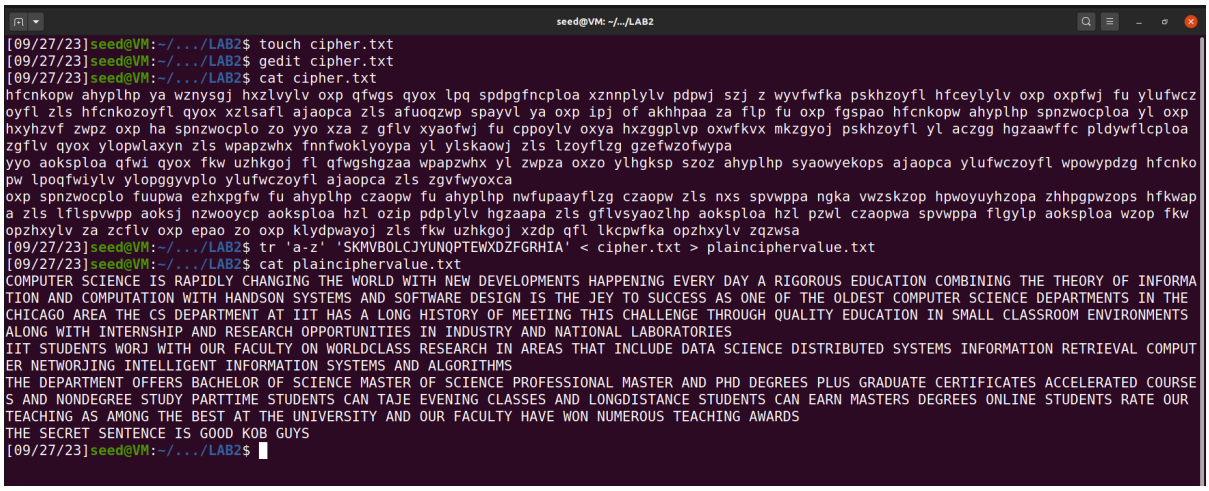
Name : Linson Peter Rodrigues

Lab 7 - Secret-Key Encryption

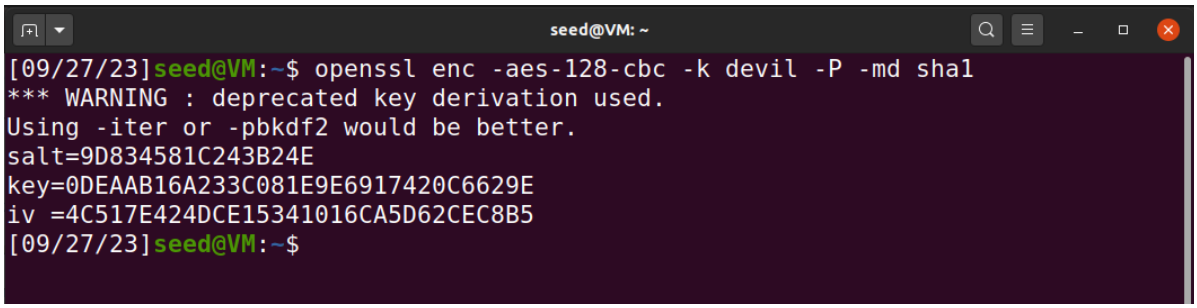
Task 1: Frequency Analysis

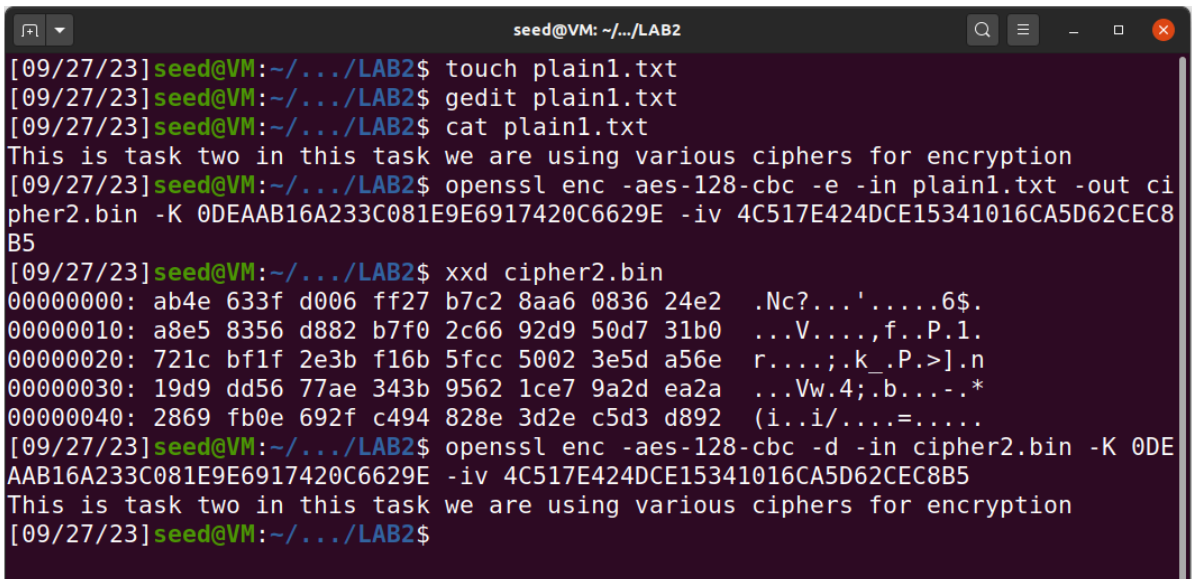


Observation: Used frequency analysis to figure out the encryption key and the following output was displayed.

Task 2: Encryption using Different Ciphers and Modes

1. **-aes-128-cbc**





Observation: Was able to encrypt and decrypt the text using -aes-128-cbc

2. **-aria-128-cbc**

```
[09/27/23]seed@VM:~$ openssl enc -aria-128-cbc -k linson -P -md sha1
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
salt=CA7F1FB9100D4809
key=8AC20F59771F9C515A421B274EBEA1B5
iv =4A249DDA61180D11B711F9597F4770DC
[09/27/23]seed@VM:~$
```

```
[09/27/23]seed@VM:~/.../LAB2$ man openssl
[09/27/23]seed@VM:~/.../LAB2$ openssl enc -aria-128-cbc -e -in plain1.txt -out cipher3.bin
 -K 8AC20F59771F9C515A421B274EBEA1B5 -iv 4A249DDA61180D11B711F9597F4770DC
[09/27/23]seed@VM:~/.../LAB2$ xxd cipher3.bin
00000000: 2296 32bc cfc2 9ef5 a1cb 50db bb55 3e50  ".2.......P..U>P
00000010: b22e 784e 6c60 2efb 0090 c044 d4fc bc16  ..xNl`.....D....
00000020: 36c2 6ca1 9a2a 4e23 2cb3 4ca3 3895 2a32  6.l..*N#,.L.8.*2
00000030: c14e e216 ac59 75e1 338f 5922 f7ed baad  .N...Yu.3.Y"....
00000040: d216 2c87 0af7 454b e080 cca7 adcf a17b  ..,...EK.......{
[09/27/23]seed@VM:~/.../LAB2$ openssl enc -aria-128-cbc -d -in cipher3.bin -K 8AC20F59771F
9C515A421B274EBEA1B5  -iv 4A249DDA61180D11B711F9597F4770DC
This is task two in this task we are using various ciphers for encryption
[09/27/23]seed@VM:~/.../LAB2$
```

