Project: Enigma Machine and Turing-Welchman Bombe

Maria Camila REMOLINA GUTIÉRREZ
maria.remolina_gutierrez@telecom-sudparis.eu

Advisor: Prof. Eric RENAULT

April 28, 2019

Abstract

This is the work proposal to follow in the course Project as part of the master M1 in Computer Science and Communication Networks at Télécom SudParis. The goal is to implement the Enigma machine used in World War II, followed by the Bombe machine that breaks the cipher, created by Alan Turing and Gordon Welchman at Bletchley Park.

1 Introduction

The enigma machine is a cipher machine used by the Nazi Germany during World War II in order to send secret coded messages. It was initially a commercial machine bought by banks are businesses. But then the military took it and added an extra security layer called plugboard. It was innovative at the time because it was not a substitution cipher, i.e. the same letter can get different results after encryption.

The machine works by a combination of moving rotors and inside wiring as seen in Fig. fig:machine. The way to use it is that when the sender types a message, a bulb lights up indicating the correspondent coded letter. Then, in order to decode, the receiver types the coded message he received and the initial message lights up on the board. In war times the coded messages were transmitted over morse code.

In the military version of the Enigma Machine there were 5 possible rotors to pick from, each with 26 possible positions, then there were 10 possible switching in the plugboard that could choose a pair from the available 26 letters. That accounts for 158962555217826360000 different combinations for the setting of the army Enigma Machine [1]. The initial setting for each day was given to the bases in a sheet of paper that had the monthly configurations of the machine. So they changed the setting everyday.

So in order to decipher the code, you needed either to have the code sheet or to break the message. This latter was what the scientists at Bletchley Park did; and what I will try to recreate in this project.

2 General Goal

To understand the code breaking process behind the enigma cipher.

3 Specific Goals

- To implement the Enigma machine with software
- To implement the Bombe machine that breaks the Enigma cipher
- To understand the mathematical and probabilistic techniques used to break a cipher with limited time and computational resources.
- To understand the weaknesses exploited that allowed to break the Enigma cipher

4 Methodology

I will create 2 different programs within the same project:

1. The Enigma machine
2. The Bombe machine

The implementation of both will be in Python and it will be publicly available in the GitHub repository `https://github.com/mariacamilarg/enigma_bombe`. As for the computational resources, I will need only my personal computer (with Linux O.S.) with standard architecture.

5 Work Schedule

This will be the main work of the course Scientific Project with 2.5 ECTS. It will be performed during the course of 2 months approximately, in the time stipulated for the class. The delivery date will be in mid June of 2019.

References

[1] Numberphile. *158,962,555,217,826,360,000 (Enigma Machine)*. YouTube (2013).

[2] A. Hodges. *Alan Turing: The Enigma*. Princeton, N.J: Princeton University Press (2012).

Advisor Signature

Student Signature

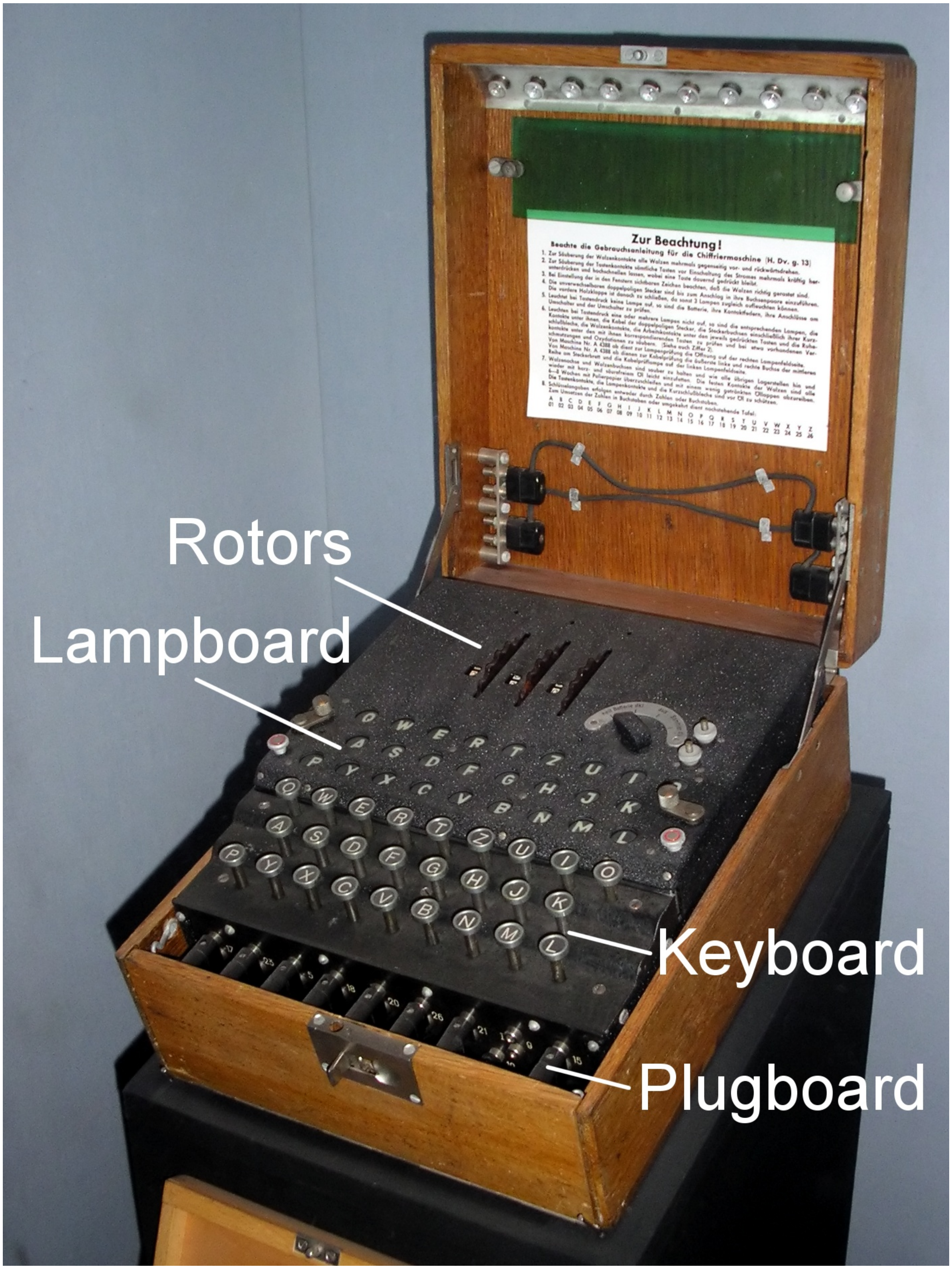

Figure 1: Enigma Machine - Military Edition