Lab3

Name: Zhiyuan Ma, Wenting Zheng

Task 1: Frequency Analysis

abcdefghijklmnopqrstuvwxyz ->
cfmypvbrlqxwiejdsgkhnazotu

tr 'abcdefghijklmnopqrstuvwxyz' 'cfmypvbrlqxwiejdsgkhnazotu' < in.txt > out.txt

```
[11/08/22]seed@VM:~/lab3$ ls
ciphertext.txt
[11/08/22]seed@VM:~/lab3$  tr 'abcdefghijklmnopqrstuvwxyz' 'cfmypvbrlqxwiejdsgkhnazotu' < ciphertext.txt > o
ut.txt
[11/08/22]seed@VM:~/lab3$ ls
ciphertext.txt  out.txt
[11/08/22]seed@VM:~/lab3$ cat out.txt
the oscars turn  on sunday which seems about right after this long strange
awards trip the bagger feels like a nonagenarian too
```

Example for out.txt:
the oscars turn on sunday which seems about right after this long strange
awards trip the bagger feels like a nonagenarian too

the awards race was bookended by the demise of harvey weinstein at its outset
and the apparent implosion of his film company at the end and it was shaped by
the emergence of metoo times up blackgown politics armcandy activism and
a national conversation as brief and mad as a fever dream about whether there
ought to be a president winfrey the season didnt just seem extra long it was
extra long because the oscars were moved to the first weekend in march to
avoid conflicting with the closing ceremony of the winter olympics thanks
pyeongchang

one big question surrounding this years academy awards is how or if the
ceremony will address metoo especially after the golden globes which became
a jubilant comingout party for times up the movement spearheaded by
powerful hollywood women who helped raise millions of dollars to fight sexual
harassment around the country

signaling their support golden globes attendees swathed themselves in black
sported lapel pins and sounded off about sexist power imbalances from the red
carpet and the stage on the air e was called out about pay inequity after
its former anchor catt sadler quit once she learned that she was making far

less than a male cohost and during the ceremony natalie portman took a blunt and satisfying dig at the allmale roster of nominated directors how could that be topped

as it turns out at least in terms of the oscars it probably wont be

women involved in times up said that although the globes signified the initiatives launch they never intended it to be just an awards season campaign or one that became associated only with redcarpet actions instead a spokeswoman said the group is working behind closed doors and has since amassed million for its legal defense fund which after the globes was flooded with thousands of donations of or less from people in some countries

Task 2: Encryption using Different Ciphers and Modes

First: aes-128-cfb

```
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-cfb -e -in out.txt -out cipher.bin -K 00112233445566778889aab
bccddeeff -iv 0102030405060708
[11/08/22]seed@VM:~/lab3$ ls
cipher.bin  ciphertext.txt  out.txt
[11/08/22]seed@VM:~/lab3$
```

Second: bf-cbc

```
[11/08/22]seed@VM:~/lab3$ openssl enc -bf-cbc -e -in out.txt -out cipher.bin -K 00112233445566778889aabbccdd
eeff -iv 0102030405060708
[11/08/22]seed@VM:~/lab3$ ls
cipher.bin  ciphertext.txt  out.txt
```

Third: aes-128-cbc

```
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-cbc -e -in out.txt -out cipher.bin -K 00112233445566778889aab
bccddeeff -iv 0102030405060708
[11/08/22]seed@VM:~/lab3$ ls
cipher.bin  ciphertext.txt  out.txt
```

