Name: Grishma Vemireddy

Student ID: 2045611

Problem 1: Successful Validation

Given the task of encrypting the sender's message using public-key encryption (RSA), producing a hash for integrity check, signing the hash to ensure that it came from the sender and verifying the signature. I used the preferred parameters: key_size = 2048, Hash: 'SHA-256' and sign_hash() in the program. Following the directions listed in the python RSA documentation and in homework instructions. I have 2 classes: Sender class and Receiver class. In the Sender class, I have 3 functions: the constructor _init_ , the encryption function, and sign function. Following the methods found in the RSA documentation, I initialize public and private key using rsa.newkeys(key_size) and I send in the plaintext from main, encrypted using rsa.encrypt, hash using rsa.compute_hash(), and sign using rsa.sign_hash(). In the receiver class, I have a constructor _init_, decrypt function uses rsa.decrypt() and verify function uses rsa.verify(). I wrote the program using the functions/methods found in the RSA documentation,. I also print the decrypted message using .decode('utf-8') and print verification message.

The **output** of this program:

```
Decrypted message: Our primary objective remains unchanged: gather intel and
prevent the dissemination of classified information.

Agent Eagle
Verification: SHA-256
```

Problem 2: Simulation Attack (on message)

Given the task of modifying the main program to simulate an attack with someone changing the message after signing it. Following the suggestion in the instructions, the class definitions are same as problem 1. I only modified the code in main function from problem 1 to now first sign the original plaintext, then modify the plaintext by swapping the position 0 with position 2 and encrypt the modified plaintext. I decrypt the modified plaintext and verify by comparing the sign of the original plaintext with the modified plaintext.

The **output** for this program:

```
Decrypted message: ruO primary objective remains unchanged: gather intel and
prevent the dissemination of classified information.

Agent Eagle
Verification Failed
```

Problem 3: Stimulated Attack (on signature)

Given the task of simulating an attack on the signature, keeping the class definitions the same I performed an attack by intercepting the message and modifying the signature by swapping the first byte with the last byte and then I verify original plaintext with modified signature. Another attack I tried was flipping specific bits. Both of these attacks failed verification.

The **output** for this program:

```
Decrypted message: Our primary objective remains unchanged: gather intel and
prevent the dissemination of classified information.

Agent Eagle
Verification Failed
```