Observation: Was able to encrypt and decrypt the text using -aria-128-cbc

3. **-camellia-192-cbc**

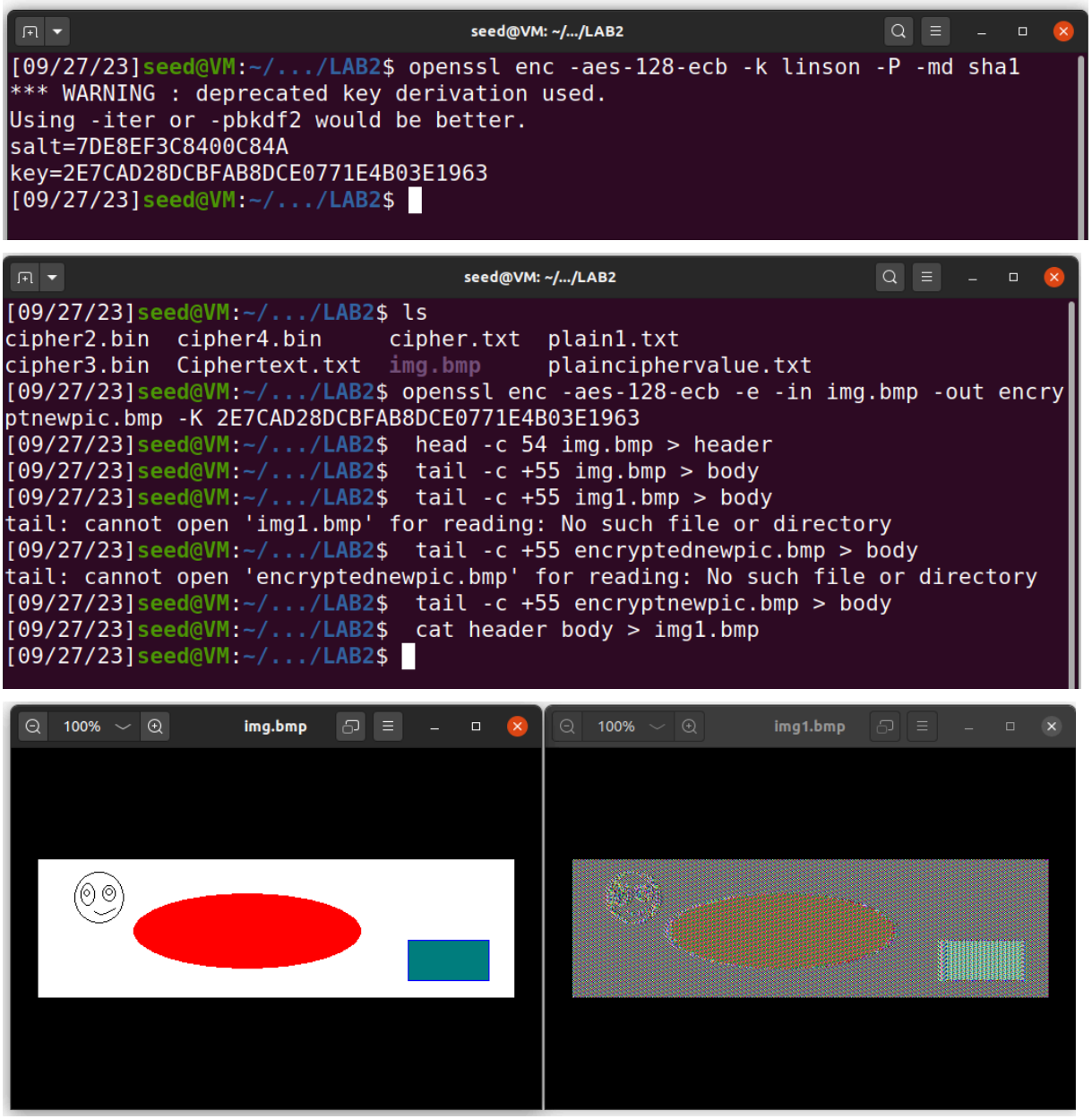
```
[09/27/23]seed@VM:~$ openssl enc -camellia-192-cbc -k linson -P -md sha1
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
salt=F0CF6867162FBB9D
key=C6DB83471E5F4A992CDA3C3FA255779B65FC145C1C5E0EEC
iv =C5C212BE460F35BBF806B02E457A5144
[09/27/23]seed@VM:~$
```

```
[09/27/23]seed@VM:~/.../LAB2$ openssl enc -camellia-192-cbc -e -in plain1.txt -out cipher4
.bin -K C6DB83471E5F4A992CDA3C3FA255779B65FC145C1C5E0EEC -iv C5C212BE460F35BBF806B02E457A5
144
[09/27/23]seed@VM:~/.../LAB2$ xxd cipher4.bin
00000000: 4e51 c250 f83f b1a0 05d7 80ff d534 4016  NQ.P.?.......4@.
00000010: 1703 d575 c45b 9686 7233 1b3d b851 dab8  ...u.[..r3.=.Q..
00000020: 8f79 b00c 0db0 33c6 e2db d563 0213 ab67  .y....3....c...g
00000030: 06e0 6274 7822 7f09 e24d fe06 232a 803a  ..btx"...M..#*.:
00000040: 7b1f 007f fbf6 2fc1 4945 3cd8 18c2 9427  {...../.IE<....'
[09/27/23]seed@VM:~/.../LAB2$ openssl enc -camellia-192-cbc -d -in cipher4.bin -K C6DB8347
1E5F4A992CDA3C3FA255779B65FC145C1C5E0EEC  -iv C5C212BE460F35BBF806B02E457A5144
This is task two in this task we are using various ciphers for encryption
[09/27/23]seed@VM:~/.../LAB2$
```

Observation: Was able to encrypt and decrypt the text using -camellia-192-cbc

Task 3: Encryption Mode – ECB vs. CBC

ECB

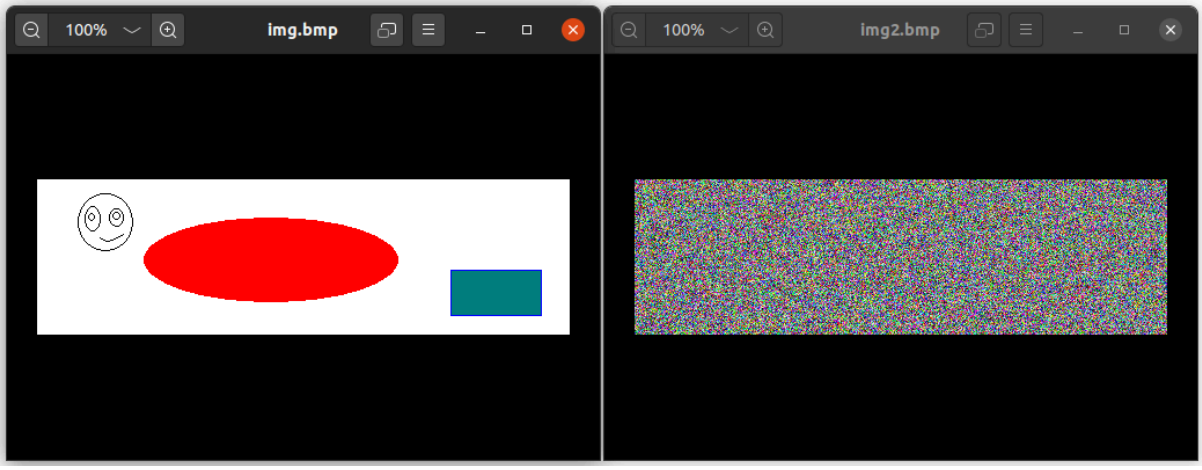


Observation : If the ECB encrypted image is compared to the CBC encrypted image, it can be seen that the ECB encryption kind of exposes the shape and pattern of the original image, which makes it less secure for its users because the adversary may be able to guess what the Plaintext looks like.

CBC

```
[09/28/23]seed@VM:~/.../LAB2$ openssl enc -aes-128-cbc -k linson -P -md sha1
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
salt=6E335A4190598A21
key=19ABB4AEA70E8C2D24DB99340F05BC2F
iv =92F6C4FD69645F052949AFF84478EEE4
[09/28/23]seed@VM:~/.../LAB2$
```

```
[09/28/23]seed@VM:~/.../LAB2$ openssl enc -aes-128-cbc -e -in img.bmp -out
encryptnewpic.bmp -K 19ABB4AEA70E8C2D24DB99340F05BC2F -iv 92F6C4FD69645F052
949AFF84478EEE4
[09/28/23]seed@VM:~/.../LAB2$  head -c 54 img.bmp > header
[09/28/23]seed@VM:~/.../LAB2$  tail -c +55 img.bmp > body
[09/28/23]seed@VM:~/.../LAB2$  tail -c +55 encryptnewpic.bmp > body
[09/28/23]seed@VM:~/.../LAB2$  cat header body > img2.bmp
[09/28/23]seed@VM:~/.../LAB2$
[09/28/23]seed@VM:~/.../LAB2$
[09/28/23]seed@VM:~/.../LAB2$
```



Observation : According to observation, it can be inferred that the encrypted image acquired the original image's size. Additionally, there are no hints or patterns in the ciphertext that would allow an opponent to deduce the true original image.

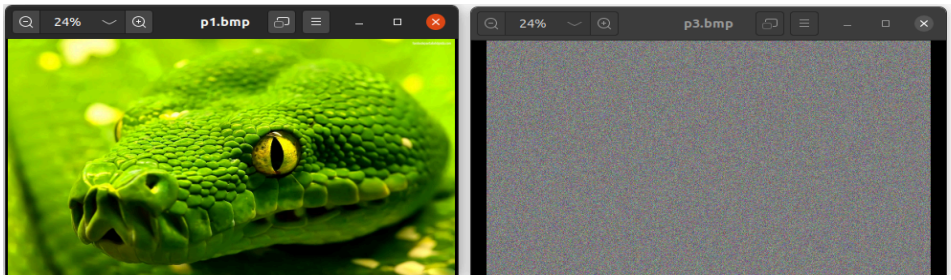
Explanation :
Block Cypher Symmetric Encryption is implemented through the cypher mode known as Cypher Block Chaining (CBC). The current plaintext is encrypted with a different key and each previous ciphertext is appended to it in the CBC cypher mode.
As already known, a block cypher is a kind of symmetric encryption that encrypts plaintext with a fixed block size (64 bits) and generates ciphertext with the same block size (64 bits) as the plaintext. And that explains why the Encrypted image is the exact same size as the Original image.

NEW IMAGE

CBC

```
[09/28/23]seed@VM:~/.../LAB2$ openssl enc -aes-128-cbc -k linson123 -P -md sha1
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
salt=8E8C53DAB29C907A
key=43D44F959F15A389B7B47CA93F0680B8
iv =3FE209A1906ECA94A67D132BC7FF5733
[09/28/23]seed@VM:~/.../LAB2$
```

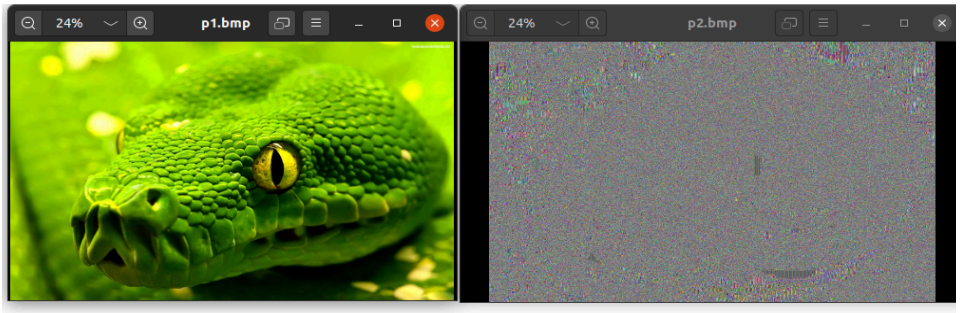
```
[09/28/23]seed@VM:~/.../LAB2$ openssl enc -aes-128-cbc -e -in p1.bmp -out encrypt1.bm
p -K 43D44F959F15A389B7B47CA93F0680B8 -iv 3FE209A1906ECA94A67D132BC7FF5733
[09/28/23]seed@VM:~/.../LAB2$ head -c 54 p1.bmp > header
[09/28/23]seed@VM:~/.../LAB2$ tail -c +55 encrypt1.bmp > body
[09/28/23]seed@VM:~/.../LAB2$ cat header body > p3.bmp
[09/28/23]seed@VM:~/.../LAB2$
```



ECB

```
seed@VM: ~/.../LAB2
[09/28/23]seed@VM:~/.../LAB2$ openssl enc -aes-128-ecb -k linson123 -P -md sha1
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
salt=92600BE166992DD5
key=CCE80A266C5D34B40DA729B50115583C
```

```
seed@VM: ~/.../LAB2
[09/28/23]seed@VM:~/.../LAB2$ openssl enc -aes-128-ecb -e -in p1.bmp -out encrypt.bmp
 -K CCE80A266C5D34B40DA729B50115583C
[09/28/23]seed@VM:~/.../LAB2$ head -c 54 p1.bmp > header
[09/28/23]seed@VM:~/.../LAB2$ tail -c +55 encrypt.bmp > body
[09/28/23]seed@VM:~/.../LAB2$ cat header body > p2.bmp
[09/28/23]seed@VM:~/.../LAB2$
```



Observation : With the new image I chose, I first encrypted the image with the CBC mode and named it p1.bmp and it worked, the ECB mode isn't working for the new image.

