How Polish Mathematicians Deciphered the Enigma

MARIAN REJEWSKI

The paper gives a personal view of work in the Polish Cipher Bureau from 1932 to 1939 as mathematicians worked to decipher the codes of the military version of the Enigma. The author, who was a participant, relates details of the device and the successes and frustrations involved in the work. He also describes mathematical principles that enabled him and his colleagues to break successive versions of the Enigma code and to construct technical devices (cyclometers and "bombs") that facilitated decipherment of Enigma-coded messages.

Keywords: *Enigma, cryptology*
CR Category: *1.2*

Introduction

At the end of 1927, or possibly at the beginning of 1928, a parcel containing radio equipment, according to the declaration, arrived from Germany at the customs house in Warsaw. Because the parcel had been sent erroneously in place of other equipment, a representative of a German firm very insistently demanded the return of the parcel to the German government before it was cleared through customs. His demands were so urgent that they awakened the suspicions of the customs officers, who informed the Cipher Bureau of the Second Department of the General Staff, an institution interested in every kind of innovation in the area of radio equipment. Since it happened to be Saturday afternoon, the employees delegated by the bureau had time to study the matter at leisure. The box was carefully opened, and it was determined that indeed it did not contain radio equipment; it contained a cipher machine. The machine was thoroughly examined, and then the box was carefully refastened.

You can easily surmise that this cipher machine was the Enigma—clearly the commercial version—because at that time the military version was not in use at all. The episode had no immediate significance, being simply the time the Cipher Bureau became interested in the Enigma machine and manifested that interest by the completely legal purchase of another unit of the commercial machine.

When the first machine-enciphered messages appeared on the air on July 15, 1928, transmitted by a German military station, Polish radio telegraphers working at monitoring stations began to pick up the transmissions. Polish cryptologists in the German section of the Cipher Bureau received orders to undertake an attempt to decipher them. But the effort was unsuccessful and after a time was terminated. Very minute traces of that work were left in the form of several sheets of paper densely filled with writing; the commercial version of the Enigma machine also was available.

This article was entitled "Jak matematycy polscy rozszyfrowali Enigmę" in the Annals of the Polish Mathematical Society, Series II, *Wiadomości Matematyczne*, Volume 23, 1980, 1–28, copyright © Państwowe Wydawnictwo Naukowe, Warsaw, 1980, translated by Joan Stepenske with the permission of the publisher.

Editor's Note. We would like to thank Joan Stepenske for translating this article from the Polish. We also want to thank Zbigniew Semadeni and Wladyslaw M. Turski for their efforts in obtaining the article and in ensuring a faithful translation. We are grateful to Joanna Siemień for compiling bibliographic data.