Task 3: Encryption Mode – ECB vs. CBC

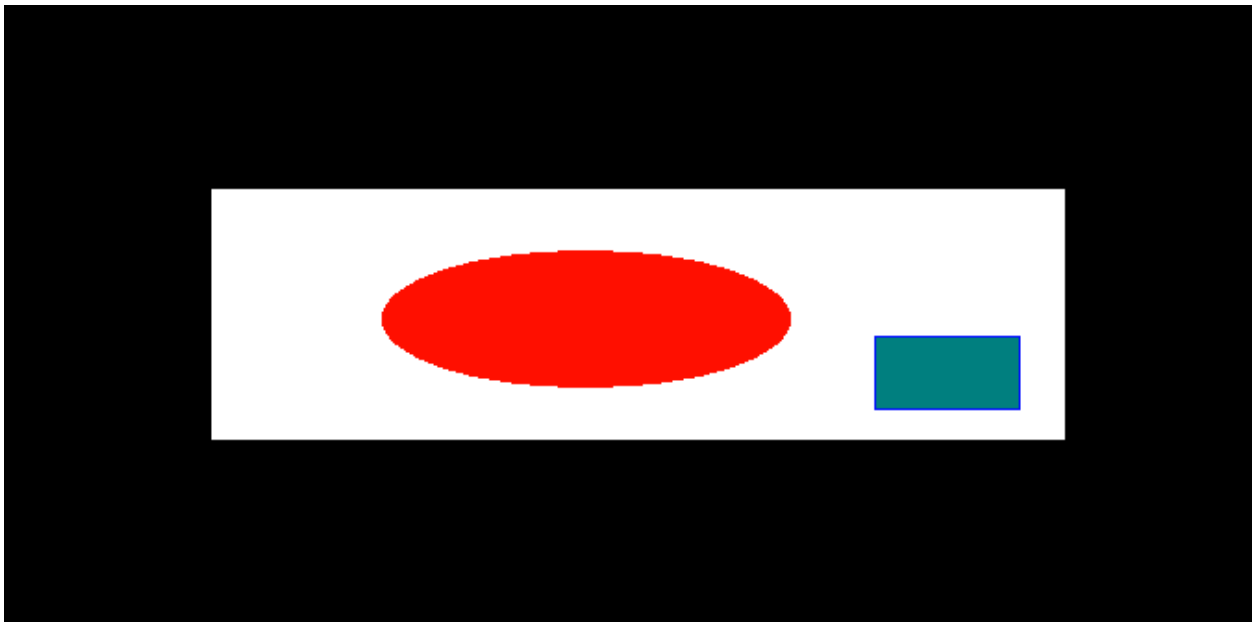
ECB:

```
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-ecb -e -in pic_original.bmp -out
cipher.bin -K 00112233445566778889aabbccddeeff -iv 0102030405060708
warning: iv not use by this cipher
[11/08/22]seed@VM:~/lab3$ ls
cipher.bin  ciphertext.txt  out.txt  pic_original.bmp
```

CBC:

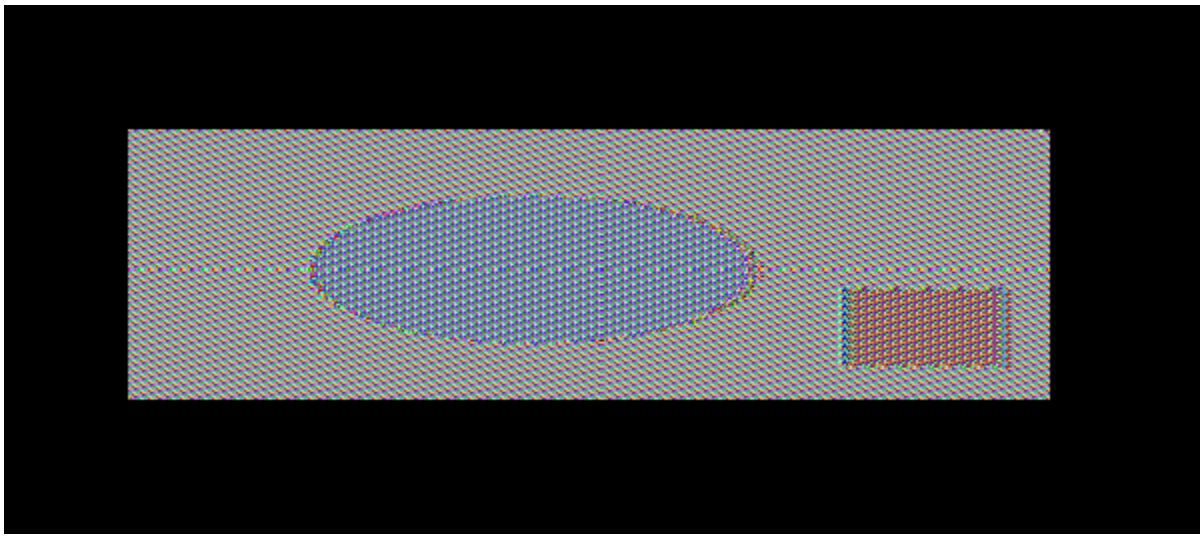
```
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-cbc -e -in pic_original.bmp -out
cipher1.bin -K 00112233445566778889aabbccddeeff -iv 0102030405060708
[11/08/22]seed@VM:~/lab3$ ls
cipher1.bin  cipher.bin  ciphertext.txt  out.txt  pic_original.bmp
[11/08/22]seed@VM:~/lab3$
```

