**Crypto Project Overview**

*Author: Himesh Buch*

*Date: 3/26/2020*

## Team members:

Aaron Argueta (Team leader)

Himesh Buch

Yash

Deep Ghodasara

Unnit Patel

Shreyas Adhiya

### Crypto Modes:

We will be implementing these three crypto methods for the final project. The basic user interface for the project is ready, along with the backend server. The final step is to code these algorithms and do final testing

#### Known plaintext:

In this attack, the adversary will have access to some parts of the ciphertext and its corresponding plaintext. Once it sees that, it will try to figure out the key and, in the end, will be able to decrypt all messages

Things to know for coding:

1. Let the adversary know the first two letters of the plaintext and its corresponding ciphertext
2. We will use affine ciphertext decryption scheme here to decrypt the messages
3. More info on that can be found here: <https://www.youtube.com/watch?v=ry3g0xN8QKU>

#### Chosen ciphertext:

In this attack, the adversary will send an encrypted message to the oracle and tries to figure out the key. Here is an example:

1. Alice and Bob will send each other ciphertext via oracle and will receive plaintext in return
2. The imposter Chuck will do the same and send ciphertext messages to the oracle and will receive plaintext in return
3. He then will have to encrypt those plaintext messages and will figure out what the key is

Things to know for coding:

1. Alice will send some ciphertext to Bob, and Bob will receive plaintext version of it
2. Chuck will do the same and once he gets the hold of plaintext, he will try to encrypt the plaintext and will figure out what the key is
3. Once he has the key, he will be able to view Alice and Bob’s messages
4. This attack is somewhat similar to chosen plaintext attack

#### Chosen plaintext:

In this attack, the adversary will send a plaintext and tries to figure out the key. Here is an example:

1. Basically, the oracle will encrypt a plaintext message and send back a decrypted version of it
2. Alice and Bob will send each other plaintext via the oracle, but those messages will appear as ciphertext because the oracle will encrypt the message with some encryption scheme
3. Chuck will need to figure out what the key is, and eventually, figure out the plaintexts that Alice and Bob are sending to each other
4. Chuck will also send a message to the oracle and will receive a ciphertext. He then will decrypt it and figure out what the key is
5. He will use this key to decrypt the messages of Alice and Bob

Things to know for coding:

1. First, design an encryption scheme to encrypt plaintext to ciphertext
2. Send messages from Alice to Bob and vice-versa, and only display the ciphertext
3. Make Chuck send a message to oracle, and he will also receive a ciphertext
4. Use that ciphertext to figure out what the key is
5. Now, use that key to decrypt all the messages Alice and Bob have sent to each other and display it
6. Since, all three of them are in the same system, we can assume that they all have access to all the messages

### Future directions:

Here are the responsibilities of each members for the rest of the project:

Yash and Aaron: will work on known plaintext attack scheme

Himesh and Unnit: will work on chosen ciphertext attack scheme and putting everything together

Shreyas and Deep: will work on chosen plaintext attack scheme

*A video presentation is also required, and we plan on recording individual clips along with a practical example of the project*