The Enigma

Anika Ramachandran

May 4, 2016

1 Introduction

The Enigma was a machine used by Germans to encode and decode messages during World War II. Many believed it was impossible to break but due to the determination of some persistent mathematicians, it was finally broken. The story of the enigma is a long one including when it was created, out-witted, improved, and then broken yet again.

2 Setting the Stage

2.1 Before the Enigma Existed

Let us begin with a story. It was 1918, and cryptanalysts were much ahead of cryptographers. They had the Vigenère cipher which could be used with long, random keys. These random keys were created with the use of pencil and paper and the randomness of one individual on one-time pads. These pads had long lists of keys; however, the keys could be stolen and were not always random due to human error. Messages were sent over telegraph and by now, it was common knowledge that other countries and people could tap into their lines and discover the messages. The messages had to be secure, otherwise you were running considerable risk.

Germany did not have many countries on its side during the World War. Its strength came from surprise not size. The Enigma would prove to be a crucial part of initial German success but failed Germany when it was broken without the knowledge of the Germans.

Around this time, a man named Leon Alberti wanted to make the process of encryption using the Vigenère cipher easier. He created a cipher disk, which had the alphabet listed on the outside and inside. It could be rotated in order to create a new mono-alphabetic cipher, the outside letters matching with the inside ones. Using the key, the ring could be rotated to match the letters of the key each time, and a message could be encrypted slightly faster.

2.2 The Creation of the Enigma

In 1918, German inventor Arthur Scherbius and his friend Richard Ritter created the Scherbius & Ritter company which specialized in all sorts of innovative technologies. Scherbius took interest in the cryptography system that seemed to be short-falling. Being involved with the new technology, he decided to use it to improve the cryptography system. The result was the Enigma, practically an electronic version of the Alberti cipher disk. Scherbius' Enigma soon became a system of encryption that challenged the best cryptanalysts in history. A picture of the Enigma can be found in Figure 1.

3 How the Enigma Works

The enigma has 5 major parts. The keyboard, the plugboard, the scramblers, the reflector, and the display. First, there is the keyboard through which the operator can type the message to be encrypted. The message is then sent through a plugboard where some letters are swapped while the rest are left the same. For example the letters A and P may be swapped. In that case, if A or P is typed, a P and A respectively would

Figure 1: This is an image of the enigma.

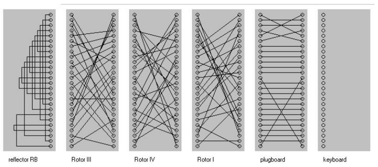


Figure 2: This shows the inner workings of the enigma.

come out of the plugboard; however, a different letter like C, would remain a C coming out. The plugboard consisted of six transpositions; 14 letters were fixed by the plugboard permutation.

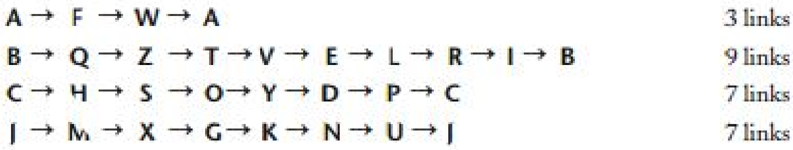
The next step is a rotor system, called the scramblers, which make up the most important part of the machine. The scrambler is a thick disc with random internal wiring. The wires enter the scrambler at random points, and randomly relocate themselves inside the disks, before emerging at random points on the other side. Scherbius also intended for the disk to rotate each time a letter was typed. So, if the same letter was typed twice in a row, two different letters would be the output. This will help lose repetition which aids cryptanalysts. Since one disk would just have the letter encryption repeat after the first complete revolution of the disk, there were three disks, when the enigma was first created. The following disk only turning each time the previous disk has completed a full revolution.

