreaking race. Nevertheless, the Polish team set the course for the Brits who used their vast financial resources and knowledge in digital computing to build upon Polish achievements, although with some problems along the way. Furthermore, it is worth noting that the Polish team never actually saw a real Enigma or even its detailed plans. This aspect turned out to be pivotal for British

[34] National Archive of the UK. (1945). Catalogue description Cryptographic history of work on German Naval ENIGMA by C H O'D Alexander, Imperial Defence College [online] Available at: https://discovery.nationalarchives.gov.uk/details/r/C6136631 [Accessed 09.10.2023]
[35] Avery, Andrew J., "All the King's Men: British Codebreaking Operations: 1938-43" (2015). Electronic Theses and Dissertations. Paper 2475. https://dc.etsu.edu/etd/2475 [Accessed 09.10.2023]
[36] *Ibid*
[37] *Ibid*
[38] National Archive of the UK. (1945). Catalogue description Cryptographic history of work on German Naval ENIGMA by C H O'D Alexander, Imperial Defence College [online] Available at: https://discovery.nationalarchives.gov.uk/details/r/C6136631 [Accessed 09.10.2023]

cryptologists in deciphering the Enigma, underscoring the significance of the contribution made by the Polish mathematicians.

Section 3: Reflection

While evaluating the contribution of the Polish mathematicians in the breaking of Enigma, I employed several methods commonly used by historians, including the study of publications as well as the study of archives.

One challenge regarding the study of publications was their selection, given their sheer number and the predominant use of the English language. I had to select sources carefully from the abundance available on the breaking of Enigma, aiming to incorporate a diverse range of perspectives in my investigation. This task proved difficult because English-speaking sources rely predominantly on other English-written sources and hence tend to favor the English contribution. Moreover, Grajek's "Enigma Relay" is not a solitary case and Polish-speaking sources, in general, attempt to counterbalance the above-mentioned disadvantage and showcase a sense of inferiority complex by highlighting, almost exclusively, the achievements of the Polish mathematicians, frequently exaggerating them. This indicates that historians struggle to achieve objectivity as the sources they rely on are biased.

Another obstacle I encountered concerning the study of publications was my nationality. As a Pole, my history education and visits to the Enigma Cipher Center in Poznań[39] had taught me that Polish mathematicians alone deciphered Enigma. However, my investigation revealed that this narrative is not completely true, which was hard to accept and blurred my judgement. This highlights that historians must contend with biases and preconceptions imposed on them by their society and culture in their pursuit of historical truth.

Last significant challenge I faced was relying on the interpretations by other historians, while studying archives, due to limited financial resources for firsthand

[39] Enigma Cipher Centre. (n.d.). Main Page. [online] Available at: https://csenigma.pl/en/ [Accessed 09.10.2023]

access. Although many Enigma-related documents were declassified in the 1990s[40], most remain non-digitalized and inaccessible online, such as the exchange of Enigma information in the years 1941-1942[41]. This necessitates a visit to the National Archives for on-site reading. Unfortunately, the high costs make such a trip unfeasible. Consequently, I must depend on the interpretations of these documents by other historians who have had access, such as Avery in his dissertation, but who may have had misinterpreted facts. This situation suggests that historians must approach the interpretations of primary sources with caution, especially when financial constraints hinder them from in-person review, as such interpretations might be misleading.

[40] MagellanTV. (2021). The Enigma Machine Declassified: Beyond Bletchley Park. [online] Available at: https://www.magellantv.com/articles/the-enigma-machine-declassified-beyond-bletchley-park. [Accessed 09.10.2023]
[41] *Ibid*

Bibliography

Avery, Andrew J. (2015). *All the King's Men: British Codebreaking Operations: 1938-43*. Electronic Theses and Dissertations. Paper 2475. Available at: https://dc.etsu.edu/etd/2475 [Accessed 09.10.2023]

