Honors Capstone Reflective Critique

Adam Downs

May 2, 2023

The Enigma Machine was a cipher used by the Germans in World War II to encrypt their communications. It was subsequently broken by British cryptographers at Bletchley Park, which provided valuable information to the Allies throughout the war. Literature is scattered regarding the methods used to break these messages. There is also a lesser-known version of the Enigma Machine used by the German Navy that utilized a fourth rotor in addition to more robust methods of disguising message settings. The goal of this capstone research was to compile a more complete view of how these machines operated and were cryptanalyzed.

Using Maple software, we continued to develop applications that simulate the processes we explored. We have a Maplet simulator that demonstrates how the Turing Bombe and Checking Machine would determine a logically consistent set of plugboard partners for three and four rotor Enigmas for a particular set of rotor orders, reflector, and ring settings for a given set of assumed window letters. In addition, our Maplet can determine when logically inconsistent plugboard partners rule out a particular set of settings completely or demonstrate when a false stop occurs.

For messages encrypted by the Army and Air Force Enigmas, we demonstrated how the process of Clonking allows one to recover the actual ring settings that were used by all Enigma operators on a particular day, thus allowing one to discover each operator's window settings. This resulted in the ability to decipher all messages encrypted by each Army and Air Force German Enigma operator for a particular day.

Finally, we continued the development of Maplets that demonstrated how the Navy German Enigma operators communicated individual window letter settings to each other in a more secure way than the Army and Air Force operators. We were able to demonstrate that the Enigma Navy operators' individual window letters could be determined by a capture of key setting sheets, and then the individual window letter settings could be recovered using a common German crib.

The developed software helps to guide users through a simulated cryptanalysis process, providing visual representations of various stages of the process and painting a clearer picture of the underlying methods. The developed applications cohesively describe the details of World War II Enigma Machine cryptanalysis. Understanding this historic example of the cryptanalysis of a seemingly unbreakable cipher helps to provide insight into the troubleshooting and problem-solving processes that are effective for these types of problems. There are many avenues for further exploration.

Although our Turing Bombe simulator can be programmed to test for all of the possible ring settings instead of one specific set of ring settings, it cannot complete this process in a reasonable amount of time. Improving the speed of the program would likely require re-programming certain portions of the code more efficiently or using a faster programming language than Maple. Though we worked towards this over the course of this research, the process ended up being too time consuming and we had to move on to our other goals.

Another avenue for further exploration is the process of recovering the German Navy operators' individual window letter settings. We did not have the opportunity to discuss this process, which is more difficult than that for the Army or Air Force when the key sheet settings were not captured.