Task 4

1) Input file: /Files/ciphertext.txt, 4759 bytes

Mode:

ECB:

<u>Command</u>: *openssl enc -aes-128-ecb -in ciphertext.txt -out cipherECB.txt -K 00112233445566778889aabbccddeeff*

<u>Result</u>: Encrypted file size: 4768 bytes. This mode required padding becasue it was not a multiple of 16 bytes block size.

CBC:

<u>Command</u>: *openssl enc -aes-128-cbc -in ciphertext.txt -out cipherCBC.txt -K 00112233445566778889aabbccddeeff -iv 01020304050607080910111213141516*

<u>Result</u>: Encrypted file size: 4768 bytes. This mode requires padding because it was not a multiple of 16 bytes block size.

CFB:

<u>command</u>: *openssl enc -aes-128-cfb -in ciphertext.txt -out cipherCFB.txt -K 00112233445566778889aabbccddeeff -iv 01020304050607080910111213141516*

<u>Result</u>: Encrypted file size: 4759 bytes. This mode does not require padding. As a result there was no padding added to the end file.

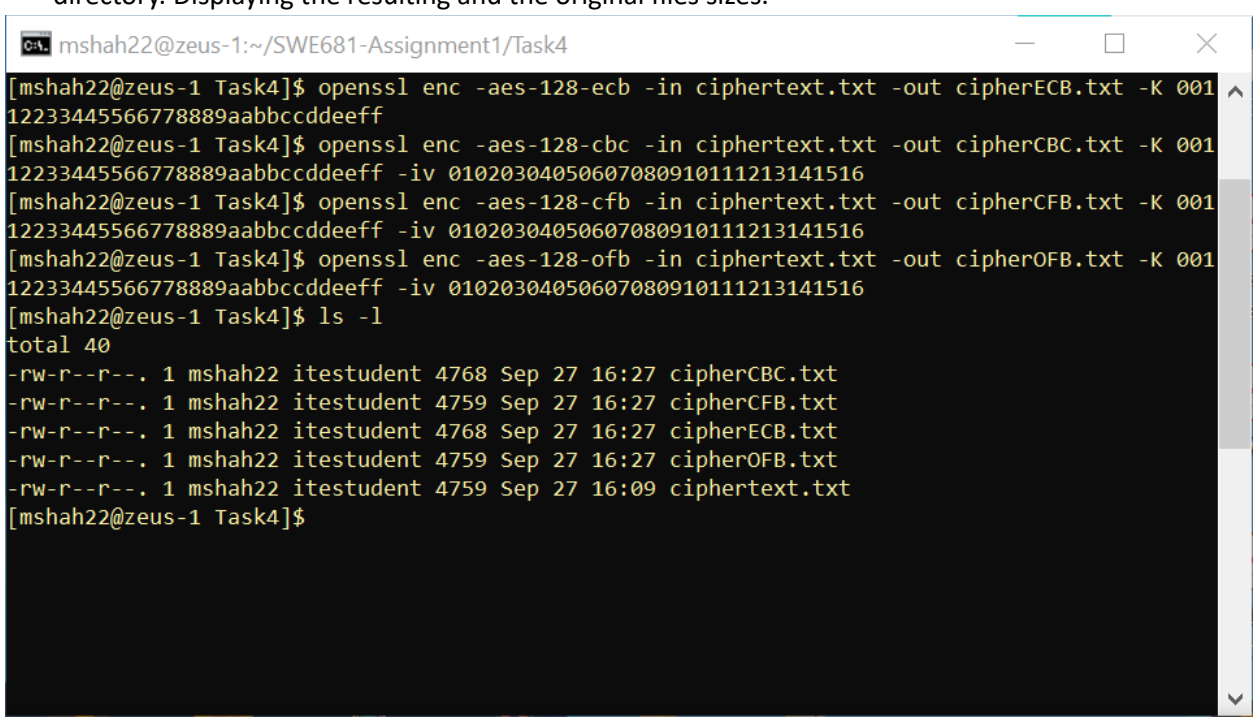
OFB:

<u>command</u>: *openssl enc -aes-128-ofb -in ciphertext.txt -out cipherOFB.txt -K 00112233445566778889aabbccddeeff -iv 01020304050607080910111213141516*

<u>Result</u>: Similar to CFB, there was not padding added to the encrypted file.

<u>Screenshots</u>

- Testing ECB, CBC, CFB, OFB modes using the provided ciphertext.txt file in the /Files/ directory. Displaying the resulting and the original files sizes.



2) Three files created of the following sizes: 5, 10, 16 bytes. We used the CBC mode to encrypt the files and the following were the sizes of the ecncrypted files:

Original size 5 bytes -> 16 bytes
Original size 10 bytes -> 16 bytes
Original size 16 bytes -> 32 bytes

It's interesting to see that even the 16 bytes original file had 16 bytes padded to it to make it 32 bytes.