Task 4 : Padding

ECB

```
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-ecb -k linson -p -md sha1
Salted__;ff▯salt=3B8DB42E0807661E
key=5BCF867F3C2278F47FCDDA98DB97088C
```

```
[10/03/23]seed@VM:~/.../LAB02$ echo -n "ABCDE" > A5.txt
[10/03/23]seed@VM:~/.../LAB02$ echo -n "ABCDE12345" > A10.txt
[10/03/23]seed@VM:~/.../LAB02$ echo -n "ABCDE12345FGHIJK" > A16.txt
[10/03/23]seed@VM:~/.../LAB02$ ls -l A5.txt A10.txt A16.txt
-rw-rw-r-- 1 seed seed 10 Oct  3 10:31 A10.txt
-rw-rw-r-- 1 seed seed 16 Oct  3 10:31 A16.txt
-rw-rw-r-- 1 seed seed  5 Oct  3 10:31 A5.txt
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A5.txt
00000000  41 42 43 44 45                                    |ABCDE|
00000005
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A10.txt
00000000  41 42 43 44 45 31 32 33  34 35                    |ABCDE12345|
0000000a
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A16.txt
00000000  41 42 43 44 45 31 32 33  34 35 46 47 48 49 4a 4b  |ABCDE12345FGHIJK|
00000010
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-ecb -e -in A5.txt -out A5ecb.txt -K 5BCF867F3C2278F47FCDDA98DB97088C
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-ecb -e -in A10.txt -out A10ecb.txt -K 5BCF867F3C2278F47FCDDA98DB97088C
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-ecb -e -in A16.txt -out A16ecb.txt -K 5BCF867F3C2278F47FCDDA98DB97088C
[10/03/23]seed@VM:~/.../LAB02$ ls -l A5ecb.txt A10ecb.txt A16ecb.txt
-rw-rw-r-- 1 seed seed 16 Oct  3 10:34 A10ecb.txt
-rw-rw-r-- 1 seed seed 32 Oct  3 10:34 A16ecb.txt
-rw-rw-r-- 1 seed seed 16 Oct  3 10:34 A5ecb.txt
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A5ecb.txt
00000000  cf df 4a 84 95 8c 8a 33  5b ea 2e e4 a8 e6 bb 2e  |..J....3[.......|
00000010
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A10ecb.txt
00000000  e8 05 64 53 9c 79 94 cd  b5 5c 65 e9 cc b0 68 8a  |..dS.y...\e...h.|
00000010
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A16ecb.txt
00000000  d6 96 40 1c aa b7 df 64  1c 6c df 15 a3 77 db a8  |..@....d.l...w..|
00000010  fc 01 21 a2 9f ba 5a 7a  f1 84 51 f1 bf a4 c5 2b  |..!...Zz..Q....+|
00000020
```

```
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-ecb -d -nopad -in A5ecb.txt -out A5ecb_d.txt -K 5BCF867F3C2278F47FCDDA98DB97088C
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-ecb -d -nopad -in A10ecb.txt -out A10ecb_d.txt -K 5BCF867F3C2278F47FCDDA98DB97088C
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-ecb -d -nopad -in A16ecb.txt -out A16ecb_d.txt -K 5BCF867F3C2278F47FCDDA98DB97088C
[10/03/23]seed@VM:~/.../LAB02$ ls -l A5ecb_d.txt A10ecb_d.txt A16ecb_d.txt
-rw-rw-r-- 1 seed seed 16 Oct  3 10:39 A10ecb_d.txt
-rw-rw-r-- 1 seed seed 32 Oct  3 10:39 A16ecb_d.txt
-rw-rw-r-- 1 seed seed 16 Oct  3 10:39 A5ecb_d.txt
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A5ecb_d.txt
00000000  41 42 43 44 45 0b 0b 0b  0b 0b 0b 0b 0b 0b 0b 0b  |ABCDE...........|
00000010
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A10ecb_d.txt
00000000  41 42 43 44 45 31 32 33  34 35 06 06 06 06 06 06  |ABCDE12345......|
00000010
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A16ecb_d.txt
00000000  41 42 43 44 45 31 32 33  34 35 46 47 48 49 4a 4b  |ABCDE12345FGHIJK|
00000010  10 10 10 10 10 10 10 10  10 10 10 10 10 10 10 10  |................|
00000020
[10/03/23]seed@VM:~/.../LAB02$
```

```
[10/03/23]seed@VM:~/.../LAB02$ xxd A5ecb.txt
00000000: cfdf 4a84 958c 8a33 5bea 2ee4 a8e6 bb2e  ..J....3[.......
[10/03/23]seed@VM:~/.../LAB02$ xxd A10ecb.txt
00000000: e805 6453 9c79 94cd b55c 65e9 ccb0 688a  ..dS.y...\e...h.
[10/03/23]seed@VM:~/.../LAB02$ xxd A16ecb.txt
00000000: d696 401c aab7 df64 1c6c df15 a377 dba8  ..@....d.l...w..
00000010: fc01 21a2 9fba 5a7a f184 51f1 bfa4 c52b  ..!...Zz..Q....+
[10/03/23]seed@VM:~/.../LAB02$ xxd A16ecb_d.txt
00000000: 4142 4344 4531 3233 3435 4647 4849 4a4b  ABCDE12345FGHIJK
00000010: 1010 1010 1010 1010 1010 1010 1010 1010  ................
[10/03/23]seed@VM:~/.../LAB02$ xxd A10ecb_d.txt
00000000: 4142 4344 4531 3233 3435 0606 0606 0606  ABCDE12345......
[10/03/23]seed@VM:~/.../LAB02$ xxd A5ecb_d.txt
00000000: 4142 4344 450b 0b0b 0b0b 0b0b 0b0b 0b0b  ABCDE...........
[10/03/23]seed@VM:~/.../LAB02$
```

CBC

```
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-cbc -k linson -p -md sha1
Salted__]@4@@N@@salt=5DC234A3F74EF9AE
key=9CC2721A737A770BE4F06E533DAEDD4B
iv =A09715D69620E24D7B1ED46CB279090D
```

```
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-cbc -e -in A5.txt -out A5cbc.txt -K 9CC2721A737A770BE4F06E533DAEDD4B -iv A09715D69620E24D
7B1ED46CB279090D
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-cbc -e -in A10.txt -out A10cbc.txt -K 9CC2721A737A770BE4F06E533DAEDD4B -iv A09715D69620E2
4D7B1ED46CB279090D
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-cbc -e -in A16.txt -out A16cbc.txt -K 9CC2721A737A770BE4F06E533DAEDD4B -iv A09715D69620E2
4D7B1ED46CB279090D
[10/03/23]seed@VM:~/.../LAB02$ ls -l A5cbc.txt A10cbc.txt A16cbc.txt
-rw-rw-r-- 1 seed seed 16 Oct  3 10:51 A10cbc.txt
-rw-rw-r-- 1 seed seed 32 Oct  3 10:51 A16cbc.txt
-rw-rw-r-- 1 seed seed 16 Oct  3 10:51 A5cbc.txt
[10/03/23]seed@VM:~/.../LAB02$ hexdum -C A5cbc.txt
No command 'hexdum' found, did you mean:
 Command 'hexdump' from package 'bsdmainutils' (main)
hexdum: command not found
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A5cbc.txt
00000000  e7 57 46 ef 0c b6 00 b6  50 5a 95 7c 17 ec ac ae  |.WF.....PZ.|....|
00000010
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A10cbc.txt
00000000  6d 55 95 fb a4 00 68 45  8d ce 2e 86 5c dd e7 e3  |mU....hE....\...|
00000010
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A16cbc.txt
00000000  16 3a 7e 4a 6a 23 f1 46  48 29 d8 ff e7 6b a8 b3  |.:~Jj#.FH)...k..|
00000010  8f ab 59 36 84 1b d7 1b  42 90 28 f7 9c 3a 7a bc  |..Y6....B.(..:z.|
00000020
```

```
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-cbc -d -nopad -in A16cbc.txt -out A16cbc_d.txt -K 9CC2721A737A770BE4F06E533DAEDD4B -iv A0
9715D69620E24D7B1ED46CB279090D
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-cbc -d -nopad -in A10cbc.txt -out A10cbc_d.txt -K 9CC2721A737A770BE4F06E533DAEDD4B -iv A0
9715D69620E24D7B1ED46CB279090D
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-cbc -d -nopad -in A5cbc.txt -out A5cbc_d.txt -K 9CC2721A737A770BE4F06E533DAEDD4B -iv A097
15D69620E24D7B1ED46CB279090D
[10/03/23]seed@VM:~/.../LAB02$ ls -l A5cbc_d.txt A10cbc_d.txt A16cbc_d.txt
-rw-rw-r-- 1 seed seed 16 Oct  3 10:55 A10cbc_d.txt
-rw-rw-r-- 1 seed seed 32 Oct  3 10:54 A16cbc_d.txt
-rw-rw-r-- 1 seed seed 16 Oct  3 10:55 A5cbc_d.txt
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A5cbc_d.txt
00000000  41 42 43 44 45 0b 0b 0b  0b 0b 0b 0b 0b 0b 0b 0b  |ABCDE...........|
00000010
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A10cbc_d.txt
00000000  41 42 43 44 45 31 32 33  34 35 06 06 06 06 06 06  |ABCDE12345......|
00000010
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A16cbc_d.txt
00000000  41 42 43 44 45 31 32 33  34 35 46 47 48 49 4a 4b  |ABCDE12345FGHIJK|
00000010  10 10 10 10 10 10 10 10  10 10 10 10 10 10 10 10  |................|
00000020
[10/03/23]seed@VM:~/.../LAB02$
```

```
[10/03/23]seed@VM:~/.../LAB02$ xxd A5cbc.txt
00000000: e757 46ef 0cb6 00b6 505a 957c 17ec acae  .WF.....PZ.|....
[10/03/23]seed@VM:~/.../LAB02$ xxd A10cbc.txt
00000000: 6d55 95fb a400 6845 8dce 2e86 5cdd e7e3  mU....hE....\...
[10/03/23]seed@VM:~/.../LAB02$ xxd A16cbc.txt
00000000: 163a 7e4a 6a23 f146 4829 d8ff e76b a8b3  .:~Jj#.FH)...k..
00000010: 8fab 5936 841b d71b 4290 28f7 9c3a 7abc  ..Y6....B.(..:z.
[10/03/23]seed@VM:~/.../LAB02$ xxd A16cbc_d.txt
00000000: 4142 4344 4531 3233 3435 4647 4849 4a4b  ABCDE12345FGHIJK
00000010: 1010 1010 1010 1010 1010 1010 1010 1010  ................
[10/03/23]seed@VM:~/.../LAB02$ xxd A10cbc_d.txt
00000000: 4142 4344 4531 3233 3435 0606 0606 0606  ABCDE12345......
[10/03/23]seed@VM:~/.../LAB02$ xxd A5cbc_d.txt
00000000: 4142 4344 450b 0b0b 0b0b 0b0b 0b0b 0b0b  ABCDE...........
```

