Grant Combs

Dr. Horn (advisor), Dr. Appleton, Dr. Sarkela (still awaiting response)

CS480

10 September 2021

Senior Project Proposal

For the past several years, I have been interested in the encrypting and decrypting of messages, or "cryptanalysis", as it more formally is called. From sending ciphered letters to my friends to learning about the Enigma machine and the Zodiac Killer's infamous letters, codebreaking has turned into a fairly substantial extracurricular hobby throughout my time in college. Due to my interest in the topic, I would like to design a program that is able to decrypt messages via a variety of codebreaking techniques.

The idea is as such: the user enters the encrypted message, then is asked whether they know the method through which the message was encrypted. If so, they can select the method, and the program will attempt to decode the message. If not, the program can provide useful information regarding the cipher, such as the frequency of each letter, if there are any common recurring patterns, and more. Using this information, the program will be able to suggest what technique was used to encrypt the message, then attempt to decrypt it.

I will first develop a user interface. I plan to use Visual Studio's Windows Forms Designer for this aspect of the program. As I have never used or have had experience with Windows Forms Designer, this will require a great deal of learning. This will, however, restrict my program to working with Windows only. Once I establish the basic user interface, I will be

able to add decryption methods one-by-one. As there are an infinite number of ways to theoretically encrypt/decrypt a message, I will add methods in until I am satisfied with the thoroughness of the program. The program will be written in C++, a language in which I am fairly well-versed and with which I am reasonably comfortable using for a project of this size.

Another great area of learning will be in learning to code algorithms for decrypting messages. While I am familiar with deciphering messages by hand, I have never put much thought into generalizing the methods I use and developing them into a user-friendly program. Additionally, I am sure that there are a great number of algorithms of which I am not yet familiar, which will be both relevant and education in the context of this project.

Overall, the goal is to develop a code-breaking application for Windows using C++ and Visual Studio Windows Forms Designer. I will learn how to use Windows Forms Designer, as well as algorithms behind the deciphering of enciphered messages; additionally, the project is scalable due to the ability to add deciphering techniques as I see fit.