Original Image:



Ecb:

```
[11/08/22]seed@VM:~/lab3$ tail -c +55 cipher.bin > body
[11/08/22]seed@VM:~/lab3$ cat header body > new.bmp
```

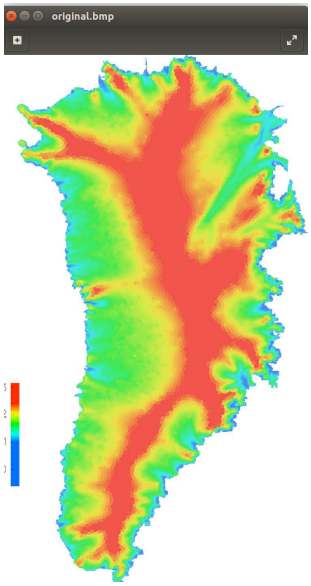


cbc:

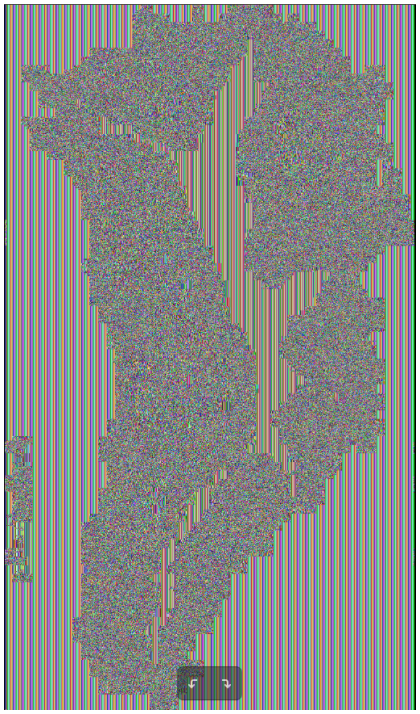
```
[11/08/22]seed@VM:~/lab3$  head -c 54 pic_original.bmp > header
[11/08/22]seed@VM:~/lab3$  tail -c +55 cipher1.bin > body
[11/08/22]seed@VM:~/lab3$ cat header body > new.bmp
```

Self-defined image: The conclusion is that we could see the shape of original image after ecb, but we can't see any detail after cbc

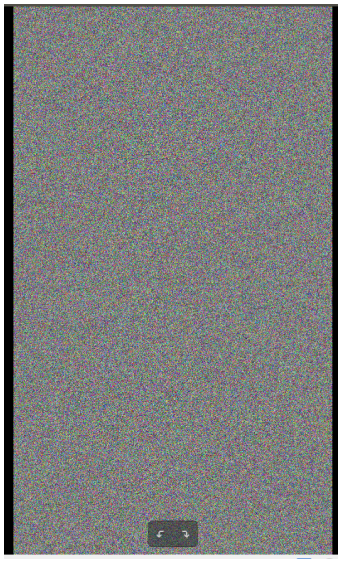
Original:



Ecb: could still see the image



Cbc: can’t see the shape any more



Task 4: Padding

We encrypt out.txt into cipher.bin and compare the size, out.txt is 4759
ECB: 4759-> 4768 has padding

```
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-ecb -e -in out.txt -out cipher.bi
n -K 00112233445566778889aabbccddeeff -iv 0102030405060708
warning: iv not use by this cipher
[11/08/22]seed@VM:~/lab3$ ls -al *
-rw-rw-r-- 1 seed seed 2995056 Nov  8 14:27 cipher1.bin
-rw-rw-r-- 1 seed seed    4768 Nov  8 17:37 cipher.bin
-rw-rw-r-- 1 seed seed    4759 Nov  8 01:29 ciphertext.txt
-rw-rw-r-- 1 seed seed 2995056 Nov  8 14:30 new.bmp
-rw-rw-r-- 1 seed seed 2995046 Mar 15  2011 original.bmp
-rw-rw-r-- 1 seed seed    4759 Nov  8 02:32 out.txt
-rw-rw-r-- 1 seed seed  184974 Oct 26 14:01 pic_original.bmp
```

