The Polish Cryptanalysis of Enigma

Richard E. Klima
klimare@appstate.edu
Department of Mathematical Sciences
Appalachian State University
Boone, North Carolina 28608
USA

Neil P. Sigmon
npsigmon@radford.edu
Department of Mathematics and Statistics
Radford University
Radford, Virginia 24142
USA

Abstract

The cryptanalysis of the Enigma cipher machine during World War II by British and American codebreakers led by Alan Turing at Bletchley Park has been well-documented, and rightfully recognized as one of the supreme achievements of the human intellect. However, without the successful cryptanalysis of an earlier version of Enigma by Polish codebreakers led by Marian Rejewski in the 1930s, the work of the British and Americans in the 1940s might have taken much longer, prolonging the war at the potential cost of untold additional lives. The mathematics integral to the Polish cryptanalysis of Enigma involved some basic theory of permutations. The purpose of this paper is to present an overview of these ideas and how they served to this effect. To assist in demonstrating this, technology involving Maplets will be used.

1 Introduction

In 1918, German electrical engineer Arthur Scherbius applied for a patent for a mechanical cipher machine. Later marketed commercially under the name *Enigma*, this machine was designed with electric current running through revolving wired wheels, called *rotors*. Scherbius offered Enigma to

the German military, who, after learning that their World War I ciphers had routinely been cracked, adopted and used Enigma as their primary field cipher prior to and throughout World War II.

In the early 1930s, due to suspicions that Germany was seeking to rearm and reclaim territories lost to Poland following World War I, the Poles began carefully monitoring German radio transmissions, which were encrypted using Enigma. Unable to decrypt these messages, the Polish government recruited mathematics students for the purpose of cryptanalyzing Enigma. Among these students were Marian Rejewski, Jerzy Różycki, and Henryk Zygalski, who became employees of the Cipher Bureau in Warsaw in the summer of 1932, coinciding with the beginning or their work on Enigma. Among Rejewski, Różycki, and Zygalski, the most renowned is Rejewski, who in particular pioneered the use of permutations in attacking Enigma.

In this paper, we will give an overview of the theory of permutations that Rejewski needed, and characterize the various components of Enigma and reasons for Germany's ill-fated confidence in its security. We will also describe and demonstrate several aspects of the successful efforts by the Polish codebreakers in cryptanalyzing the pre-war version of Enigma.

2 Permutations

Traditional collegiate abstract algebra courses often cover the basic theory of permutations, the details of which can thus be found in many resources typically used as textbooks in such courses. Due to their importance in the Polish method for cryptanalyzing Enigma, we will begin by giving an overview of some of the theory of permutations and their representations involving cycles.

A *permutation* on a set Ω is a function $\sigma : \Omega \to \Omega$ that is both one-to-one and onto. In this paper we will assume Ω is a finite set. As an example, if $\Omega = \{\mathtt{A},\mathtt{B},\mathtt{C},\mathtt{D}\}$, then one permutation on Ω is the function σ with $\sigma(\mathtt{A}) = \mathtt{B}$, $\sigma(\mathtt{B}) = \mathtt{C}$, $\sigma(\mathtt{C}) = \mathtt{D}$, and $\sigma(\mathtt{D}) = \mathtt{A}$. Similarly, the function τ with $\tau(\mathtt{A}) = \mathtt{C}$, $\tau(\mathtt{B}) = \mathtt{B}$, $\tau(\mathtt{C}) = \mathtt{D}$, and $\tau(\mathtt{D}) = \mathtt{A}$ is a permutation on Ω. On the other hand, the function μ with $\mu(\mathtt{A}) = \mathtt{B}$, $\mu(\mathtt{B}) = \mathtt{A}$, $\mu(\mathtt{C}) = \mathtt{B}$, and $\mu(\mathtt{D}) = \mathtt{D}$ is not a permutation on Ω, since it is not one-to-one.

Permutations can be represented most efficiently using *cycle* notation. A permutation on a finite set $\{x_1, x_2, \ldots, x_n\}$ that maps $x_1 \mapsto x_2 \mapsto x_3 \mapsto \cdots \mapsto x_n \mapsto x_1$ is represented using cycle notation as $(x_1 x_2 \cdots x_n)$, with each element within the parentheses written to the right of the element from which it maps, until the parentheses close when the element at the "end" (the far right) maps back to the one at the "start" (the far left). So, for example, the permutation σ on $\Omega = \{\mathtt{A},\mathtt{B},\mathtt{C},\mathtt{D}\}$ with $\sigma(\mathtt{A}) = \mathtt{B}$, $\sigma(\mathtt{B}) = \mathtt{C}$, $\sigma(\mathtt{C}) = \mathtt{D}$, and $\sigma(\mathtt{D}) = \mathtt{A}$ would be represented using cycle notation as $\sigma = (\mathtt{ABCD})$. The permutation τ on Ω with $\tau(\mathtt{A}) = \mathtt{C}$, $\tau(\mathtt{B}) = \mathtt{B}$, $\tau(\mathtt{C}) = \mathtt{D}$, and $\tau(\mathtt{D}) = \mathtt{A}$ would be represented as $\tau = (\mathtt{ACD})(\mathtt{B})$, which requires two "cycles," one containing the single element $\mathtt{B}$, since $\mathtt{B}$ maps to itself under τ, and thus must be at both the start and end of the cycle in which it is contained. Such cycles of "length" 1 are often not explicitly written in representations of permutations, since an element's absence from an expression can be interpreted as indicating that it maps to itself. Thus, τ could also be expressed as $\tau = (\mathtt{ACD})$. In this paper though we will include cycles of length 1.