Cryptologia, 37:167–174, 2013

ISSN: 0161-1194 print
DOI: 10.1080/01611194.2013.767678

Taylor & Francis
Taylor & Francis Group

Review of *Memories of My Work at the Cipher Bureau of the General Staff Second Department 1930–1945* by Marian Rejewski

CHRIS CHRISTENSEN

Rejewksi, Marian. *Memories of My Work at the Cipher Bureau of the General Staff Second Department 1930–1945*. Adam Mickiewicz University Press, Poznan, Poland. 2011. 175 pages (in English and a similar number of pages containing the same material in Polish), Hardcover, approximately $18. ISBN 978-83-232-2237-8.

The year 2010 marked the thirtieth anniversary of the death of Marian Rejewski, whose name is known to all who are interested in Enigma. To honor Rejewski and his colleagues Jerzy Rozycki and Henryk Zygalski, Adam Mickiewicz University Press decided to publish in book from two of Rejewski's typed manuscripts, which had been deposited in Wojskowy Instytut Historyczny.

Memories of My Work in the Cipher Bureau of the General Staff Second Department was written by Rejewski in 1967. This document is pages 13 through 92 of the book. "Memories" consists of a very brief Introduction, a brief Conclusion, and 11 chapters that describe Rejewski's memories of his work with the Cipher Bureau:

1. Work at the Branch Office in Poznan
2. Commencing Work at the General Staff
3. The Enigma Machine. Recovering the Message Keys
4. The Enigma Machine Description
5. Permutation Theory
6. The Enigma Machine. Reconstructing Rotor Connections
7. The Enigma Machine. Recovering the Daily Keys
8. The Use of the Enigma Machine in Poland
9. The Use of the Enigma Machine in the West
10. Clandestine Work in France
11. Work in Great Britain

The second manuscript by Rejewski, "Supplement to *Memories of My Work in the Cipher Bureau of the General Staff Second Department*" was written in 1974. This document is pages 93 through 126 of the book. "Supplement" consists of brief commentaries (one or two pages long) on each of the chapters of "Memories."

> My *Memories*, written in 1967, were primarily concerned with the technical aspects. I wrote mainly about ciphers, and very little about the people

Address correspondence to Chris Christensen, Department of Mathematics and Statistics, Northern Kentucky University, Highland Heights, KY 41099, USA. E-mail: CHRISTENSEN@nku.edu

> involved with breaking the ciphers. In view of the interest that Enigma has attracted today [1974], this time I want to write a bit more about ourselves, but I will not be able to avoid writing about ciphers altogether. At the same time, I would like to use this occasion and set the record straight regarding certain mistaken assumptions expressed either by the authors of articles in the press on the topic of Enigma, or by the readers of these articles, Also, some of the points made by Gen. [Gustave] Bertrand[1] in his book require clarification. Such is the purpose of this *Supplement*. Marian Rejewski. [p. 95]

Pages 123 through 126 contain personal details and information about the fate of each of the fifteen members of the Z Team—the name by which they were called while they were working in France. Rejewski notes that Bertrand in his 1973 book "did not mention any of the Polish names involved. ... As a member of the team, of course I could have revealed the names of all the members of the team, but at the time I knew very little of their subsequent life events." [p. 95] Rejewski gathered information about the Z team members from Bertrand, Zygalski, and others, and in the Conclusion to "Supplement" he has written a brief paragraph about each.

The editors[2] have done excellent work preparing this book. They have not merged the two manuscripts; however, they did (apparently very carefully) adjust page number references and combine the "Table of Contents." They also state that they corrected some flaws in Rejewski's footnotes, corrected obvious typing errors, and corrected a few names. Rejewski's footnotes appear in "Memories" and "Supplement."

Pages 127–132 contain a brief biography of Rejewski by Marek Grajek. The biography is followed by two pages containing a map of Europe and an index which describe "Marian Rejewski's route"—21 locations which begin with his childhood and youth in Bydgoszcz and follow his career until his death in Warsaw on 13 February 1980.

There is a two-page "Index of Names" which indexes both "Memories" and "Supplement." The middle of the book contains fourteen pages of images of people and documents, many that have not appeared in other publications about the Polish codebreakers.

This book contains "Memories" and "Supplement" in both English and Polish. The Polish text begins from one end of the book, and the English text begins at the other end after the book is flipped top to bottom. The images in the center are shared by both the Polish and English versions, and the captions are in both languages. The English translation reads very well.

The editors should also be thanked for adding a section of "Notes" (pp. 135–155) which contains 132 brief but very useful notes by the editors. The notes are keyed to Rejewski's two papers. (It would be useful if each note included the page to which the note refers.)

A standard reference in English for the work of the Polish codebreakers is Wlasyslaw Kozaczuk's *Enigma*[3] [8] (which appeared in Polish in 1979 and in an

---

[1] *Enigma ou la plus grande énigme de la guerre 1939–1945*, which was published in 1973.

