Darrel Chang
Tingting Chen
CS 4600
5/15/23

Final Project Report

System Design:

The program, created using python’s cryptography library, consists of two main components. I implemented two classes. One sender class and one receiver class. When instantiated, each will produce a key pair and store the public key in a “public_info” folder that is known by anyone. The private key will be stored in a “private” folder that only they are supposed to know.

Encryption Process:

The message sent is encrypted using the symmetric encryption scheme AES-256 CFB. The symmetrically encrypted message is encrypted along with the AES key using the RSA public key of the recipient, to ensure that only the recipient can decrypt it using their private key. An HMAC with SHA-256 is used to generate a MAC for the encrypted message as good practice, to ensure its authenticity and data integrity can be checked before it is decrypted.

How to use:

1. Instantiate an object of each class (Sender and Receiver)
2. The sender may send encrypted messages using the encrypt_message function, which takes a string message, and a Receiver object as the recipient of the message. The function will return if the message was transmitted successfully.
3. The receiver can then decrypt the message by calling the decrypt_message function, which takes the filename.txt of the encrypted message. It will display if the HMAC was successfully verified and then display the decrypted message.