CFB

```
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-cfb -k linson -p -md sha1Salted__,▒]V@et@salt=2C024A56E16574FA
key=473FAB6913A055222A32BB327440DD08
iv =122E2986B32B5EBF22FDC5C1D008D089
```

```
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-cfb -e -in A5.txt -out A5cfb.txt -K 473FAB6913A055222A32BB327440DD08 -iv 122E2986B32B5EBF
22FDC5C1D008D089
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-cfb -e -in A10.txt -out A10cfb.txt -K 473FAB6913A055222A32BB327440DD08 -iv 122E2986B32B5E
BF22FDC5C1D008D089
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-cfb -e -in A16.txt -out A16cfb.txt -K 473FAB6913A055222A32BB327440DD08 -iv 122E2986B32B5E
BF22FDC5C1D008D089
[10/03/23]seed@VM:~/.../LAB02$ ls-l A5cfb.txt A10cfb.txt A16cfb.txt
ls-l: command not found
[10/03/23]seed@VM:~/.../LAB02$ ls -l A5cfb.txt A10cfb.txt A16cfb.txt
-rw-rw-r-- 1 seed seed 10 Oct  3 11:04 A10cfb.txt
-rw-rw-r-- 1 seed seed 16 Oct  3 11:04 A16cfb.txt
-rw-rw-r-- 1 seed seed  5 Oct  3 11:04 A5cfb.txt
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A5cfb.txt
00000000  b4 e1 e5 59 a1                                    |...Y.|
00000005
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A10cfb.txt
00000000  b4 e1 e5 59 a1 12 02 19  ef af                    |...Y......|
0000000a
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A16cfb.txt
00000000  b4 e1 e5 59 a1 12 02 19  ef af 19 95 5b 98 68 05  |...Y........[.h.|
00000010
```

```
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-cfb -d -nopad -in A16cfb.txt -out A16cfb_d.txt -K 473FAB6913A055222A32BB327440DD08 -iv 12
2E2986B32B5EBF22FDC5C1D008D089
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-cfb -d -nopad -in A10cfb.txt -out A10cfb_d.txt -K 473FAB6913A055222A32BB327440DD08 -iv 12
2E2986B32B5EBF22FDC5C1D008D089
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -aes-128-cfb -d -nopad -in A5cfb.txt -out A5cfb_d.txt -K 473FAB6913A055222A32BB327440DD08 -iv 122E
2986B32B5EBF22FDC5C1D008D089
[10/03/23]seed@VM:~/.../LAB02$ ls -l A5cfb_d.txt A10cfb_d.txt A16cfb_d.txt
-rw-rw-r-- 1 seed seed 10 Oct  3 11:08 A10cfb_d.txt
-rw-rw-r-- 1 seed seed 16 Oct  3 11:08 A16cfb_d.txt
-rw-rw-r-- 1 seed seed  5 Oct  3 11:09 A5cfb_d.txt
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A5cfb_d.txt
00000000  41 42 43 44 45                                    |ABCDE|
00000005
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A10cfb_d.txt
00000000  41 42 43 44 45 31 32 33  34 35                    |ABCDE12345|
0000000a
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A16cfb_d.txt
00000000  41 42 43 44 45 31 32 33  34 35 46 47 48 49 4a 4b  |ABCDE12345FGHIJK|
00000010
```

```
[10/03/23]seed@VM:~/.../LAB02$ xxd A5cfb.txt
00000000: b4e1 e559 a1                                    ...Y.
[10/03/23]seed@VM:~/.../LAB02$ xxd A10cfb.txt
00000000: b4e1 e559 a112 0219 efaf                        ...Y......
[10/03/23]seed@VM:~/.../LAB02$ xxd A16cfb.txt
00000000: b4e1 e559 a112 0219 efaf 1995 5b98 6805  ...Y........[.h.
[10/03/23]seed@VM:~/.../LAB02$ xxd A16cfb_d.txt
00000000: 4142 4344 4531 3233 3435 4647 4849 4a4b  ABCDE12345FGHIJK
[10/03/23]seed@VM:~/.../LAB02$ xxd A10cfb_d.txt
00000000: 4142 4344 4531 3233 3435                        ABCDE12345
[10/03/23]seed@VM:~/.../LAB02$ xxd A5cfb_d.txt
00000000: 4142 4344 45                                    ABCDE
```

OFB

```
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -rc2-ofb -k linson -p -md sha1
Salted__▒▒▒▒X.h▒▒salt=1C0658CC9C2E6818
key=7F885597597FF7C66EABC4F36D39F02E
iv =AFE875B409DBF427
```

```
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -rc2-ofb -e -in A5.txt -out A5ofb.txt -K 7F885597597FF7C66EABC4F36D39F02E -iv AFE875B409DBF427
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -rc2-ofb -e -in A10.txt -out A10ofb.txt -K 7F885597597FF7C66EABC4F36D39F02E -iv AFE875B409DBF427
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -rc2-ofb -e -in A16.txt -out A16ofb.txt -K 7F885597597FF7C66EABC4F36D39F02E -iv AFE875B409DBF427
[10/03/23]seed@VM:~/.../LAB02$ ls -l A5ofb.txt
-rw-rw-r-- 1 seed seed 5 Oct  3 12:17 A5ofb.txt
[10/03/23]seed@VM:~/.../LAB02$ ls -l A5ofb.txt A10ofb.txt A16ofb.txt
-rw-rw-r-- 1 seed seed 10 Oct  3 12:18 A10ofb.txt
-rw-rw-r-- 1 seed seed 16 Oct  3 12:19 A16ofb.txt
-rw-rw-r-- 1 seed seed  5 Oct  3 12:17 A5ofb.txt
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A5ofb.txt
00000000  7a cf c8 9f 18                                    |z....|
00000005
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A10ofb.txt
00000000  7a cf c8 9f 18 9e a6 4d  49 de                    |z......MI.|
0000000a
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A20ofb.txt
hexdump: A20ofb.txt: No such file or directory
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A16ofb.txt
00000000  7a cf c8 9f 18 9e a6 4d  49 de 45 36 92 87 a6 01  |z......MI.E6....|
00000010
```

```
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -rc2-ofb -d -nopad -in A5ofb.txt -out A5ofb_d.txt -K 7F885597597FF7C66EABC4F36D39F02E -iv AFE875B4
09DBF427
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -rc2-ofb -d -nopad -in A10ofb.txt -out A10ofb_d.txt -K 7F885597597FF7C66EABC4F36D39F02E -iv AFE875
B409DBF427
[10/03/23]seed@VM:~/.../LAB02$ openssl enc -rc2-ofb -d -nopad -in A16ofb.txt -out A16ofb_d.txt -K 7F885597597FF7C66EABC4F36D39F02E -iv AFE875
B409DBF427
[10/03/23]seed@VM:~/.../LAB02$ ls -l A5ofb_d.txt
-rw-rw-r-- 1 seed seed 5 Oct  3 12:26 A5ofb_d.txt
[10/03/23]seed@VM:~/.../LAB02$ ls -l A5ofb_d.txt A10ofb_d.txt A16ofb_d.txt
-rw-rw-r-- 1 seed seed 10 Oct  3 12:27 A10ofb_d.txt
-rw-rw-r-- 1 seed seed 16 Oct  3 12:27 A16ofb_d.txt
-rw-rw-r-- 1 seed seed  5 Oct  3 12:26 A5ofb_d.txt
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A5ofb_d.txt
00000000  41 42 43 44 45                                    |ABCDE|
00000005
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A10ofb_d.txt
00000000  41 42 43 44 45 31 32 33  34 35                    |ABCDE12345|
0000000a
[10/03/23]seed@VM:~/.../LAB02$ hexdump -C A16ofb_d.txt
00000000  41 42 43 44 45 31 32 33  34 35 46 47 48 49 4a 4b  |ABCDE12345FGHIJK|
00000010
[10/03/23]seed@VM:~/.../LAB02$
```

```
[10/03/23]seed@VM:~/.../LAB02$ xxd A5ofb.txt
00000000: 7acf c89f 18                                    z....
[10/03/23]seed@VM:~/.../LAB02$ xxd A10ofb.txt
00000000: 7acf c89f 189e a64d 49de                        z......MI.
[10/03/23]seed@VM:~/.../LAB02$ xxd A16ofb.txt
00000000: 7acf c89f 189e a64d 49de 4536 9287 a601         z......MI.E6....
[10/03/23]seed@VM:~/.../LAB02$ xxd A16ofb_d.txt
00000000: 4142 4344 4531 3233 3435 4647 4849 4a4b         ABCDE12345FGHIJK
[10/03/23]seed@VM:~/.../LAB02$ xxd A10ofb_d.txt
00000000: 4142 4344 4531 3233 3435                        ABCDE12345
[10/03/23]seed@VM:~/.../LAB02$ xxd A5ofb_d.txt
00000000: 4142 4344 45                                    ABCDE
```

Observation :
Modes **ECB** and **CBC** added padding to the size of all three encrypted files.
Modes **OFB** and **CFB** did not add any padding to the size of the files.

