Scott Maxa and Kristen Cunningham

Dr. Moyer

Cryptography

January 22, 2020

Coding Enigma – Outline

1. History

During this section we are going to focus on the history of the enigma machine pre-WWII. We are going to talk about its original use, how it was modified for being used during WWII, and how it was implemented during WWII including the key system it was dependent on.

1. Breaking Enigma

In this section we are going to specifically explore the various different factors that led to the breaking of the enigma. For one, the Polish had already been working on breaking enigma for many years prior to the war. The Polish shared the research that they had a head start on collecting with the other Allied parties once the Germans starting using the enigma during WWII. We will also discuss the different keywords that started being hints for codebreakers, such as common German phrases and German soldiers’ habit of talking about their girlfriends over encrypted messages. Lastly, we will mention how even when the enigma was broken, the allied powers different take advantage of all of their new intel in order to not tip off the Germans that they had broken the machine.

1. Navy

While the codebreakers were careful not to tip off the Germans that the enigma had been broken, a general in the navy had the gut feeling that it had been broken. This general then decided to add an extra rotor to the enigma machines used by the navy, which was then called M4.

1. Inner-Workings – Rotors

Here we will just have technical explanations of how the rotors in the enigma machine worked. We are going to talk about the inner wirings, how the starting points effected those wirings, and the shift factors for each of the rotors. We are also going to talk about something called the “knock out” effect, which neither of us have heard about before but showed up in a couple of our resources.

1. Inner-Workings – Reflectors and Plugboards

In this section we are just going to quickly go over the reflectors and the plugboard components of the enigma machine. We will talk about the order of the level of encryptions that the plaintext goes through while it is being encrypted. The main point of this slide is that the vital flaw, that a letter can’t map to itself, occurs in the reflector.

1. Implementation

During this section we are only going to highlight a couple of cool parts of our programming of the enigma machine and how we implemented certain aspects.

1. Demo
2. Trivia

This is our class activity where we plan to quiz the class on the information they had just seen in our slides while also having fun by rewarding correct answers with candy!

MC Questions

1. How many different rotors are there?
   1. 26
   2. 8 \*\*\*
   3. -4
   4. 9
2. How many possible plugboard wires are there?
   1. 10 \*\*\*
   2. 15
   3. 256
   4. 1.7
3. What were the two codenames for M4?
   1. Tom and Jerry
   2. Mermaid Man and Barnacle Boy
   3. Shark and Triton \*\*\*
   4. Peter and Anne
4. Which step of the process contained the vital flaw?
   1. First Stage – Plugboard
   2. Second Stage – Rotors moving forward
   3. Middle Stage – Reflector \*\*\*
   4. Third Stage – Rotors moving backward
   5. Last Stage – Plugboard
5. Which was not a German key phrase exploited by the codebreakers?
   1. Heil Hitler
   2. Cilli
   3. Weather report
   4. Quotes from Marx’s Communist Manifesto \*\*\*
6. What was the vital flaw in the design of the enigma machine?
   1. It was heavy
   2. A letter couldn’t be itself \*\*\*
   3. The rotors would cut operators fingers
   4. The plugboard could map letters to itself

(\*\*\* Indicates the Correct Answer)