CBC: 4759->4768 has padding

```
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-cbc -e -in out.txt -out cipher.bi
n -K 00112233445566778889aabbccddeeff -iv 0102030405060708
[11/08/22]seed@VM:~/lab3$ ls -al *
-rw-rw-r-- 1 seed seed 2995056 Nov  8 14:27 cipher1.bin
-rw-rw-r-- 1 seed seed    4768 Nov  8 17:38 cipher.bin
-rw-rw-r-- 1 seed seed    4759 Nov  8 01:29 ciphertext.txt
-rw-rw-r-- 1 seed seed 2995056 Nov  8 14:30 new.bmp
-rw-rw-r-- 1 seed seed 2995046 Mar 15  2011 original.bmp
-rw-rw-r-- 1 seed seed    4759 Nov  8 02:32 out.txt
-rw-rw-r-- 1 seed seed  184974 Oct 26 14:01 pic_original.bmp
[11/08/22]seed@VM:~/lab3$
```

CFB: 4759-> 4759 no padding

```
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-cfb -e -in out.txt -out cipher.bi
n -K 00112233445566778889aabbccddeeff -iv 0102030405060708
[11/08/22]seed@VM:~/lab3$ ls -al *
-rw-rw-r-- 1 seed seed 2995056 Nov  8 14:27 cipher1.bin
-rw-rw-r-- 1 seed seed    4759 Nov  8 17:41 cipher.bin
-rw-rw-r-- 1 seed seed    4759 Nov  8 01:29 ciphertext.txt
-rw-rw-r-- 1 seed seed 2995056 Nov  8 14:30 new.bmp
-rw-rw-r-- 1 seed seed 2995046 Mar 15  2011 original.bmp
-rw-rw-r-- 1 seed seed    4759 Nov  8 02:32 out.txt
-rw-rw-r-- 1 seed seed  184974 Oct 26 14:01 pic_original.bmp
[11/08/22]seed@VM:~/lab3$
```

OFB:4759->4759 no padding

```
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-ofb -e -in out.txt -out cipher.bi
n -K 00112233445566778889aabbccddeeff -iv 0102030405060708
[11/08/22]seed@VM:~/lab3$ ls -al *
-rw-rw-r-- 1 seed seed 2995056 Nov  8 14:27 cipher1.bin
-rw-rw-r-- 1 seed seed    4759 Nov  8 17:42 cipher.bin
-rw-rw-r-- 1 seed seed    4759 Nov  8 01:29 ciphertext.txt
-rw-rw-r-- 1 seed seed 2995056 Nov  8 14:30 new.bmp
-rw-rw-r-- 1 seed seed 2995046 Mar 15  2011 original.bmp
-rw-rw-r-- 1 seed seed    4759 Nov  8 02:32 out.txt
-rw-rw-r-- 1 seed seed  184974 Oct 26 14:01 pic_original.bmp
[11/08/22]seed@VM:~/lab3$
```

2. Make three files size 5, 10 ,16

```
[11/08/22]seed@VM:~/lab3$ ls -al *
-rw-rw-r-- 1 seed seed 2995056 Nov  8 14:27 cipher1.bin
-rw-rw-r-- 1 seed seed    4759 Nov  8 17:42 cipher.bin
-rw-rw-r-- 1 seed seed    4759 Nov  8 01:29 ciphertext.txt
-rw-rw-r-- 1 seed seed       5 Nov  8 17:50 f1.txt
-rw-rw-r-- 1 seed seed      10 Nov  8 17:50 f2.txt
-rw-rw-r-- 1 seed seed      16 Nov  8 17:50 f3.txt
-rw-rw-r-- 1 seed seed 2995056 Nov  8 14:30 new.bmp
-rw-rw-r-- 1 seed seed 2995046 Mar 15  2011 original.bmp
-rw-rw-r-- 1 seed seed    4759 Nov  8 02:32 out.txt
-rw-rw-r-- 1 seed seed  184974 Oct 26 14:01 pic_original.bmp
```