Explanation :
The input (plaintext) for ECB and CBC modes must be an exact multiple of their block size; as a result, when the plaintext is not an exact multiple of the block size, it must be padded before encryption.
However, because OFB and CFB modes are Stream cyphers and the ciphertext and plaintext are identical, there is no requirement for padding when encrypting plaintexts using these cypher modes.

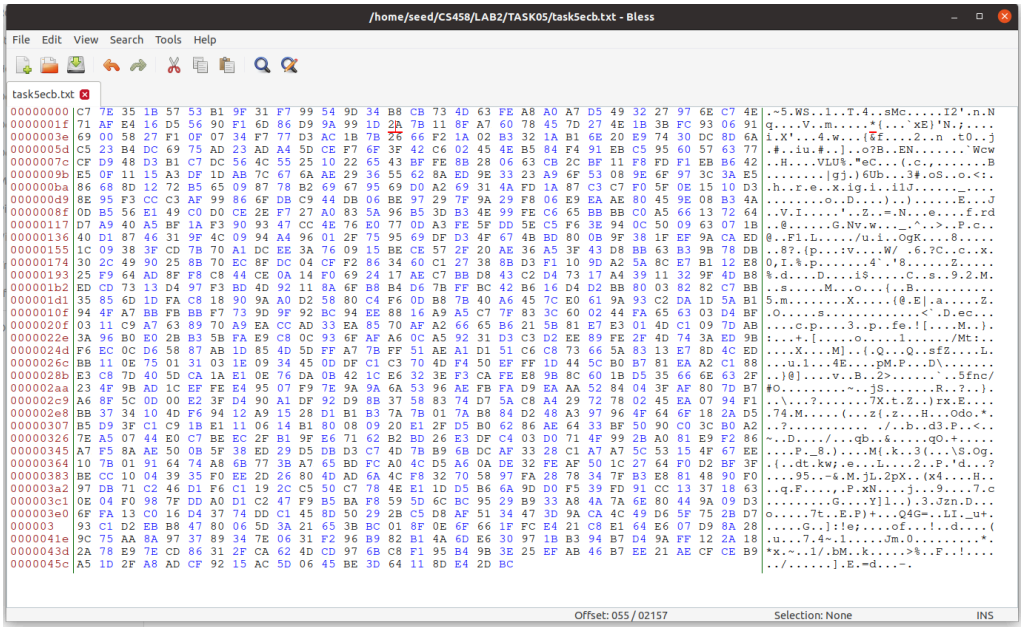
Task 5: Error Propagation – Corrupted Cipher Text

ECB

If the ciphertext is encrypted in ECB mode, all the plaintext will be retrieved after decryption ,except only the corrupted block.

```
[10/05/23]seed@VM:~/.../TASK05$ ls -l task5.txt
-rw-rw-r-- 1 seed seed 1128 Oct  5 15:07 task5.txt
[10/05/23]seed@VM:~/.../TASK05$ openssl enc -aes-128-ecb -k linson -p -md sha1
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
Salted__ÐÐ1ÐÐ4Ðsalt=1AA23180B234E50E
key=CCBD744DCB39D874E4398BD1ACC98416
```

```
[10/05/23]seed@VM:~/.../TASK05$ ls -l task5.txt
-rw-rw-r-- 1 seed seed 1128 Oct  5 15:07 task5.txt
[10/05/23]seed@VM:~/.../TASK05$ openssl enc -aes-128-ecb -e -in task5.txt -out task5ecb.txt -K CCBD744DCB39D874E4398BD1ACC98416
[10/05/23]seed@VM:~/.../TASK05$ bless task5ecb.txt
Gtk-Message: 16:20:57.433: Failed to load module "canberra-gtk-module"
Could not find a part of the path '/home/seed/.config/bless/plugins'.
Could not find a part of the path '/home/seed/.config/bless/plugins'.
Could not find a part of the path '/home/seed/.config/bless/plugins'.
Could not find file "/home/seed/.config/bless/export_patterns"
[10/05/23]seed@VM:~/.../TASK05$ openssl enc -aes-128-ecb -d -in task5ecb.txt -out task5ecb_d.txt -K CCBD744DCB39D874E4398BD1ACC98416
[10/05/23]seed@VM:~/.../TASK05$ cat task5ecb_d.txt
hfcnkopw ahyplhp ya wznysgj hxzl@?rA@@k>>s~yox lpq spdpgfncploa xznnplylv pdpwj szj z wyvfwfka pskhzoyfl hfceylylv oxp oxpfwj fu ylufwczoyfl
zls hfcnkozoyfl qyox xzlsafl ajaopca zls afuoqzwp spayvl ya oxp ipj of akhhpaa za flp fu oxp fgspao hfcnkopw ahyplhp spnzwocploa yl oxp hxyhz
vf zwpz oxp ha spnzwocplo zo yyo xza z gflv xyaofwj fu cppoylv oxya hxzggplvp oxwfkvx mkzgyoj pskhzoyfl yl aczgg hgzaawffc pldywflcploa zgflv
 qyox ylopwlaxyn zls wpapzwhx fnnfwoklyoypa yl ylskaowj zls lzoyflzg gzefwzofwypa
yyo aoksploa qfwi qyox fkw uzhkgoj fl qfwgshgzaa wpapzwhx yl zwpza oxzo ylhgksp szoz ahyplhp syaowyekops ajaopca ylufwczoyfl wpowypdzg hfcnko
pw lpoqfwiylv ylopggyvplo ylufwczoyfl ajaopca zls zgvfwyoxca
oxp spnzwocplo fuupwa ezhxpgfw fu ahyplhp czaopw fu ahyplhp nwfupaayflzg czaopw zls nxs spvwppa ngka vwzskzop hpwoyuyhzopa zhhpgpwzops hfkwap
a zls lflspvwpp aoksj nzwooycp aoksploa hzl ozip pdplylv hgzaapa zls gflvsyaozlhp aoksploa hzl pzwl czaopwa spvwppa flgylp aoksploa wzop fkw
opzhxylv za zcflv oxp epao zo oxp klydpwayoj zls fkw uzhkgoj xzdp qfl lkcpwfka opzhxylv zqzwsa
oxp aphwpo aplоplhp ya vffs bfe vkja
[10/05/23]seed@VM:~/.../TASK05$ cat task5.txt
hfcnkopw ahyplhp ya wznysgj hxzlvylv oxp qfwgs qyox lpq spdpgfncploa xznnplylv pdpwj szj z wyvfwfka pskhzoyfl hfceylylv oxp oxpfwj fu ylufwcz
oyfl zls hfcnkozoyfl qyox xzlsafl ajaopca zls afuoqzwp spayvl ya oxp ipj of akhhpaa za flp fu oxp fgspao hfcnkopw ahyplhp spnzwocploa yl oxp
hxyhzvf zwpz oxp ha spnzwocplo zo yyo xza z gflv xyaofwj fu cppoylv oxya hxzggplvp oxwfkvx mkzgyoj pskhzoyfl yl aczgg hgzaawffc pldywflcploa
zgflv qyox ylopwlaxyn zls wpapzwhx fnnfwoklyoypa yl ylskaowj zls lzoyflzg gzefwzofwypa
yyo aoksploa qfwi qyox fkw uzhkgoj fl qfwgshgzaa wpapzwhx yl zwpza oxzo ylhgksp szoz ahyplhp syaowyekops ajaopca ylufwczoyfl wpowypdzg hfcnko
pw lpoqfwiylv ylopggyvplo ylufwczoyfl ajaopca zls zgvfwyoxca
oxp spnzwocplo fuupwa ezhxpgfw fu ahyplhp czaopw fu ahyplhp nwfupaayflzg czaopw zls nxs spvwppa ngka vwzskzop hpwoyuyhzopa zhhpgpwzops hfkwap
a zls lflspvwpp aoksj nzwooycp aoksploa hzl ozip pdplylv hgzaapa zls gflvsyaozlhp aoksploa hzl pzwl czaopwa spvwppa flgylp aoksploa wzop fkw
opzhxylv za zcflv oxp epao zo oxp klydpwayoj zls fkw uzhkgoj xzdp qfl lkcpwfka opzhxylv zqzwsa
oxp aphwpo aplоplhp ya vffs bfe vkja
[10/05/23]seed@VM:~/.../TASK05$
```



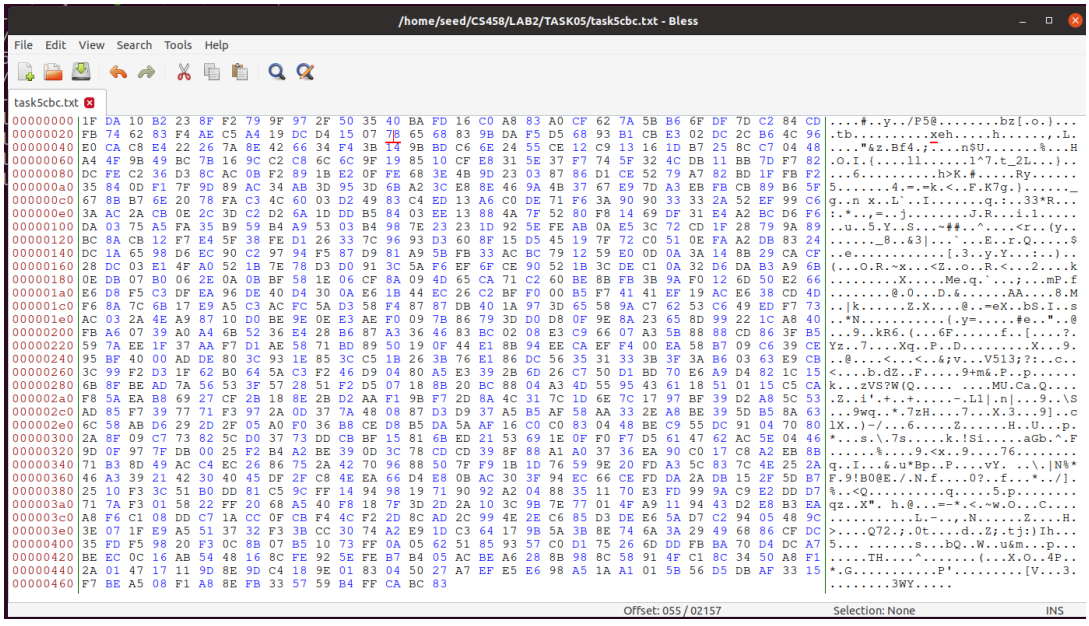
Observation : The corrupted bit from the 55th byte of the ciphertext block spread to all n bits in plaintext when operating in ECB mode.

