CSC B58: Enigma Breakdown

James Camano

March 10, 2019

(**Last Edited - March 10, 2019**: *Began documentation of Enigma*)

This document sets out to describe the components of the Enigma machine.

1 Introduction

Project Enigma sets out to imitate both the German *Enigma* text cipher machine.

This imitation of Enigma (which will henceforth be called the same name) creates a cipher of a character input by starting off with an initial set state, performing *alphabet shift arithmetic* to the character input based on that state and then 'advancing' the state. Finally, this shifted input is returned as output.

2 Components

Enigma consists of:

1. A set of rotors $\{R^i\}_{i=1}^{n}$, whose values cycle from $0 - 25$ [1].

3 Encryption Algorithm

Define:

- The alphabet $\Sigma = \{\bar{a} : \bar{a} \text{ is a character in the English alphabet}\}$
- R_n to be a rotor with setting n. That is, R_n's value is n
- $\varphi_k \in \Sigma$ to be the k^{th} letter in the alphabet. (i.e. $\varphi_1 = b$)
- $g(R_n) = \begin{cases} R_{n+1}, \text{ if } n+1 \leq 25 \\ R_0, \text{ if } n+1 > 25 \end{cases}$
- $f(\varphi_k, R_n) = \begin{cases} \varphi_{k+n}, \text{ if } k+n \leq 25 \\ \varphi_{k+n-26}, \text{ if } k+n > 25 \end{cases}$

Then, the encryption algorithm is as follows:

[1] Currently, $n = 1$.

1. $\omega := f(\varphi_k, R_n)$
2. $R_n := g(R_n)$

Where φ_k is assumed to be the input letter, and ω is the corresponding output of the Enigma machine.

4 Decryption Algorithm

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.