Lab-3 task –1

```
# AES-128-CBC
```

```
openssl enc -aes-128-cbc -e -in test.txt -out aes128cbc.bin -K 11223344556677889900aabbccddeeff -iv 20304050607082143234324324233333
```

```
openssl enc -aes-128-cbc -d -in aes128cbc.bin -out aes128cbcdecrypted.txt -K 11223344556677889900aabbccddeeff -iv 20304050607082143234324324233333
```

```
# AES-128-CFB
```

```
openssl enc -aes-128-cfb -e -in test.txt -out aes128cfb.bin -K 11223344556677889900aabbccddeeff -iv 20304050607082143234324324233333
```

```
openssl enc -aes-128-cfb -d -in aes128cfb.bin -out aes128cfbdecrypted.txt -K 11223344556677889900aabbccddeeff -iv 20304050607082143234324324233333
```

```
# AES-256-CBC
```

```
openssl enc -aes-256-cbc -e -in test.txt -out aes256cbc.bin -K 11112222333344445555666677778888 -iv 5a04ec902686fb05a6b7a338b6e07760
```

```
openssl enc -aes-256-cbc -d -in aes256cbc.bin -out aes256cbcdecrypted.txt -K 11112222333344445555666677778888 -iv 5a04ec902686fb05a6b7a338b6e07760
```

```
# AES-128-ECB
```

```
openssl enc -aes-128-ecb -e -in test.txt -out aes128ecb.bin -K 11223344556677889900aabbccddeeff
```

```
openssl enc -aes-128-ecb -d -in aes128ecb.bin -out aes128ecbdecrypted.txt -K 11223344556677889900aabbccddeeff
```

LAB 3 TASK 2:

```
openssl enc -aes-128-ecb -e -in sample.bmp -out encryptedImage.bmp -K 00112233445566778889aabbccddeeff
```

```
ghex sample.bmp &
```

goto byte 54

copy

```
ghex encryptedImage.bmp &
```

find and replace

see image in viewer

```
openssl enc -aes-128-ecb -d -in encryptedImage.bmp -out decryptedImage.bmp -K 00112233445566778889aabbccddeeff
```

```
ghex decryptedImage.bmp
```

find and replace

see image.

```
openssl enc -aes-128-cbc -e -in sample.bmp -out encryptedImageCBC.bmp -K 00112233445566778889aabbccddeeff -iv 20304050607082143234324324233333
```

```
ghex sample.bmp &
```

goto byte 54

copy

```
ghex encryptedImageCBC.bmp &
```

find and replace

see image in viewer

```
openssl enc -aes-128-cbc -d -in encryptedImageCBC.bmp -out decryptedImageCBC.bmp -K 00112233445566778889aabbccddeeff -iv 20304050607082143234324324233333
```

```
ghex decryptedImageCBC.bmp &
```

find and replace

see image.

LAB 3 TASK 3:

create a text file bigText.txt

```
openssl enc -aes-128-ecb -e -in bigText.txt -out aes128ECBencrypted.bin -K 00112233445566778889aabbccddeeff
```

```
ghex aes128ECBencrypted.bin &
```

go to 30th bit

change the HEX value

```
openssl enc -aes-128-ecb -d -in aes128ECBencrypted.bin -out aes128ECBdecrypted.txt -K 00112233445566778889aabbccddeeff
```

check the file

```
openssl enc -aes-128-cbc -e -in bigText.txt -out aes128CBCencrypted.bin -K 00112233445566778889aabbccddeeff -iv 20304050607082143234324324233333
```

```
ghex aes128CBCencrypted.bin &
```

go to 30th bit

change the HEX value

```
openssl enc -aes-128-cbc -d -in aes128CBCencrypted.bin -out aes128CBCdecrypted.txt -K 00112233445566778889aabbccddeeff -iv 20304050607082143234324324233333
```

check the file

LAB 3 TASK 4:

