CS110 Group Project Proposal

Members: Ryan, Cory, Adam, Nate, Prof. Mohan

For our final project, our group chooses to investigate and dive deeper into cryptography. In doing this we will investigate multiple methods and algorithms used to encrypt and decrypt messages. This will allow us to gain a greater knowledge of how each different algorithm is used in encryption and decryption. This will give us a better understanding so that we can begin to develop our own methods and algorithms for this process. We will also develop a method that allows users to send and receive encrypted messages which can then be decrypted by running the message in our program. The encryption method, which we investigated during a laboratory assignment, was CaesarCypher. CaesarCypher used the ASCII Unicode values of each character and then added a specific integer value to the ASCII value. This, in turn, returned a character which was a specific number away in the alphabet. This could then be subtracted to show the original method. This is a very basic form of cryptography. For the project, we plan to investigate more advanced cryptography methods. Upon doing research, we have found a large number of frameworks in the Java API which support and contain many secure cryptography algorithms. Along with this, there are already many highly advanced and effective algorithms that have been developed and can be used in Java, including ElGamal, DES, DH, MD5, SHA-1 and DSA (Java Cryptography, pg. 24-25). We plan on furthering our studying in these different methods to help us better reach our goal. Our goal in this project will be to create an algorithm which uses some of the methods used by other algorithms and also some of our own methods to ultimately complete the same task in a new and creative way. When this algorithm is successfully developed, we hope that it will allow for users to send a message that will be encrypted as it gets inputted. Then we will attempt to reverse engineer this algorithm in order to support decryption of messages. Finally, we will work on sending and receiving encrypted messages via some platform such as E-Mail. After this is all implemented we will attempt to make the whole program very user-friendly and hopefully create a helpful UI which allows the user(s) to effectively use our program.