CBC

Because encryption and decryption in CBC mode are chained, the corrupted text will have an impact on some message blocks.

```
[10/05/23]seed@VM:~/.../TASK05$ openssl enc -aes-128-cbc -k linson123 -p -md sha1
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
Salted__ÐY]!ÐÐ.salt=A6595D21BAC62E03
key=39DF8F823C3FF7321053EA72432EA144
iv =1652A292980266C1C3968D98F181E7B4
```

```
[10/05/23]seed@VM:~/.../TASK05$ ls -l task5.txt
-rw-rw-r-- 1 seed seed 1128 Oct  5 15:07 task5.txt
[10/05/23]seed@VM:~/.../TASK05$ openssl enc -aes-128-cbc -e -in task5.txt -out task5cbc.txt -K 39DF8F823C3FF7321053EA72432EA144 -iv 1652A2929
80266C1C3968D98F181E7B4
[10/05/23]seed@VM:~/.../TASK05$ bless task5cbc.txt
Gtk-Message: 16:37:05.374: Failed to load module "canberra-gtk-module"
Could not find a part of the path '/home/seed/.config/bless/plugins'.
Could not find a part of the path '/home/seed/.config/bless/plugins'.
Could not find a part of the path '/home/seed/.config/bless/plugins'.
Could not find file "/home/seed/.config/bless/export_patterns"
[10/05/23]seed@VM:~/.../TASK05$ openssl enc -aes-128-cbc -d -in task5cbc.txt -out task5cbc_d.txt -K 39DF8F823C3FF7321053EA72432EA144 -iv 1652
A292980266C1C3968D98F181E7B4
[10/05/23]seed@VM:~/.../TASK05$ cat task5cbc_d.txt
hfcnkopw ahyplhp ya wznysgj hxzlS@@fJ@@/~@@)@NOwyox lpq spdpghncploa xznnplylv pdpwj szj z wyvfwfka pskhzoyfl hfceylylv oxp oxpfwj fu ylufwcz
oyfl zls hfcnkozoyfl qyox xzlsafl ajaopca zls afuoqzwp spayvl ya oxp ipj of akhhpaa za flp fu oxp fgspao hfcnkopw ahyplhp spnzwocploa yl oxp
hxyhzvf zwpz oxp ha spnzwocplo zo yyo xza z gflv xyaofwj fu cppoylv oxya hxzggplvp oxwfkvx mkzgyoj pskhzoyfl yl aczgg hgzaawffc pldywflcploa
zgflv qyox ylopwlaxyn zls wpapzwhx fnnfwoklyoypa yl ylskaowj zls lzoyflzg gzefwzofwypa
yyo aoksploa qfwi qyox fkw uzhkgoj fl qfwgshgzaa wpapzwhx yl zwpza oxzo ylhgksp szoz ahyplhp syaowyekops ajaopca ylufwczoyfl wpowypdzg hfcnko
pw lpoqfwiylv ylopggyvplo ylufwczoyfl ajaopca zls zgvfwyoxca
oxp spnzwocplo fuupwa ezhxpgfw fu ahyplhp czaopw fu ahyplhp nwfupaayflzg czaopw zls nxs spvwppa ngka vwzskzop hpwoyuyhzopa zhhpgpwzops hfkwap
a zls lflspvwpp aoksj nzwooycp aoksploa hzl ozip pdplylv hgzaapa zls gflvsyaozlhp aoksploa hzl pzwl czaopwa spvwppa flgylp aoksploa wzop fkw
opzhxylv za zcflv oxp epao zo oxp klydpwayoj zls fkw uzhkgoj xzdp qfl lkcpwfka opzhxylv zqzwsa
oxp aphwpo aploplhp ya vffs bfe vkja
[10/05/23]seed@VM:~/.../TASK05$ cat task5.txt
hfcnkopw ahyplhp ya wznysgj hxzlvylv oxp qfwgs qyox lpq spdpgfncploa xznnplylv pdpwj szj z wyvfwfka pskhzoyfl hfceylylv oxp oxpfwj fu ylufwcz
oyfl zls hfcnkozoyfl qyox xzlsafl ajaopca zls afuoqzwp spayvl ya oxp ipj of akhhpaa za flp fu oxp fgspao hfcnkopw ahyplhp spnzwocploa yl oxp
hxyhzvf zwpz oxp ha spnzwocplo zo yyo xza z gflv xyaofwj fu cppoylv oxya hxzggplvp oxwfkvx mkzgyoj pskhzoyfl yl aczgg hgzaawffc pldywflcploa
zgflv qyox ylopwlaxyn zls wpapzwhx fnnfwoklyoypa yl ylskaowj zls lzoyflzg gzefwzofwypa
yyo aoksploa qfwi qyox fkw uzhkgoj fl qfwgshgzaa wpapzwhx yl zwpza oxzo ylhgksp szoz ahyplhp syaowyekops ajaopca ylufwczoyfl wpowypdzg hfcnko
pw lpoqfwiylv ylopggyvplo ylufwczoyfl ajaopca zls zgvfwyoxca
oxp spnzwocplo fuupwa ezhxpgfw fu ahyplhp czaopw fu ahyplhp nwfupaayflzg czaopw zls nxs spvwppa ngka vwzskzop hpwoyuyhzopa zhhpgpwzops hfkwap
a zls lflspvwpp aoksj nzwooycp aoksploa hzl ozip pdplylv hgzaapa zls gflvsyaozlhp aoksploa hzl pzwl czaopwa spvwppa flgylp aoksploa wzop fkw
opzhxylv za zcflv oxp epao zo oxp klydpwayoj zls fkw uzhkgoj xzdp qfl lkcpwfka opzhxylv zqzwsa
oxp aphwpo aploplhp ya vffs bfe vkja
[10/05/23]seed@VM:~/.../TASK05$
```



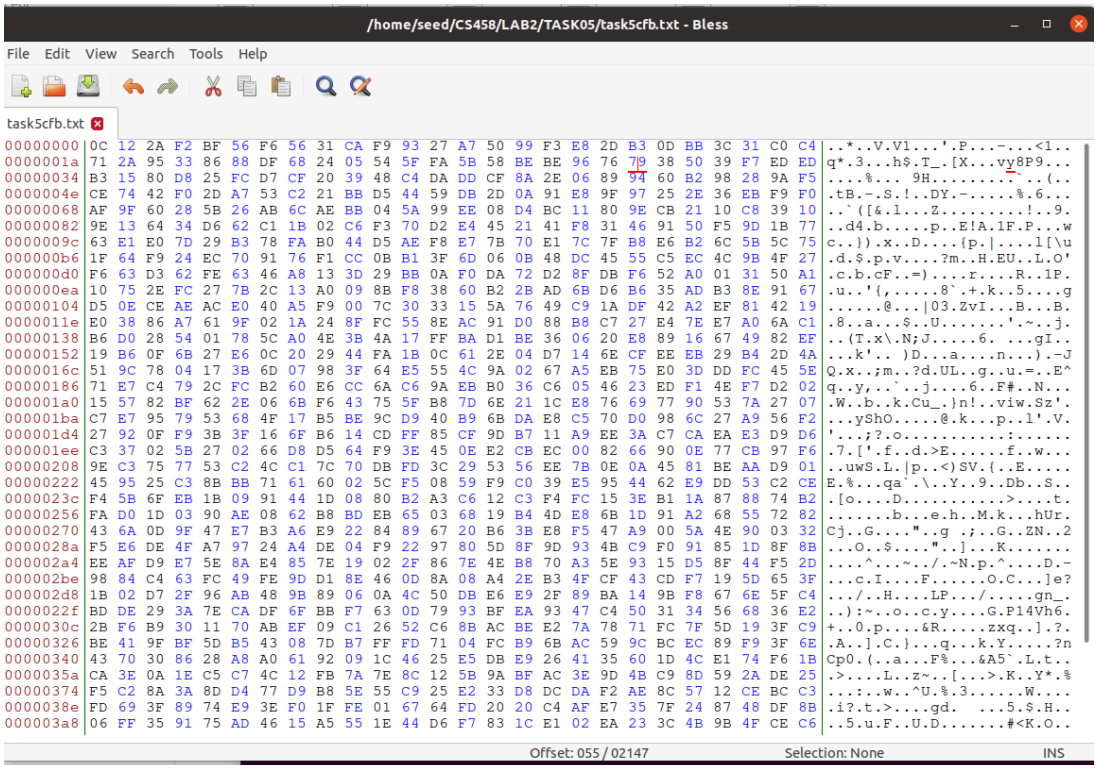
Observation : Two blocks were corrupted by the incorrect encryption in CBC mode.