Avery, Andrew J. (n.d). *Education*. [LinkedIn]. Available from: https://www.linkedin.com/in/andrew-j-avery-97948791/ [Accessed 09.10.2023]

Christensen, Chris . (2015). *Review of IEEE Milestone Award to the Polish Cipher Bureau for "The First Breaking of Enigma Code"*. Cryptologia. 39:2. 178-193. DOI: 10.1080/01611194.2015.1009751

Comer, Tony (2021). *Poland's Decisive Role in Cracking Enigma and Transforming the UK's SIGINT Operations*. [online] Available at: https://rusi.org/explore-our-research/publications/commentary/polands-decisive-role-cracking-enigma-and-transforming-uks-sigint-operations. [Accessed 09.10.2023]

Comer, Tony. (2021). *Poland's Decisive Role in Cracking Enigma and Transforming the UK's SIGINT Operations*. RUSI. Available at: https://rusi.org/explore-our-research/publications/commentary/polands-decisive-role-cracking-enigma-and-transforming-uks-sigint-operations [Accessed 09.10.2023]

Crypto Museum (n.d). *History of the Enigma – the rotor-based cipher machine*. Available at https://www.cryptomuseum.com/crypto/enigma/hist.htm [Accessed 09.10.2023]

Ellsbury, Graham. (n.d.). *The Turing Bombe*. [online] Available at: http://www.ellsbury.com/bombe1.htm. [Accessed 09.10.2023]

Encyclopaedia Britannica (2019). Enigma | German code device | Britannica. In: *Encyclopædia Britannica*. [online] Available at: https://www.britannica.com/topic/Enigma-German-code-device. [Accessed 09.10.2023]

Enigma Cipher Centre. (n.d.). *Main Page*. [online] Available at: https://csenigma.pl/en/ [Accessed 09.10.2023]

Government Communications Headquarters. (2019). *Our origins & WWI*. [online] Available at: https://www.gchq.gov.uk/section/history/our-origins-and-wwi. [Accessed 09.10.2023]

Government Communications Headquarters. (2020). *How codebreakers helped fight the Battle of Britain*. [online] Available at: https://www.gchq.gov.uk/information/how-codebreakers-helped-fight-battle-britain. [Accessed 09.10.2023]

Grajek, Marek. (2016). *Enigma Relay*. Pilsudki Institute of London, UK. Available at: https://www.pilsudski.org.uk/en/aktualnosci.php?news=212&wid=22&wai=&year= [Accessed 09.10.2023]

International Conference on Cryptologic History. (2021). *Marek Grajek*. [online] Available at: https://www.cryptologichistory.org/speakers/marek-grajek [Accessed 09.10.2023]

Kraus, George and Kozaczuk, Wladyslaw. (1988). *Enigma. How the German Machine Cipher Was Broken, and how It Was Read by the Allies in World War II*. Naval War College Review: Vol. 41 : No. 4 , Article 12. Available at: https://digital-commons.usnwc.edu/nwc-review/vol41/iss4/12

Mahon, A. P. (2009). *Naval Enigma: The History of Hut Eight, 1939-194*5. Great Britain: Military Press.

National Archive of the UK. (1945). *Catalogue description Cryptographic history of work on German Naval ENIGMA by C H O'D Alexander*. Imperial Defence College [online] Available at: https://discovery.nationalarchives.gov.uk/details/r/C6136631 [Accessed 09.10.2023]

The National Museum of Computing. (n.d.). *Bombe History*. [online] Available at: https://www.tnmoc.org/bh-6-enter-turing-and-welchman [Accessed 09.10.2023]

The Piłsudski Institute of London (n.d.). *Mission Statement*. [online] Available at: https://www.pilsudski.org.uk/en/aktualnosci.php?news=84&wid=14 [Accessed 09.10.2023]

University of California San Diego. (n.d.). *The Polish Attack on Enigma*. [online] Available at: https://mathweb.ucsd.edu/~crypto/students/enigma.html [Accessed 09.10.2023]