Susana Noto
PS2

Problem Set 2 Report

In order to understand the cryptography library, I spent a lot of time reading over the Juniper Notebook and other documentation. I wanted to ensure I spent a lot of time understanding the concepts before I tried to code.

The next thing I did was outline the functions and make sure they were clear, as my last assignment did not have separate functions. Then I went about tackling the different functions, starting with loading the key files. Then I went to the encryption and then decryption functions.

I used a symmetric AES key and RSA encryption. The key size is 2048 to ample security, but not a crazy large key size. I also used OAEP mode and SHA256 hash function. RSA is a widely used encryption system, and for similar reasons I used OAEP. I used SHA256 to avoid collisions while still having a secure hash. For AES, I used CFB mode with a 128 bit IV. I liked CFB because it does not require padding, and a 128 bit IV ensures randomness. For the signatures, I used RSA digital signature and MFG1 with SHA256 and a maximum salt length. All of this was done to ensure high security so signature forgery is not likely.

Overally, I did a lot of research in the cryptography library to ensure that I utilized the library for maximum security and simplicity. Lastly, I created a testing script that generates keys to help ensure that the code works when using command line arguments.