[2] Magdalena Jaroszewska (Editor-in-Chief), Marek Grajek, Jerzy Jaworski, and Tomasz Kubial.

[3] Rejewski's "Memories" is a reference for *Enigma*.

English translation by Christopher Kasparek in 1984). Four appendices contain information directly from Rejewski:

Appendix B: A Conversation with Marian Rejewski by Richard A. Woytak.[4] [8, pp. 229–240]

Appendix C: Summary of Our Methods for Reconstructing ENIGMA and Reconstructing Daily Keys, and of German Efforts to Frustrate Those Methods by Marian Rejewski.[5] [8, pp. 241–245]

Appendix D: How the Polish Mathematicians Broke Enigma by Marian Rejewski.[6] [8, pp. 246–271]

Appendix E: The Mathematical Solution of the Enigma Cipher by Marian Rejewski.[7] [8, pp. 272–291]

Another article by Rejewski is [15]. In this article, Rejewski, in response to a request by Richard A. Woytak, commented on "Appendix 1" of Hinsley's *British Intelligence in the Second World War, Volume 1*.[8] Rejewski made 34 brief comments on Hinsley's appendix.

"Memories" shares much material—both historical and mathematical—with the writings of Rejewski that are mentioned above, but it is still a valuable English-language contribution to our knowledge of Enigma and the Polish contribution to World War II codebreaking.[9] Rejewski tells the story of the Polish codebreakers in an interesting and pleasant style. He tells of his mathematical ideas in a way that is informal. It seems typical of Rejewski that he exhibits his mathematical ideas but he does prove them. The editors have included notes that fill gaps in Rejewski's mathematical discussions. Unfortunately, there is a jarring contrast between Rejewski's informal mathematical style and the editors' formal and abstract mathematical style.

The editors' notes are generally excellent, an aid to understanding Rejewski's comments, and fill in gaps in his history and his mathematical discussions. Note 21, however, seems to attribute a bit too much to the Polish codebreakers:

> When describing the theoretical frequency of letter pairs [see p. 28.], Rejewski presents the concept of the index of coincidence, described for the first time in 1920 by William Friedman, father of contemporary American cryptology. Friedman's original writings were declassified only in 1995. Rejewski's analysis might indicate that the concept of the index

---

[4]This conversation was recorded on 24 July 1978. The conversation also appears as [16].

[5]This paper was written in 1977.

[6]This paper appeared first in Polish in 1980. A slightly different version appears as [13], which includes two Afterwords, one by Cipher A. Deavours and another by I. J. (Jack) Good.

[7]This appendix was an appendix to the Polish version of *Enigma*. A translation by Christopher Kasparek also appeared in *Cryptologia* [14].

[8]See "The Polish, French and British Contributions to the Breaking of the Enigma" [5, pp. 487–495].

[9]Another reference for the historical aspects of the Polish codebreakers is [9]. One of the authors, Kozaczuk, is a historian who interviewed Rejewski and whose 1967 book *Battle for the Secrets* (in Polish) first told of the work of the Poles. A recent book by Z. J. Kapera in the Enigma Series [7] tells the story of the Polish codebreakers in France. Kapera's book is brief and includes a bit too much detail about the number of messages decrypted, etc. The review in *Cryptologia* [2] lists the other publications in the Enigma Series.

> of coincidence was independently discovered by Polish codebreakers, most probably Jerzy Rozycki, in association with his *clock method*, presented by Rejewski later on [in "Memories"]. [p. 138]

While it is true that Friedman's index of coincidence paper was classified, in one of those strange "secrecy things," it was originally published and later classified.

David Kahn in [6] described the early history of the publication of Friedman's index of coincidence paper:

> *The Index of Coincidence* was No. 22 [of Riverbank Publications], and [George] Fabyan [the founder of Riverbank Laboratories], to save money, had it printed in France in 1922. General Francois Cartier, the head of the French Ministry of War's cryptologic agency, saw it, and quickly recognized its value, and had it translated. He then had the military publisher Fournier, whose office was across the street from the war ministry on the Boulevard Saint-Germain, publish this translation, acknowledging it as such but falsely dating it 1921, as if the French had thought of this brilliant concept before the Americans. Fournier also published an English-language version, dated 1922. Neither credited Friedman as the author, but an edition published in Riverbank in 1922 did carry his name on the title page. [6, pp. 162–163]

The Index of Coincidence was later classified and remained classified for some time. The Polish codebreakers, however, might have seen the paper or learned the technique in their classes at Poznan. The editors state in Note 8 that

> A book published in 1925 by an outstanding French codebreaker of WWI, Marcel Givierge *Cours de Cryptographie* was the basis for the theory presented during the [course in cryptography taught to the Rejewski and others at Poznan in late 1928 or early 1929]. [p. 137]

A footnote on page 66 of an English translation [4] of Givierge's *Cours* refers to there being a French edition of Friedman's paper. The footnote says

> See for example the work entitled *L'Indice de coincidence et ses applications en Cryptographie*, by Fournier, 1921, a translation of a work in the English language. Note: This is a translation from the manuscript of *The Index of Coincidence and its Applications in Cryptography* by William F. Friedman, Riverbank Publication No. 22, 1922.

