Kristen Cunningham and Scott Maxa

Dr. Moyer

Cryptography

January 16, 2020

Coding Engima – 5 Sources

Source 1: Standford.edu (<https://web.stanford.edu/class/cs106j/handouts/36-TheEnigmaMachine.pdf> - Handout)

This website explains the basic functionality of the engima machine. It describes the rotors codependent movements, such as the first rotor shifts every letter, the second every 26 letters and the third every 676 letters, ignoring the knock out effect. It explains how all of the connections within a rotor a hardcoded and concrete. One important thing to note from this site is that the rotors shift with each key click, meaning the shift occurs before the actual letter is encoded. It also shows in a diagram how once the plaintext passes through the rotors once it goes through a reflector before passing back through the rotors for a second time.

Source 2: Codesandciphers.org (<https://www.codesandciphers.org.uk/enigma/enigma2.htm>)

This source mainly consists of the connections of all the rotors and reflectors. It is a short page that lays out for each rotor (1, 2, 3, 4, 5, 6, 7, 8, Beta, Gamma) which plaintext alphabet letter maps to what ciphertext alphabet letter. We based all of our rotor wirings off of this page. This page also introduced certain rotors “knock out” effects which we had not previously known about. These knock out effects essentially shifts the 3rd rotor prematurely if the letter is used in one of the three rotors.

Source 3: theguardian.com (<https://www.theguardian.com/technology/2014/nov/14/how-did-enigma-machine-work-imitation-game> - Article)

This article has step by step graphics that show the encryption process of the enigma machine. We found it very helpful for putting together all of the steps and practicing tracking a single plaintext letter as it is encrypted into a ciphertext letter. This article also contains some information regarding the Bombe machine that Alan Turing created.

Source 4: plus.maths.org (<https://plus.maths.org/content/exploring-enigma>)

This source mainly focuses on the historical information regarding the enigma machine and WWII. It talks about the plugboard aspect of the machine, which was added to create another level of complexity from the original machine used before the war. It also talks about Bletchley Park and the people who worked to decrypt the machine. This includes the certain phrases that the Germans put into their messages that gave the British hints for what the key could be. A nice part of this site is that it math practice problems where you can practice portions of the enigma encryption process to better understand what is happening.

Source 5: The Essential Turing (Whitworth Library – Print)

This novel is all about Alan Turing. It does not only focus on his work during WWII building the bombe machine and breaking the enigma machine, it explores his life events before he got to Bletchley park. It talks about the specific effects that Turing and his work had on the development of computers. A particularly interesting part to me is that there is also a section that discusses the impact that Turing and Charles Babbage had on each other’s lives. Instead of focusing on the mechanics of the enigma machine like most of our other sources, this book explores the impact that Alan Turing had on the world, and much of Turing’s intellect was shaped by his experience breaking enigma and building the Bombe machine.