Screenshots

- Creating three files of 5,10,16 bytes.

```
[mshah22@zeus-1 Task4]$ echo -n "12345" > fivePlain.txt
[mshah22@zeus-1 Task4]$ echo -n "123456789a" > TenPlain.txt
[mshah22@zeus-1 Task4]$ echo -n "123456789abcdefg" > SixteenPlain.txt
[mshah22@zeus-1 Task4]$ ls -l
total 52
-rw-r--r--. 1 mshah22 itestudent 4768 Sep 27 16:27 cipherCBC.txt
-rw-r--r--. 1 mshah22 itestudent 4759 Sep 27 16:27 cipherCFB.txt
-rw-r--r--. 1 mshah22 itestudent 4768 Sep 27 16:27 cipherECB.txt
-rw-r--r--. 1 mshah22 itestudent 4759 Sep 27 16:27 cipherOFB.txt
-rw-r--r--. 1 mshah22 itestudent 4759 Sep 27 16:09 ciphertext.txt
-rw-r--r--. 1 mshah22 itestudent    5 Sep 27 16:35 fivePlain.txt
-rw-r--r--. 1 mshah22 itestudent   16 Sep 27 16:36 SixteenPlain.txt
-rw-r--r--. 1 mshah22 itestudent   10 Sep 27 16:35 TenPlain.txt
[mshah22@zeus-1 Task4]$
```

- Encrypting 5,10,16 bytes files with -aes-128-cbc

```
[mshah22@zeus-1 Task4]$ openssl enc -aes-128-cbc -in fivePlain.txt -out fiveCBC.txt -K 001122
33445566778889aabbccddeeff -iv 0102030405060708091011121314151 6
[mshah22@zeus-1 Task4]$ openssl enc -aes-128-cbc -in TenPlain.txt -out tenCBC.txt -K 00112233
445566778889aabbccddeeff -iv 0102030405060708091011121314151 6
[mshah22@zeus-1 Task4]$ openssl enc -aes-128-cbc -in SixteenPlain.txt -out sixteenCBC.txt -K
00112233445566778889aabbccddeeff -iv 0102030405060708091011121314151 6
```

```
-rw-r--r--. 1 mshah22 itestudent   16 Sep 27 16:37 fiveCBC.txt
-rw-r--r--. 1 mshah22 itestudent    5 Sep 27 16:35 fivePlain.txt
-rw-r--r--. 1 mshah22 itestudent   32 Sep 27 16:38 sixteenCBC.txt
-rw-r--r--. 1 mshah22 itestudent   16 Sep 27 16:36 SixteenPlain.txt
-rw-r--r--. 1 mshah22 itestudent   16 Sep 27 16:38 tenCBC.txt
-rw-r--r--. 1 mshah22 itestudent   10 Sep 27 16:35 TenPlain.txt
[mshah22@zeus-1 Task4]$
```

- Decrypting the three encrypted files with -nopad option.

```
[mshah22@zeus-1 Task4]$ openssl enc -aes-128-cbc -d -nopad -in fiveCBC.txt -out fiveDec.txt -
K 00112233445566778889aabbccddeeff -iv 0102030405060708091011121314151 6
[mshah22@zeus-1 Task4]$ openssl enc -aes-128-cbc -d -nopad -in tenCBC.txt -out tenDec.txt -K
00112233445566778889aabbccddeeff -iv 0102030405060708091011121314151 6
[mshah22@zeus-1 Task4]$ openssl enc -aes-128-cbc -d -nopad -in sixteenCBC.txt -out sixteenDec
.txt -K 00112233445566778889aabbccddeeff -iv 0102030405060708091011121314151 6
[mshah22@zeus-1 Task4]$ ls -l
```

- Hexdump of the three decrypted files as mentioned above.

```
[mshah22@zeus-1 Task4]$ hexdump -C fiveDec.txt
00000000  31 32 33 34 35 0b 0b 0b  0b 0b 0b 0b 0b 0b 0b 0b  |12345...........|
00000010
[mshah22@zeus-1 Task4]$ hexdump -C tenDec.txt
00000000  31 32 33 34 35 36 37 38  39 61 06 06 06 06 06 06  |123456789a......|
00000010
[mshah22@zeus-1 Task4]$ hexdump -C sixteenDec.txt
00000000  31 32 33 34 35 36 37 38  39 61 62 63 64 65 66 67  |123456789abcdefg|
00000010  10 10 10 10 10 10 10 10  10 10 10 10 10 10 10 10  |................|
00000020
[mshah22@zeus-1 Task4]$
```