So, a French edition of Friedman's work was available when the Poles were taking their course in cryptography, and the index of coincidence might have been mentioned in the text on which the course was based.

Theorems from permutation theory were critical in Rejewski's breaking of Enigma. In Note 100, the editors state that

> The British mathematician, Irving John Good [1916-2009], who during WWII participated in breaking Enigma ciphers at Bletchley Park, described one of the theorems formulated by Rejewski for the purpose

> of his pioneering attack as the "theorem which won World War II." Rejewski's theorem on the product of permutations is still today referred to as the "central theorem of rotor cryptology". [p. 151]

Cipher Deavours in the first "Afterword" to [13] named the theorem that states that "a permutation and any conjugate of it have the same cycle structure" as "the theorem that won World War II." [13, p. 232] I. J. Good wrote the second "Afterword" to [13], but he did not name the theorem. Bauer [1, p. 110] called the same theorem "The Main Theorem of Rotor Encryption."

On page 42, Rejewski states another theorem from permutation theory that was critical to his breaking of Enigma: "If we multiply two permutations, consisting solely of transpositions, then the product has an even number of cycles of the same length." This result nullified the plugboard and allowed Rejewski to determine daily keys. In "Memories," Rejewski gives a brief example but offers no proof of the theorem. In his "Supplement," Rejewski says

> Due to my trying to be concise [it] now seems to me that my treatment of [the theorem in the previous paragraph] was too superficial, all the more so as this theorem is not available in the existing literature (it was formulated by myself). After all, it was of basic importance to the whole theory of Enigma, since only due to the properties contained in this theorem did it become possible to reconstruct keys and to explicate the theory of reconstructing the rotor connections.
>
> Therefore, without seeking to prove its mathematical sustainability, I wish to return to this theorem in a more developed form. [p. 100]

Rejewski again sidesteps a proof; he offers another example and states that "the converse is also true," but he does not give a proof.[10] Rejewski says, "[the theorem] is still without a proof, after all we are not after the mathematical precision but after the cryptologic utility." [p. 100]

On pages 101 and 102, Rejewski discusses the value of the information about Enigma that was provided to him by the French:

> On p. 63 of his book Gen. Bertrand says that the Polish Cipher Bureau received from him the daily keys to the Enigma machine for the period from December 1931 to July 1934, and some other materials, like for example the plain text and the encrypted text of a long German message consisting of several parts. He also expresses his admiration for the Polish cryptographers who managed to break the Enigma on the basis of such material together with the intercepted messages. His astonishment would have surely been increased significantly if he had known that I received only the keys for a period of two months—that is September and October 1932. . . . Since, however, so little data was needed to break the Enigma, apart from the encrypted material of course, a question arises whether it could have been done without the assistance of Gen. Bertrand, or for that matter, his supplier. The question is difficult and the answer cannot be straightforward.

[10]The editors supply a proof in Note 35.

The editors comment in Note 101:

> Rejewski's mathematician's conscience did not allow him to accept short-cuts in his solutions. . . . [H]e attempted to find, ex-post, a purely analytic solution to the problems. . . . After the war, when asked about the significance of the documents delivered by Bertrand, he stressed their critical practical importance. His honesty has been abused by certain historians, mostly French ones, maintaining that if the documents delivered by French intelligence played such a crucial role in breaking the Enigma cipher, a big part of the glory goes to France. One should remember, however, that before the documents were delivered to Warsaw, they had been investigated by the French and British codebreakers and described as useless. When, in the 1970's, Rejewski tried to reconstruct his purely analytic method of breaking the Enigma, even his fantastic memory failed him. Contemporary codebreakers were able to take over the problem, fill in the gaps in his reasoning and confirm that Rejewski's method would work.[11] [pp. 151–152]

Unfortunately, the editors do not help resolve the question of why the Polish cryptanalytic machine received the name "bomba." [See Note 57, p. 145.]

In Chapter 10, "Clandestine Work in France," Rejewski nicely describes solutions of a transposition cipher and the Playfair cipher. On page 73, he briefly mentions his quick solution (in July 1941) of the Polish LCP ciphering machine [LACIDA].[12] (See also, Note 81, pp. 148–149.)

