**Crypto Project Overview**

*Author: Himesh Buch*

*Date: 4/28/2020*

**Team members:**

Aaron Argueta (Team leader)

Himesh Buch

Yash

Deep Ghodasara

Unnit Patel

Shreyas Adhiya

**Introduction:**

We have used Block, Stream, and RSA key encryption cipher methods for this project, and we were successfully able to implement attacks like, Known Plaintext attack, Ciphertext-only attack, Chose Plaintext attack, and chosen ciphertext attack. The code along with the video presentation of it will be submitted.

**Basic understanding of the attacks:**

*known plaintext attack:*

Chuck has access to both plaintext and encrypted version

*chosen plaintext attack:*

Chuck will send plaintext to get the ciphertexts back

*chosen ciphertext attack:*

Chuck will send ciphertext and get plaintext back

*ciphertext only attack:*

Chuck has access to ciphertexts

**Ciphers:**

For block cipher, we have used a triple key encryption DES system for encrypting and decrypting the messages. For stream cipher, the code uses the key and converts the messages into a binary format of 1s and 0s, which will be the encrypted message. For RSA key encryption, we have used the RSA java library for encryption and decryption. It has been encrypted using the private key that the code generates and uses the public key to decrypt the messages.

**Sources:**

Research from google and example codes, and to stack overflow and Wikipedia to understand the concepts of different attacks and ciphers