ECB = PADDING YES

CBC =   PADDING YES

CFB =   PADDING NO

OFB =   PADDING NO

```
openssl enc -aes-128-ecb -e -in text.txt -out ecb128encrypted.bin -K 00112233445566778889aabbccddeeff
```

```
ghex ecb128encrypted.bin &
```

```
openssl enc -aes-128-ecb -d -in ecb128encrypted.bin -out ecb128decrypted.txt -K 00112233445566778889aabbccddeeff
```

this one is larger after endryption meaning it has padding

```
openssl enc -aes-128-cbc -e -in text.txt -out cbc128encrypted.bin -K 00112233445566778889aabbccddeeff -iv 20304050607082143234324324233333
```

```
ghex cbc128encrypted.bin &
```

```
openssl enc -aes-128-cbc -d -in cbc128encrypted.bin -out cbc128decrypted.txt -K 00112233445566778889aabbccddeeff -iv 20304050607082143234324324233333
```

this one is larger after endryption meaning it has padding

```
openssl enc -aria-128-cfb8 -e -in text.txt -out cfb128encrypted.bin -K 00112233445566778889aabbccddeeff -iv 20304050607082143234324324233333
```

```
ghex cfb128encrypted.bin &
```

```
openssl enc -aria-128-cfb8 -d -in cfb128encrypted.bin -out cfb128decrypted.txt -K 00112233445566778889aabbccddeeff -iv 20304050607082143234324324233333
```

this one is same sized after endryption meaning it do not have padding (stream)

```
openssl enc -aria-128-ofb -e -in text.txt -out ofb128encrypted.bin -K 00112233445566778889aabbccddeeff -iv 20304050607082143234324324233333
```

```
ghex ofb128encrypted.bin &
```

```
openssl enc -aria-128-ofb -d -in ofb128encrypted.bin -out ofb128decrypted.txt -K 00112233445566778889aabbccddeeff -iv 20304050607082143234324324233333
```

this one is same sized after endryption meaning it do not have padding

LAB 3 TASK 5:

create a text file nammed text.txt

```
openssl dgst -sha1 text.txt
```

output: fc2ba7ee7e57ffeec9ab7d24855ff083c708eb74

```
openssl dgst -md5 text.txt
```

output: df7d8c27fad4c98a6678c5719d633bdd

```
openssl dgst -sha256 text.txt
```

output: 923b829a244a667348611ffe93016ddf798224b71a0ad6c650e68f9e10cd1c6e

LAB 3 TASK 6:

create a text file nammed text.txt

```
openssl dgst -sha1 -hmac "this is a key" text.txt
```

output: a20bd55bbc8baf920f0d6ea2191107dd7f49a1b9 openssl dgst -md5 -hmac "this is a key" text.txt

output: 2c0973f8c19b0b7fea982f0dde75bb0f

openssl dgst -sha256 -hmac "this is a key" text.txt

output: 74430d7f825720f412eb3e765cde73d25b14fcd067b05aa4fdaec3419e0e4b93

LAB 3 TASK 7:

create a text file nammed text.txt

openssl dgst -md5 text.txt

output: df7d8c27fad4c98a6678c5719d633bdd

ghex text.txt &

flip a bit

openssl dgst -md5 text.txt

output:b5eb8626d203594db137cdf1c3b37b69

match = 7

update the text file text.txt to the previous main content

openssl dgst -sha256 text.txt

output: 923b829a244a667348611ffe93016ddf798224b71a0ad6c650e68f9e10cd1c6e

ghex text.txt &

flip a bit

openssl dgst -sha256 text.txt

output: 5f4a04044aa5e14da6887551c00326cac4abba24355c076c38fb9f8dd6151e8f

```
match = 3

h1 = "923b829a244a667348611ffe93016ddf798224b71a0ad6c650e68f9e10cd1c6e"

h2 = "5f4a04044aa5e14da6887551c00326cac4abba24355c076c38fb9f8dd6151e8f"

i = 0

cnt = 0

for ch in h1:

    if ch==h2[i]:

        cnt = cnt + 1

    i = i + 1

print(cnt)
```