Swasti Mishra
Dr. Sun
COSC 366
1 November 2022

COSC 366 Written Assignment 3

Question 1

Symmetric & Asymmetric Crypto: Alice wants to send Bob a large data file containing confidential data. She wants to make sure the file cannot be modified undetected during transmission. All Alice and Bob have is their public/private key pair.

a) **Show how Alice will construct the message to be transmitted in a secure and efficient way.**

In this situation, it is likely that Alice will want to use RSA (Rivest–Shamir–Adleman) encryption, which is a method of asymmetric encryption. For Alice to construct a message for Bob in a secure and efficient way, Bob must first send Alice his public key. This key is comprised of two 1024-bit prime integers, n, the public modulus, and e, the public exponent.

b) **Show how Bob will extract the data file from the received message.**

Alice is now able to send Bob a message. Alice sends Bob the ciphertext, which is generated from the formula ciphertext = (plaintext)^e mod n. With this ciphertext, Bob now has an encrypted message. Bob can decrypt this message using Alice's private exponent (d) using the following formula: plaintext = (ciphertext)^d mod n. In this formula, n is the public modulus, and d is the private exponent. These are the two integers that make up an RSA private key.

Question 2: Encryption and Tag Generation using OpenSSL:

a) **Encrypt the message "The quick brown fox jumps over the lazy dog - [Your Name]" using AES-256-CBC and a key and IV of your choice.**

input.txt:

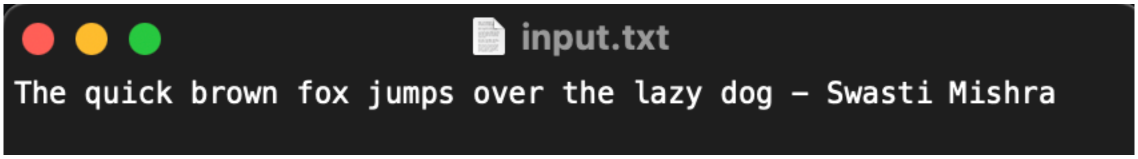
The quick brown fox jumps over the lazy dog - Swasti Mishra

keysIV.txt:

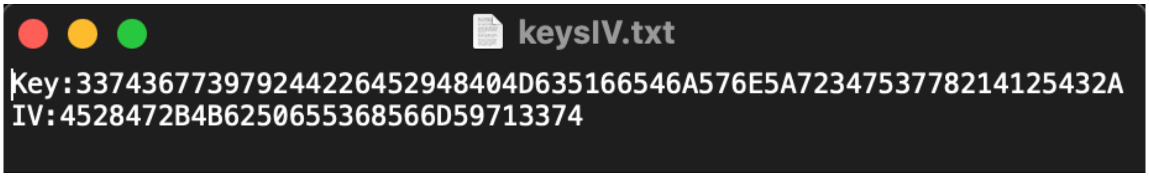
Key:337436773979244226452948404D635166546A576E5A7234753778214125432A
IV:4528472B4B6250655368566D59713374

cipher.txt:

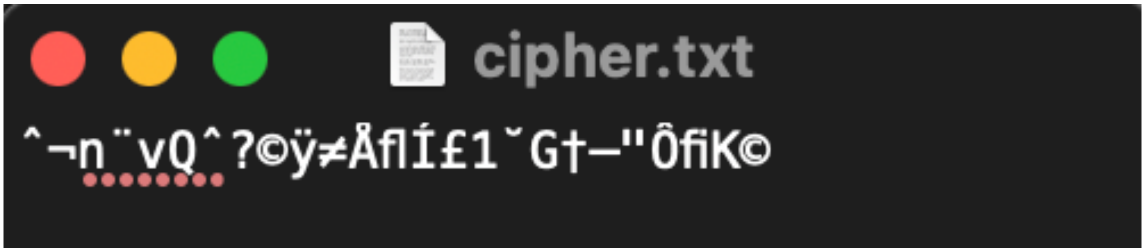
ˆ¬n¨vQˆ?©ÿ≠ÅflÍ£1˘G†—"ÔfiK©



```
The quick brown fox jumps over the lazy dog - Swasti Mishra
```

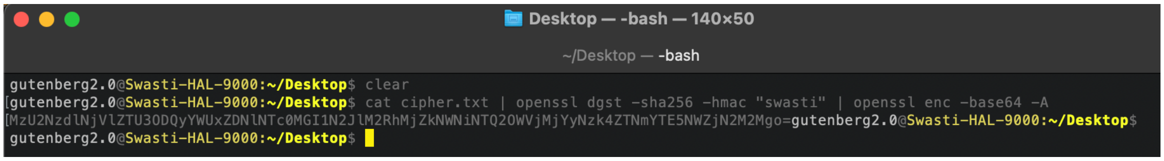


```
Key:337436773979244226452948404D635166546A576E5A7234753778214125432A
IV:4528472B4B6250655368566D59713374
```



```
^¬n¨vQ^?©ÿ≠ÅflÍ£1˘G†–"ÔfiK©
```

b) Generate a tag on the encrypted message using HMAC-SHA256 and a key of your choice (should be different from the encryption key).



```
gutenberg2.0@Swasti-HAL-9000:~/Desktop$ clear
[gutenberg2.0@Swasti-HAL-9000:~/Desktop$ cat cipher.txt | openssl dgst -sha256 -hmac "swasti" | openssl enc -base64 -A
[MzU2NzdlNjVlZTU3ODQyYWUxZDNlNTc0MGI1N2JlM2RhMjZkNWNiNTQ2OWVjMjYyNzk4ZTNmYTE5NWZjN2M2Mgo=gutenberg2.0@Swasti-HAL-9000:~/Desktop$
gutenberg2.0@Swasti-HAL-9000:~/Desktop$ 
```