Recovering the military Enigma using permutations, filling in the details of Rejewski's solution

Paz Jiménez Seral, Manuel Váquez Lapuente

Departamento de Matemáticas, Universidad de Zaragoza

paz@unizar.es

Abstract: During the last few months of 1932, the Polish mathematician Marian Rejewski solved the problem of finding the internal connections of the rotors and reflector of the Enigma cipher machine used by the German army at that time. This allowed the Polish Cipher Bureau to construct an analogue of the machine, and subsequently to find effective methods for deciphering secret messages. Rejewski performed this feat virtually alone using cryptographic material provided by the Polish secret services. His knowledge of the theory of permutation groups was essential in solving this problem. This article describes in detail how to find the complete wiring of the rotors and reflector of Enigma, as well as other specifics, using data that Rejewski had at his disposal, by systematically presenting the resolution of all cases that could have been encountered. Similarly, we complete those stages of the procedure that were only outlined by Rejewski.

References

[1] Rejewski, M. (1981). How polish mathematicians deciphered the Enigma, Annals of the History of Computing 3(3): 213-234.

[2] Rejewski, M. (2011). Memories of my work at the Cipher Bureau of the General Staff Second Department 1930-1945. Poznan (Poland): Adam Mickiewicz University Press.Proceedings.