

## Task 1

The three different modes for encryption and decryption used in this task are:

1. aes-128-cbc
2. aes-256-cbc
3. aes-128-ecb

All the commands used for each mode are listed below.

### aes-128-cbc

Key generation: openssl rand -hex 16

Iv generation: openssl rand -hex 16

Encryption: openssl enc -aes-128-cbc -e -in task1\_plaintext.txt -out aes-128-cbc\_ciphertext.bin -K b620fa572f132b8a2575e81b3817aa2a -iv 25a88346fa6eeef62f29161821a62cbd

Decryption: openssl enc -aes-128-cbc -d -in aes-128-cbc\_ciphertext.bin -out aes-128-cbc\_decrypted\_text.txt -K b620fa572f132b8a2575e81b3817aa2a -iv 25a88346fa6eeef62f29161821a62cbd

### aes-256-cbc

Key generation: openssl rand -hex 32

Iv generation: openssl rand -hex 16

Encryption: openssl enc -aes-256-cbc -e -in task1\_plaintext.txt -out aes-256-cbc\_ciphertext.bin -K 3928e2ef636d90ce0f2cb4a9818503710574c0a7060717e23c11ef0ddab98a2a -iv 3baee6d1c1893a4c6d5c348355ce65ac

Decryption: openssl enc -aes-256-cbc -d -in aes-256-cbc\_ciphertext.bin -out aes-256-cbc\_decrypted\_text.txt -K 3928e2ef636d90ce0f2cb4a9818503710574c0a7060717e23c11ef0ddab98a2a -iv 3baee6d1c1893a4c6d5c348355ce65ac

aes-128-ecb:

Key generation: openssl rand -hex 16

Encryption: openssl enc -aes-128-ecb -e -in task1\_plaintext.txt -out  
aes-128-ecb\_ciphertext.bin -K 6f4e14265209aef2e6a888461a9f2f3

Decryption: openssl enc -aes-128-ecb -d -in aes-128-ecb\_ciphertext.bin -out  
aes-128-ecb\_decrypted\_text.txt -K 6f4e14265209aef2e6a888461a9f2f3