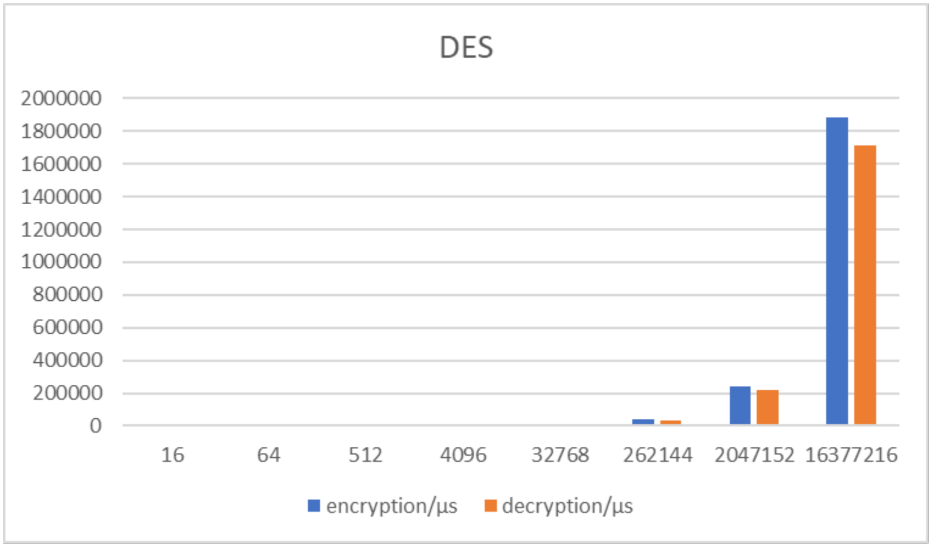
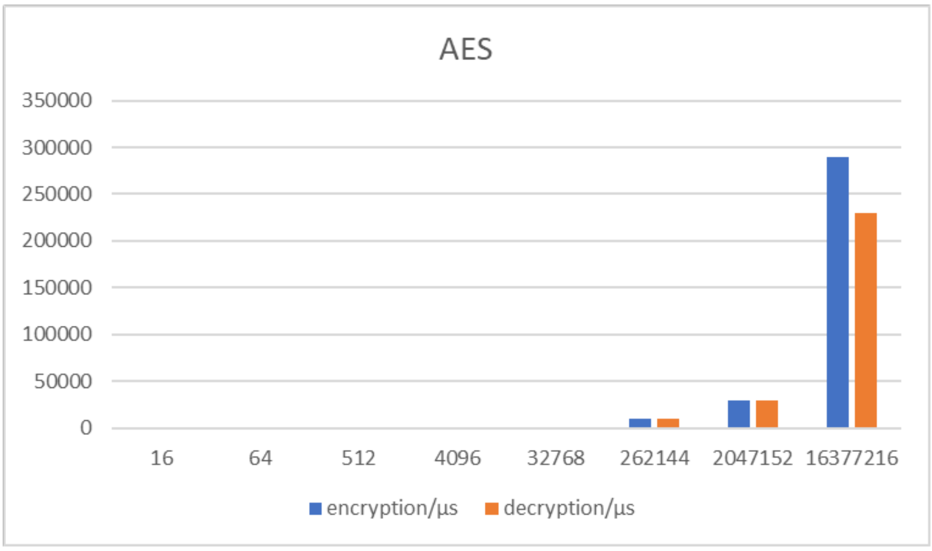
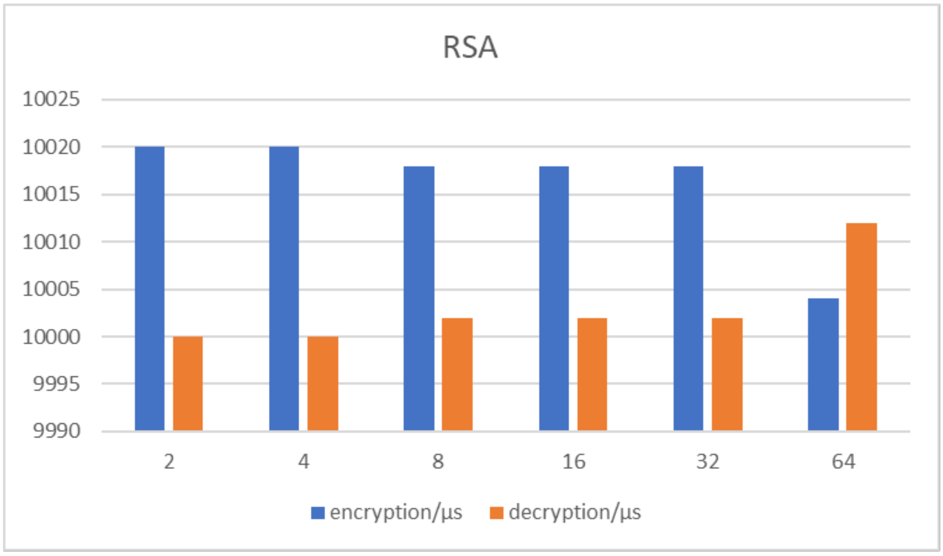
COMP4337 Lab 1 report