CFB

```
[10/05/23]seed@VM:~/.../TASK05$ openssl enc -aes-128-cfb -k linson123 -p -md sha1
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
Salted__,`t??salt=2C1B576074B412AD
key=6DC969F1451BBE3D2C2CC8EE7731BDE7
iv =D4267AB71AE58BCAB26CF89C12BE9BBC
```

```
[10/05/23]seed@VM:~/.../TASK05$ openssl enc -aes-128-cfb -e -in task5.txt -out task5cfb.txt -K 6DC969F1451BBE3D2C2CC8EE7731BDE7 -iv D4267AB71
AE58BCAB26CF89C12BE9BBC
[10/05/23]seed@VM:~/.../TASK05$ bless task5cfb.txt
Gtk-Message: 16:46:58.050: Failed to load module "canberra-gtk-module"
Could not find a part of the path '/home/seed/.config/bless/plugins'.
Could not find a part of the path '/home/seed/.config/bless/plugins'.
Could not find a part of the path '/home/seed/.config/bless/plugins'.
Could not find file "/home/seed/.config/bless/export_patterns"

(bless:4197): GLib-CRITICAL **: 16:48:11.334: Source ID 1481 was not found when attempting to remove it
[10/05/23]seed@VM:~/.../TASK05$ openssl enc -aes-128-cfb -d -in task5cfb.txt -out task5cfb_d.txt -K 6DC969F1451BBE3D2C2CC8EE7731BDE7 -iv D426
7AB71AE58BCAB26CF89C12BE9BBC
[10/05/23]seed@VM:~/.../TASK05$ cat task5cfb_d.txt
hfcnkopw ahyplhp ya wznysgj hxzlvylv oxp qfwgr q-kD@r@@@@b@I@@@@ploa xznnplylv pdpwj szj z wyvfwfka pskhzoyfl hfceylylv oxp oxpfwj fu ylufwcz
oyfl zls hfcnkozoyfl qyox xzlsafl ajaopca zls afuoqzwp spayvl ya oxp ipj of akhhpaa za flp fu oxp fgspao hfcnkopw ahyplhp spnzwocploa yl oxp
hxyhzvf zwpz oxp ha spnzwocplo zo yyo xza z gflv xyaofwj fu cppoylv oxya hxzggplvp oxwfkvx mkzgyoj pskhzoyfl yl aczgg hgzaawffc pldywflcploa
zgflv qyox ylopwlaxyn zls wpapzwhx fnnfwoklyoypa yl ylskaowj zls lzoyflzg gzefwzofwypa
yyo aoksploa qfwi qyox fkw uzhkgoj fl qfwgshgzaa wpapzwhx yl zwpza oxzo ylhgksp szoz ahyplhp syaowyekops ajaopca ylufwczoyfl wpowypdzg hfcnko
pw lpoqfwiylv ylopggyvplo ylufwczoyfl ajaopca zls zgvfwyoxca
oxp spnzwocplo fuupwa ezhxpgfw fu ahyplhp czaopw fu ahyplhp nwfupaayflzg czaopw zls nxs spvwppa ngka vwzskzop hpwoyuyhzopa zhhpgpwzops hfkwap
a zls lflspvwpp aoksj nzwooycp aoksploa hzl ozip pdplylv hgzaapa zls gflvsyaozlhp aoksploa hzl pzwl czaopwa spvwppa flgylp aoksploa wzop fkw
opzhxylv za zcflv oxp epao zo oxp klydpwayoj zls fkw uzhkgoj xzdp qfl lkcpwfka opzhxylv zqzwsa
oxp aphwpo aploplhp ya vffs bfe vkja
[10/05/23]seed@VM:~/.../TASK05$ cat task5.txt
hfcnkopw ahyplhp ya wznysgj hxzlvylv oxp qfwgs qyox lpq spdpgfncploa xznnplylv pdpwj szj z wyvfwfka pskhzoyfl hfceylylv oxp oxpfwj fu ylufwcz
oyfl zls hfcnkozoyfl qyox xzlsafl ajaopca zls afuoqzwp spayvl ya oxp ipj of akhhpaa za flp fu oxp fgspao hfcnkopw ahyplhp spnzwocploa yl oxp
hxyhzvf zwpz oxp ha spnzwocplo zo yyo xza z gflv xyaofwj fu cppoylv oxya hxzggplvp oxwfkvx mkzgyoj pskhzoyfl yl aczgg hgzaawffc pldywflcploa
zgflv qyox ylopwlaxyn zls wpapzwhx fnnfwoklyoypa yl ylskaowj zls lzoyflzg gzefwzofwypa
yyo aoksploa qfwi qyox fkw uzhkgoj fl qfwgshgzaa wpapzwhx yl zwpza oxzo ylhgksp szoz ahyplhp syaowyekops ajaopca ylufwczoyfl wpowypdzg hfcnko
pw lpoqfwiylv ylopggyvplo ylufwczoyfl ajaopca zls zgvfwyoxca
oxp spnzwocplo fuupwa ezhxpgfw fu ahyplhp czaopw fu ahyplhp nwfupaayflzg czaopw zls nxs spvwppa ngka vwzskzop hpwoyuyhzopa zhhpgpwzops hfkwap
a zls lflspvwpp aoksj nzwooycp aoksploa hzl ozip pdplylv hgzaapa zls gflvsyaozlhp aoksploa hzl pzwl czaopwa spvwppa flgylp aoksploa wzop fkw
opzhxylv za zcflv oxp epao zo oxp klydpwayoj zls fkw uzhkgoj xzdp qfl lkcpwfka opzhxylv zqzwsa
oxp aphwpo aploplhp ya vffs bfe vkja
```

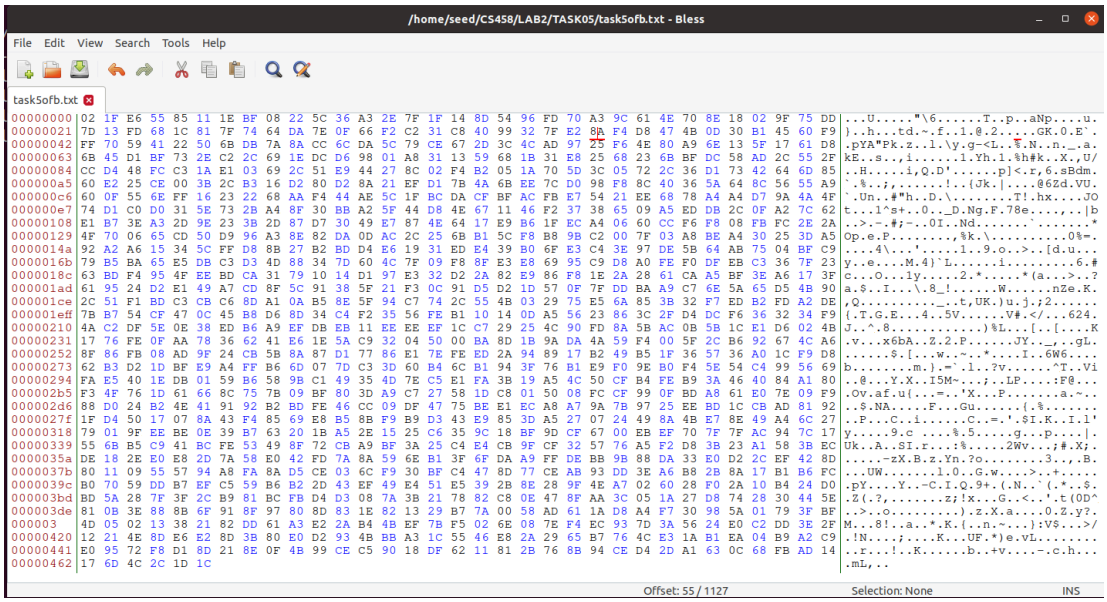


Observation : The error propagation is poor is here .