In Chapter 12, "Work in Great Britain," a brief discussion of double Playfair appears. Rejewski notes that

> Throughout the whole of our stay in Great Britain, we had to deal with but one type of cipher if I rightly remember, since evidently the radio-telegraphers were able to pick up only one type of cryptogram. It was the cipher used by the SS formations and it was called *Doppelkasten-verfahren*. [p. 87]

Comments by the editors in Note 86 [p. 150] claim that

> The reasons of the Poles giving up the Enigma ciphers were different from Rejewski's guess. Until mid-1943 the British and Americans were able to solve the majority of Enigma-related theoretical problems and the assistance of [Rejewski and Zygalski] was not essential anymore. Rejewski and Zyglaski landed in Britain [2 August 1943 in Scotland] after the discovery of the Katyn graves [13 April 1943] and General Sikorski's death [4 July 1943]. Churchill was pressing the Polish government in London to demonstrate a more conciliatory position toward Soviet demands. At the same time, the British secret service encouraged the Polish signals intelligence section to concentrate its attention on attacking the Soviet codes and ciphers. The motive was simple: Churchill declared in 1941 that

[11] See, for example, [10], [11], and [12].
[12] See [3] for a description of the machine.

> Great Britain would not attack the ciphers of its new ally, but Poland had never made such a declaration. When the Polish intelligence service was busy getting the codebreakers out of the Spanish internment camps, plans were analyzed to switch their attention from German to Soviet ciphers. For reasons unknown this plan was only partially implemented.
>
> After the codebeakers' arrival in Great Britain, the British hosts were not interested in their cooperation, which only three years ago they tried to assure acting *fas et nefas*. As at this stage of the war, attacking the Enigma ciphers was only possible with the help of sophisticated equipment, unavailable to the Polish Army in exile. In this situation the codebreakers' attentions was focused on the only system that could be attacked by using more traditional approach—the SS ciphers.

Everyone who is interested in Enigma and the Polish contribution to World War II codebreaking should read some of Rejewski's papers. ''Memories'' would be a good choice, especially because of the notes added by the editors. Unfortunately, ''Memories'' does not appear to be available at the usual online booksellers.

Acknowledgements

I thank Jan Bury for obtaining contact information for the publisher:
Adam Mickiewicz University Press
ul. Fredry 10
61-701 Poznan, Poland
E-mail: press@amu.edu.pl
Web address: http://press.amu.edu.pl

About the Reviewer

Chris Christensen teaches mathematics and cryptology at Northern Kentucky University. His first encounter with the theory of Enigma was in Robert Harris' novel *Enigma*.

References

1. Bauer, F. L. 2007. *Decrypted Secrets, Fourth Edition*. Berlin Heidelberg: Springer-Verlag.
2. Christensen, C. 2012. ''Review of 'The Shadow of Pont du Gard' by Zdzislaw Jan Kapera,'' *Cryptologia*, 36(2):176–178.
3. Gaj, K. 1992. ''Polish Cipher Machine—LACIDA,'' *Cryptologia*, 16(1):73–80.
4. Givierge, M. 1978. *Course in Cryptography*. Laguna Hills, CA: Aegean Park Press.
5. Hinsley, F. H. 1986. *British Intelligence in the Second World War*, Volume 1. Southampton: Her Majesty's Stationery Office.
6. Kahn, D. 2002. ''A Riverbank Trove,'' *Cryptologia*, 26(3):161–164.
7. Kapera, Z. J. 2011. *In the Shadow of Pont du Gard*. Krakow-Mogilany: The Enigma Press.
8. Kozaczuk, W. 1984. *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War II*. Edited and translated by Christopher Kasparek. Fredrick, MD: University Publications of America.
9. Kozaczuk, W. and J. Straszak. 2004. *Enigma: How the Poles Broke the Nazi Code*. New York: Hippocrene Books.

10. Lawrence, J. 2004. "The Versatility of Rejewski's Method: Solving for the Wiring of the Second Rotor," *Cryptologia*, 28(2):149–152.
11. Lawrence, J. 2005. "A Study of Rejewski's Equations," *Cryptologia*, 29(3):233–247.
12. Lawrence, J. 2005. "Factoring for the Plugboard—Was Rejewski's Proposed Solution for Breaking The Enigma Feasible?," *Cryptologia*, 29(4):343–366.
13. Rejewski, M. 1981. "How Polish Mathematicians Deciphered the Enigma," *Annals of the History of Computing*, 3(3):213–234.
14. Rejewski, M. 1982. "Mathematical Solution of the Enigma Cipher," *Cryptologia*, 6(1): 1–18.
15. Rejewski, M. 1982. "Remarks on Appendix 1 to British Intelligence in the Second World War by F.H. Hinsley," *Cryptologia*, 6(1):75–83.
16. Woytak, R. 1982. "A Conversation with Marian Rejewski," *Cryptologia*, 6(1):50–60.