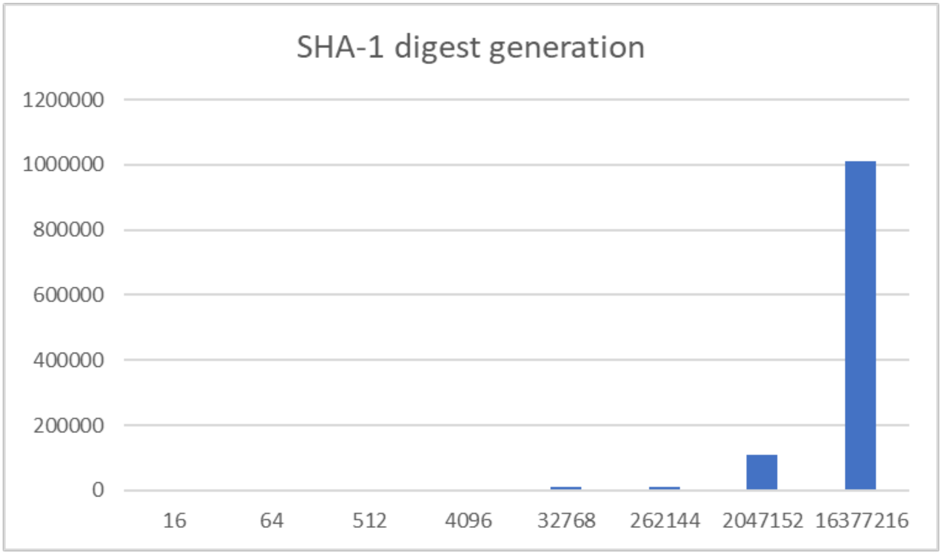
Shaoqian Zhou(z5244813) and Yimeng Gu(z5317610)

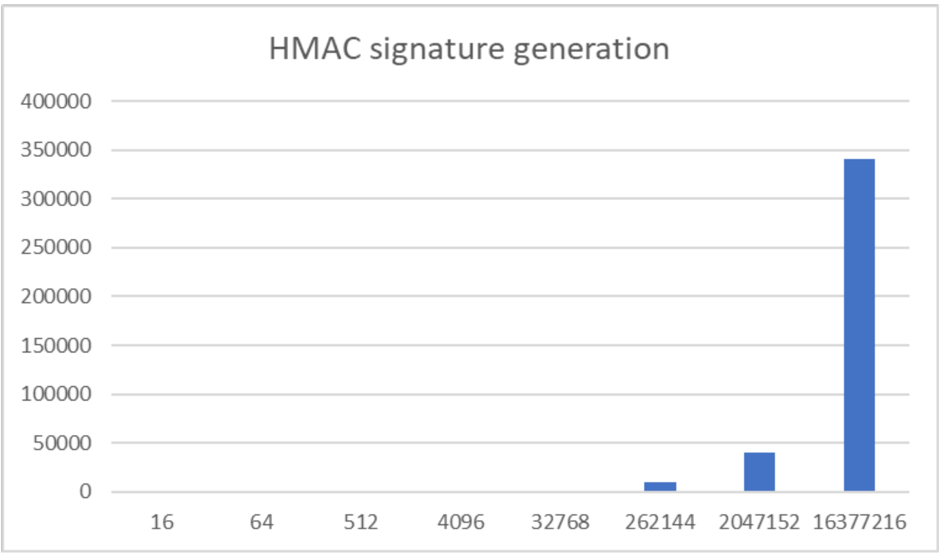
1. Programming language: Python
2. Graphs:






RSA
10025
10020
10015
10010
10005
10000
9995
9990
2
4
8
16
32
64
encryption/µs
decryption/µs


SHA-1 digest generation
1200000
1000000
800000
600000
400000
200000
0
16
64
512
4096
32768
262144
2047152
16377216


HMAC signature generation
400000
350000
300000
250000
200000
150000
100000
50000
0
16
64
512
4096
32768
262144
2047152
16377216

3. Questions

1. DES and AES: Both have their encryption and decryption time increasing exponentially with respect to the size of plaintext. However, DES takes longer to both encrypt and decrypt.

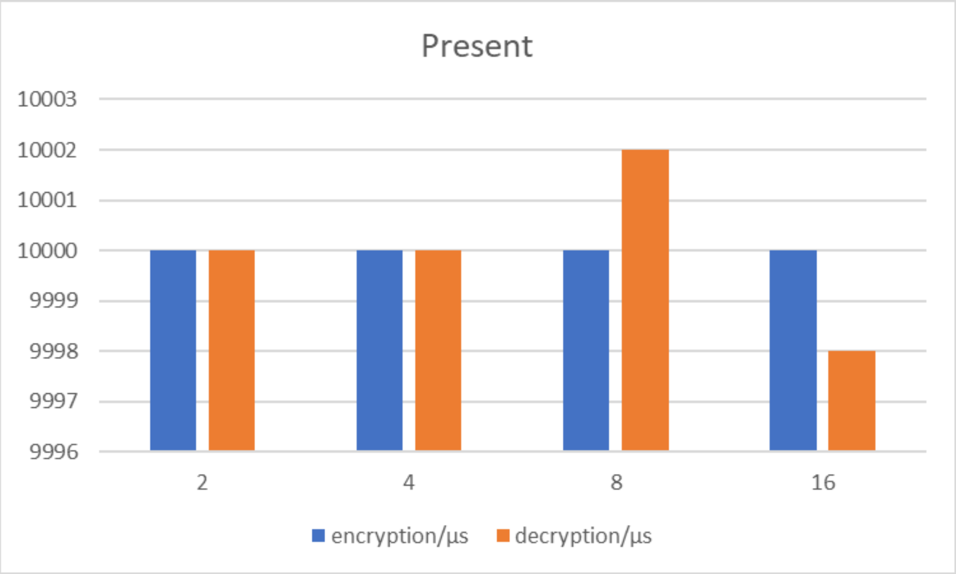
2. DES and RSA: RSA's encryption and decryption time generally do not depend on text size, whereas DES as mentioned above, takes exponentially longer time.

3. DES and SHA-1: SHA-1 is a hash algorithm that generates message digest, and the time it takes to do so is in the same order as DES does to encrypt/decrypt the same piece of message, which also increases nearly exponentially with respect to text size.

4. HMAC and SHA-1: HMAC is a hash algorithm that generates a hash signature for the sender of the message. The time it takes to do so behaves very similarly to SHA-1, i.e., increase nearly exponentially with respect to message size, except that it's an order lower than SHA-1.

5. RSA Encryption and Decryption: It takes approximately the same amount of time to encrypt and decrypt with RSA.

Part c



Since Plain_text requires 16 bytes, we generate samples of 2, 4, 6, 8, 16 bytes to test the PRESENT algorithm. The time it takes to encrypt and decrypt is almost the same for files of different sizes. Because if the size is less than 16 bytes, the algorithm will use 0 to complete the ciphertext, so it takes approximately the same time to run 2-byte and 16-byte files.