OFB

```
[10/05/23]seed@VM:~/.../TASK05$ openssl enc -rc2-ofb -k linson123 -p -md sha1
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
Salted__(???w   ?salt=2819DAE7F07709BC
key=3770F222205A9234FE6E9FC31872035F
iv =D05F368B94D2E595
```

```
[10/05/23]seed@VM:~/.../TASK05$ openssl enc -rc2-ofb -e -in task5.txt -out task5ofb.txt -K 3770F222205A9234FE6E9FC31872035F -iv D05F368B94D2E
595
[10/05/23]seed@VM:~/.../TASK05$ bless task5ofb.txt
Gtk-Message: 17:02:33.563: Failed to load module "canberra-gtk-module"
Could not find a part of the path '/home/seed/.config/bless/plugins'.
Could not find a part of the path '/home/seed/.config/bless/plugins'.
Could not find a part of the path '/home/seed/.config/bless/plugins'.
Could not find file "/home/seed/.config/bless/export_patterns"
[10/05/23]seed@VM:~/.../TASK05$ openssl enc -rc2-ofb -d -in task5ofb.txt -out task5ofb_d.txt -K 3770F222205A9234FE6E9FC31872035F -iv D05F368B
94D2E595
[10/05/23]seed@VM:~/.../TASK05$ cat task5ofb_d.txt
hfcnkopw ahyplhp ya wznysgj hxzlvylv oxp qfwgs qyox lpq&spdpgfncploa xznnplylv pdpwj szj z wyvfwfka pskhzoyfl hfceylylv oxp oxpfwj fu ylufwcz
oyfl zls hfcnkozoyfl qyox xzlsafl ajaopca zls afuoqzwp spayvl ya oxp ipj of akhhpaa za flp fu oxp fgspao hfcnkopw ahyplhp spnzwocploa yl oxp
hxyhzvf zwpz oxp ha spnzwocplo zo yyo xza z gflv xyaofwj fu cppoylv oxya hxzggplvp oxwfkvx mkzgyoj pskhzoyfl yl aczgg hgzaawffc pldywflcploa
zgflv qyox ylopwlaxyn zls wpapzwhx fnnfwoklyoypa yl ylskaowj zls lzoyflzg gzefwzofwypa
yyo aoksploa qfwi qyox fkw uzhkgoj fl qfwgshgzaa wpapzwhx yl zwpza oxzo ylhgksp szoz ahyplhp syaowyekops ajaopca ylufwczoyfl wpowypdzg hfcnko
pw lpoqfwiylv ylopggyvplo ylufwczoyfl ajaopca zls zgvfwyoxca
oxp spnzwocplo fuupwa ezhxpgfw fu ahyplhp czaopw fu ahyplhp nwfupaayflzg czaopw zls nxs spvwppa ngka vwzskzop hpwoyuyhzopa zhhpgpwzops hfkwap
a zls lflspvwpp aoksj nzwooycp aoksploa hzl ozip pdplylv hgzaapa zls gflvsyaozlhp aoksploa hzl pzwl czaopwa spvwppa flgylp aoksploa wzop fkw
opzhxylv za zcflv oxp epao zo oxp klydpwayoj zls fkw uzhkgoj xzdp qfl lkcpwfka opzhxylv zqzwsa
oxp aphwpo aploplhp ya vffs bfe vkja
[10/05/23]seed@VM:~/.../TASK05$ cat task5.txt
hfcnkopw ahyplhp ya wznysgj hxzlvylv oxp qfwgs qyox lpq spdpgfncploa xznnplylv pdpwj szj z wyvfwfka pskhzoyfl hfceylylv oxp oxpfwj fu ylufwcz
oyfl zls hfcnkozoyfl qyox xzlsafl ajaopca zls afuoqzwp spayvl ya oxp ipj of akhhpaa za flp fu oxp fgspao hfcnkopw ahyplhp spnzwocploa yl oxp
hxyhzvf zwpz oxp ha spnzwocplo zo yyo xza z gflv xyaofwj fu cppoylv oxya hxzggplvp oxwfkvx mkzgyoj pskhzoyfl yl aczgg hgzaawffc pldywflcploa
zgflv qyox ylopwlaxyn zls wpapzwhx fnnfwoklyoypa yl ylskaowj zls lzoyflzg gzefwzofwypa
yyo aoksploa qfwi qyox fkw uzhkgoj fl qfwgshgzaa wpapzwhx yl zwpza oxzo ylhgksp szoz ahyplhp syaowyekops ajaopca ylufwczoyfl wpowypdzg hfcnko
pw lpoqfwiylv ylopggyvplo ylufwczoyfl ajaopca zls zgvfwyoxca
oxp spnzwocplo fuupwa ezhxpgfw fu ahyplhp czaopw fu ahyplhp nwfupaayflzg czaopw zls nxs spvwppa ngka vwzskzop hpwoyuyhzopa zhhpgpwzops hfkwap
a zls lflspvwpp aoksj nzwooycp aoksploa hzl ozip pdplylv hgzaapa zls gflvsyaozlhp aoksploa hzl pzwl czaopwa spvwppa flgylp aoksploa wzop fkw
opzhxylv za zcflv oxp epao zo oxp klydpwayoj zls fkw uzhkgoj xzdp qfl lkcpwfka opzhxylv zqzwsa
oxp aphwpo aploplhp ya vffs bfe vkja
[10/05/23]seed@VM:~/.../TASK05$
```



Observation : After the corrupted ciphertext was decoded, only OFB mode was able to recover all of the plaintext.

Task 6: Initial Vector (IV)

Task 6.1. Uniqueness of the IV

```
[10/06/23]seed@VM:~/.../TASK06$ openssl rand -out linson.bin 32
[10/06/23]seed@VM:~/.../TASK06$ xxd -p linson.bin > linson.key
[10/06/23]seed@VM:~/.../TASK06$ openssl rand -out iv1.bin 16
[10/06/23]seed@VM:~/.../TASK06$ xxd -p iv1.bin > iv1_hex.bin
[10/06/23]seed@VM:~/.../TASK06$ openssl rand -out iv2.bin 16
[10/06/23]seed@VM:~/.../TASK06$ xxd -p iv2.bin > iv2_hex.bin
[10/06/23]seed@VM:~/.../TASK06$
```

```
[10/06/23]seed@VM:~/.../TASK06$ openssl rand -hex 32 > linson.key
[10/06/23]seed@VM:~/.../TASK06$ openssl rand out iv1.bin 16
Extra arguments given.
rand: Use -help for summary.
[10/06/23]seed@VM:~/.../TASK06$ openssl rand -out iv1.bin 16
[10/06/23]seed@VM:~/.../TASK06$ xxd -p iv1.bin > iv1_hex.bin
[10/06/23]seed@VM:~/.../TASK06$ openssl rand -out iv2.bin 16
[10/06/23]seed@VM:~/.../TASK06$ xxd -p iv2.bin > iv2_hex.bin
[10/06/23]seed@VM:~/.../TASK06$
[10/06/23]seed@VM:~/.../TASK06$
[10/06/23]seed@VM:~/.../TASK06$ openssl enc -aes-256-cbc -e -in plaintext.txt -out encryptedtext1.bin -K $(cat linson.key)
 -iv $(cat iv1_hex.bin)
[10/06/23]seed@VM:~/.../TASK06$
[10/06/23]seed@VM:~/.../TASK06$ openssl enc -aes-256-cbc -e -in plaintext.txt -out encryptedtext1.bin -K $(cat linson.key)
 -iv $(cat iv1_hex.bin)
[10/06/23]seed@VM:~/.../TASK06$ openssl enc -aes-256-cbc -e -in plaintext.txt -out encryptedtext2.bin -K $(cat linson.key)
 -iv $(cat iv2_hex.bin)
[10/06/23]seed@VM:~/.../TASK06$
[10/06/23]seed@VM:~/.../TASK06$
[10/06/23]seed@VM:~/.../TASK06$ openssl enc -aes-256-cbc -e -in plaintext.txt -out encryptedtext11.bin -K $(cat linson.key
) -iv $(cat iv1_hex.bin)
[10/06/23]seed@VM:~/.../TASK06$ openssl enc -aes-256-cbc -e -in plaintext.txt -out encryptedtext22.bin -K $(cat linson.key
) -iv $(cat iv1_hex.bin)
[10/06/23]seed@VM:~/.../TASK06$ cmp encryptedtext11.bin encryptedtext22.bin
[10/06/23]seed@VM:~/.../TASK06$
```

Observation : Different iv were used to encrypt the same plane text file and two different cipher text files were generatded.
used same iv to encrypt the same plane text file an got two identical cipher text files.

Task 6.2. Common Mistake: Use the Same IV

```python
# Define the known plaintext (P1) and its corresponding ciphertext (C1)
P1 = "This is a known message!"
C1_hex = "a469b1c502c1cab966965e50425438e1bb1b5f9037a4c15913"

# Convert the ciphertext from hex to bytes
C1 = bytes.fromhex(C1_hex)

# Calculate the keystream by XORing P1 and C1
keystream = bytes([a ^ b for a, b in zip(P1.encode(), C1)])

# Define the ciphertext for P2 (C2)
C2_hex = "bf73bcd3509299d566c35b5d450337e1bb175f903fafc15913"

# Convert the ciphertext for P2 from hex to bytes
C2 = bytes.fromhex(C2_hex)

# Decrypt P2 by XORing C2 with the keystream
P2 = bytes([a ^ b for a, b in zip(C2, keystream)])

# Print the result
print("Decrypted P2:", P2.decode())
```

```
[10/06/23]seed@VM:~/.../TASK06$ python3 task6.py
Decrypted P2: Order: Launch a missile!
[10/06/23]seed@VM:~/.../TASK06$
```

Observation : In CFB mode, the technique of encryption makes it very challenging for an adversary to successfully carry out a known plaintext attack if the attacker tries to predict the IV. Although the IV is encrypted before being XORed with the first plaintext, using the IV repeatedly will allow the attacker to achieve a high value of the P2 because using the IV leaves traces or patterns for the adversary to connect the dots and decrypt the Ciphertext of the second plaintext since encryption of the second plaintext depends on Ciphertext of the first plaintext.

Task 6.3. Common Mistake: Use a Predictable IV

Encryption method: 128-bit AES with CBC mode.
Key (in hex): 00112233445566778899aabbccddeeff (known only to Bob)
Ciphertext (C1): bef65565572ccee2a9f9553154ed9498 (known to both)
IV used on P1 (known to both)
(in ascii): 1234567890123456
(in hex) : 31323334353637383930313233343536
Next IV (known to both)
(in ascii): 1234567890123457
(in hex) : 31323334353637383930313233343537
“Yes” in Hex: 596573
“No” in Hex: 4E6F
P2(in Hex) = IV1 XOR IV2 XOR YES(in hex : 596573) =
31323334353637383930313233343536
XOR
31323334353637383930313233343537
XOR
596573
P2(in Hex) = 596572

Therefore, Bob will encrypt P2(in Hex) and check if it matches to C1 or not. If it matches to C1 then the actual content of P1 is “Yes”, otherwise it is “No”.

P1 = 31323334353637383930313233343536
XOR
31323334353637383930313233343537
P1 = 1
We consider 1 = Yes and 0 = No.
Hence, the actual content of P1 is “Yes”.

Task 7: Programming using the Crypto Library

Code:

```python
#!/usr/bin/python3
from sys import argv
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad

_, input_data, ciphertext_hex, iv_hex = argv

assert len(input_data) == 21
data = bytearray(input_data, encoding='utf-8')
ciphertext = bytearray.fromhex(ciphertext_hex)
iv = bytearray.fromhex(iv_hex)

with open('./words.txt') as f:
    keys = f.readlines()

for key_candidate in keys:
    key_candidate = key_candidate.rstrip('\n')
    if len(key_candidate) <= 16:
        key = key_candidate + '#' * (16 - len(key_candidate))
        cipher = AES.new(key=bytearray(key, encoding='utf-8'),
                         mode=AES.MODE_CBC, iv=iv)
        guess = cipher.encrypt(pad(data, 16))
        if guess == ciphertext:
            print("Found the key:", key)
            exit(0)

print("Cannot find the key!")
```

- Used python code to implement this task .
- Created a user defined code where we can use the plaintext value, iv, ciphertext to get the output .

Output :

```
[10/08/23]seed@VM:~/.../TASK07$ 7.1.py "This is a secret tool" \ec
e6753e938f8f903cabbbe12d395bf5f7eae38ad918a2d3e1c3a832476d5c7a \01
02030405060708090a0b0c0d0e0f
find the key: safety##########
```

Observation: After giving the input from the labsetup file the key was obtained .