Finally came the reflector. The reflector just reflected the signal back to the lamp board where the cipher text letter lit up. When the Germans wanted to send a message, they would type their message into the enigma, gain the cipher text, and then send the encrypted message over the telegraph. The receiver could type the cipher text into the enigma and gain the message. They both had to have, however, the same set-up which was the key.

4 Breaking the Enigma

4.1 The Start

At that time, the Enigma seemed intimidation to break. We can count the number of set-ups, or keys, there are. There are 26 x 26 x 26 scrambler orientations, there are 6 scrambler arrangements, and 100,391,791,500 ways to swap six pairs of letters in the plugboard. This accumulates to over 10,000,000,000,000,000 ways to set up the enigma and the cryptanalyst has to find the single one of those that is the actual key. To put this in perspective, a persistent person would need longer than the age of the universe to check every setting if they are really quick and can check one setting every minute . Now, it may seem that majority of the arrangements are coming from the plugboard, and that it seems necessary for the other parts of the enigma. However, the plugboard on its own would just be a mono-alphabetic substitution which would be



A → F → W → A	3 links
B → Q → Z → T → V → E → L → R → I → B	9 links
C → H → S → O → Y → D → P → C	7 links
J → M → X → G → K → N → U → J	7 links

rather easy to break.

While many nations quickly gave up on cracking the enigmatic enigma, Poland persevered. With the help on an German insider, Hans-Thilo Schmidt, they were able to obtain details on how the enigma worked. Schmidt's documents detailed how the Germans used the enigma as well. Each month, Enigma operators received a codebook, detailing a key for each day. The codebook would specify the plugboard settings, scrambler arrangement, and scrambler orientations. The key would be used for the day and switched the following. However, the Germans realized that by using the same key all day, the enemy might get enough material to deduce the code. So, they used the day code to send new scrambler orientations to the receiving operator. To ensure receipt; however, this arrangement was typed twice.

A Polish mathematician, Marian Rejewski, was one of the leaders in breaking the Enigma. Rejewski used the repetition of the keys to help break the enigma. The Germans had this repetition in order to avoid mistakes; little did they know, it would jeopardize their security. Rejewski worked with intercepted messages that all began with the six letters of the repeated three-letter message key, all encrypted according to the same agreed day key. In each message, the first and fourth letters are encryptions of the same letter. Similarly, the second and fifth letters and the third and sixth letters are encryptions of the same letter. This repetition allowed Rejewski to deduce some constraints on the initial setup of the machine. With enough messages in a single day, Rejewski could complete an alphabet of relationships. He began to create chains of letters. For example, Rejewski noticed that although the plugboard and scrambler settings both affect the chains, the number of links in the chains, is only affected by the scrambler settings. With the help of insider information from Schmidt, he built a chart with the 105,456 scrambler settings and the chain lengths they generated.

Now each day, Rejewski could find the number of links of the day encryptions and then find which set ups had the right number of chains and links in each chain. He would know the scrambler settings for that particular day. Rejewski still had to; however, determine the plugboard settings. He could generally just type the ciphertext into his enigma replica and then guess the plugboard settings.

5 The Legacy

5.1 German Improvements

Germans soon made an alteration to the way they transmitted messages, Rejewski fought back. This caused the old values of chain lengths to be useless. Rejewski decided to mechanized the system of charting chain lengths and links to also search for the correct scrambler settings. Rejewski's had six of his machines working in parallel, one for each scrambler arrangement. His machines were called bombes. They would rapidly check through each of the 17,576 settings to find the correct scrambler orientation.

5.2 The Great Legacy

In 1938, German cryptographers increased Enigma's security. They gave Enigma operators two more scramblers, so that the scrambler arrangement might involve any three of the five scramblers. Additionally, the internal wirings of these new scramblers were not known. The number of possible keys increased to over 159,000,000,000,000,000,000. Rejewski did not have enough resources to build enough bombes and check every scrambler setting. The methods were turned over to larger countries who did have the resources but the Polish were left behind.