Project 1 Report

Andrew Cox, Sebastian Martin, Joy Ray, and Xiyauan Zheng

In Task 2, when encrypting the picture with ECB mode it is very noticable about the general idea of what the picture could be. With ECB mode you can see the outline of the shapes and also the color of the each shape in the picture. When encrypting with CBC mode there is nothing distinguishable about the picture. If viewing the picture with no prior knowledge of the original picture someone would not be able to derive the original picture.

In Task 3, the plain text file was encrypted with both CBC and ECB mode, then the encrypted file was corrupted before it was decrypted. More information could be pulled from the corrupted ECB file compared to the CBC file. This is because in ECB (Electronic Code Book) encryption, each block is encrypted separately and thus are independent of one another, so when the encrypted file was corrupted, only the block in which the corruption occurs is affected. In CBC (Cipher Block Chaining), on the other hand, each block is attached to the end of the previously encrypted segment before being encrypted, so just corrupting a single block can mess up multiple blocks in the file. If more than one bit is corrupted when encrypting/decrypting with CBC, more information will be destroyed in the decrypted file.

OpenSSL is a cryptography toolkit implementing the Secure Sockets Layer and Transport Layer Security network protocols and related cryptography standards required by them. OpenSSL allows for many users to use a number of encrypting and decrypting algorithms, and also the choice of the encryption mode. OpenSSL allows user to encrypt using an initialization vector which is an arbitrary number that is used with a secret key. If an IV is used then it prevents repetition in the data encryption so it would be harder for a hacker to find patterns to break the cipher. The IV basically adds for extra security while encrypting data. An initialization vector can not be sent over the internet in plaintext it must be encrypted first. Modes are important because they provide confidentiality or authenticity which are two of the main goals of cryptography.

Team Contributions:

Andrew Cox:
Completed Task 1-3 individually and wrote the encryption code for Task 4. Assisted some team members with setting up the virtual machines.

Sebastian Martin:
Completed Task 1-3 individually and wrote code to handle the text reading for Task 4.

Joy Ray:
Completed Task 1-3 individually and wrote the report for Project 1.

Xiyanauan Zheng:
Completed Task 1-3 individually and wrote the readme files for the tasks with screenshots for each step.