4130 HW 4

Matthew Fisher

For this homework, I implemented RSA encryption and decryption by applying fundamental cryptographic ideas with Python's cryptography package. Creating a 4096-bit RSA key pair was the first step in my implementation choice to guarantee strong security in line with current cryptographic standards. A file called key.pub contained the public key, and the private key was safely kept. I then made a message.txt file in ASCII format that contained plaintext messages.

I decided to use the private key to sign the plaintext message in order to guarantee its authenticity and integrity. In this phase, the cryptography library's sign() function was used using the SHA-256 hashing method. A file called signature.sig contained the generated digital signature. In order to confirm the message's origin and guarantee that it was unchanged during transmission, my solution made sure that this signature could be later validated using the public key.

I decided to encrypt using the public key that was supplied by Dr. Nur and kept in a PEM file. The cryptography library was used to load this key, and the plaintext message was securely encrypted using the RSA-OAEP padding method with SHA-256. An extra degree of protection against cryptographic assaults was offered by the selection of RSA-OAEP. Because it could only be

decrypted with the matching private key, the encrypted message was stored in message.encr, guaranteeing security.

Four files were produced as a result of the homework: message.txt (plaintext message), signature.sig (digital signature), message.encr (encrypted message), and key.pub (public key). Throughout the project, I made implementation decisions that prioritized following safe procedures, utilizing strong cryptographic algorithms, and generating output files that were organized. This homework reinforced the significance of RSA encryption in safeguarding the CIA Triad of Info Sec by providing me with important experience with encryption, decryption, and signatures.