Annotated Bibliography

Calderbank, Michael. *The RSA Cryptosystem: History, Algorithm, Primes*, 20 Aug. 2007, math.uchicago.edu/~may/VIGRE/VIGRE2007/REUPapers/FINALAPP/Calderbank.pdf

This paper written by Michael Calderbank explores Rivest Shamir Adleman (RSA). The paper starts by going over the history of the RSA algorithm and how the algorithm came to be. In this portion of the text, Calderbank writes about the need for an asymmetric way of encrypting, and the problems with symmetric encryption. Next, Calderbank goes in depth about the RSA algorithm and how it works. Calderbank goes over the math involved in RSA encryption and decryption, and how the public and private keys are created and used for encryption and decryption with RSA. Lastly, Calderbank test theorem's regarding prime numbers and Carmichael numbers within RSA.

Ellis, Claire. *Exploring the Enigma - plus Maths*, Mar. 2005, plus.maths.org/issue34/features/ellis/2pdf/index.html/op.pdf

Claire Ellis's paper on "Exploring the Enigma" writes all about the Enigma machine and how it works. The first part of the paper explores how the Enigma machine came to, and then addresses how the machine worked. This article helped in understanding the complexities of the Enigma machine by explaining how to set up the machine, how the rotors worked, and how the other electrical and mechanical components worked together to encrypt messages for the German military. Lastly, Ellis writes about Bletchley Park, a school for code and ciphers created by the British, that worked on decrypting the Enigma machine.

Kotas, William. “A Brief History of Cryptography.” *A Brief Hist A Brief History of Cryptography*, 5 May 2000, trace.tennessee.edu/cgi/viewcontent.cgi?article=1398&context=utk_chanhonoproj.

This paper written by William Kotas covers several different types of cryptography. This paper covers the evolution of cryptography, and how encryption methods have gotten better throughout time. This paper was useful to me because it covered the three encryption and decryption algorithms used in my project. On page 5 to page 6, Kotas covers the Caesar shift cipher, explaining how it works and what Julius Caesar did for the cipher. On page 20, Kotas starts to cover the Enigma machine. Within this text Kotas writes about how the Enigma machine evolved from a version that only allowed for 17,576 different outcomes, to the several trillions of different outcomes that we saw closer to the end of World War 2. Kotas’s coverage of the Enigma machine in this portion of the article provides great insight regarding the issues and the successes with the Enigma machine. Lastly, on page 36 Kotas begins to cover the RSA algorithm. Kotas breaks down the use of RSA and how RSA was created.

Levinsky, Jacob. “Encryption: The History and Implementation.” *SUNY Open Access Repository (SOAR)*, Dr. Knarik Tunyan, May 2022, soar.suny.edu/handle/20.500.12648/12073.

This paper written by Jacob Levinsky covers all the topics included in my project and their history. Levinsky starts by defining the difference between cryptography and encryption, mentioning that encryption falls under the same umbrella as cryptography. Levinsky then on page 6 covers Julius Caesar and the Caesar cipher. Within this, Levinsky discusses how the Caesar cipher worked and some interesting facts about the cipher. Levinsky then discusses modern encryption, and the Enigma machine starting on page 8. Levinsky does

not go very in depth about the Enigma machine but gives credit to the importance of the machine in modern encryption.

Perendi, Daniel, and Prosanta Gope. *The Language's Impact on the Enigma Machine*, 13 Nov. 2015, eprint.iacr.org/2021/1434.pdf.

This paper written by Daniel Perendi and Prosanta Gope covers the Enigma machine, but mainly follows the idea of using another language rather than English that incorporates more characters and the effect this would have on the Enigma machine. This paper helped in understanding the Enigma machine, along with some of the history behind it. Although the testing of other languages does not impact my project directly; it allowed me to gain a better understanding of the Enigma machine and how it works.

Prasad, Kalika, and Munesh Kumari. "A Review on Mathematical Strength and Analysis of Enigma." *arXiv.Org*, 17 Apr. 2020, arxiv.org/abs/2004.09982.

This paper written by Kalika Prasad and Munesh Kumari provides a lot of insight on the innerworkings of the Enigma machine and how secure the machine truly was. First, the paper covers the creation of the Enigma machine, providing lots of facts about the breaking of the Enigma machine. Next, the paper goes through the Enigma machine's structure including information about all its parts and descriptions of how they work within the machine. The paper then ends by going over several mathematical equations to try to figure out the strength of the Enigma machine.