The result shows that 5 become 16, 10 becomes 16, and 16 becomes 32

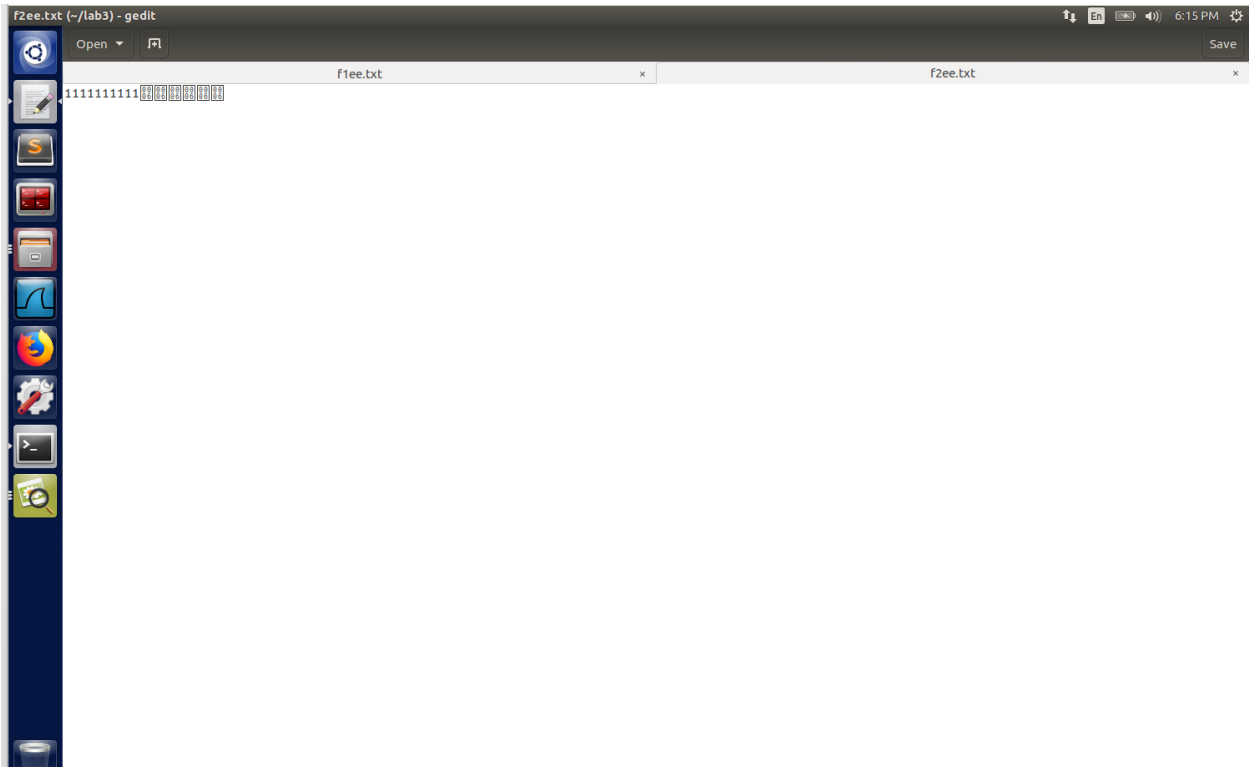
```
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-cbc -e -in f1.txt -out f1e.txt -K
 00112233445566778889aabbccddeeff -iv 0102030405060708
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-cbc -e -in f2.txt -out f2e.txt -K
 00112233445566778889aabbccddeeff -iv 0102030405060708
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-cbc -e -in f3.txt -out f3e.txt -K
 00112233445566778889aabbccddeeff -iv 0102030405060708
[11/08/22]seed@VM:~/lab3$ ls -al *
-rw-rw-r-- 1 seed seed 2995056 Nov  8 14:27 cipher1.bin
-rw-rw-r-- 1 seed seed    4759 Nov  8 17:42 cipher.bin
-rw-rw-r-- 1 seed seed    4759 Nov  8 01:29 ciphertext.txt
-rw-rw-r-- 1 seed seed      16 Nov  8 18:06 f1e.txt
-rw-rw-r-- 1 seed seed       5 Nov  8 17:50 f1.txt
-rw-rw-r-- 1 seed seed      16 Nov  8 18:06 f2e.txt
-rw-rw-r-- 1 seed seed      10 Nov  8 17:50 f2.txt
-rw-rw-r-- 1 seed seed      32 Nov  8 18:06 f3e.txt
-rw-rw-r-- 1 seed seed      16 Nov  8 17:50 f3.txt
-rw-rw-r-- 1 seed seed 2995056 Nov  8 14:30 new.bmp
-rw-rw-r-- 1 seed seed 2995046 Mar 15  2011 original.bmp
-rw-rw-r-- 1 seed seed    4759 Nov  8 02:32 out.txt
-rw-rw-r-- 1 seed seed  184974 Oct 26 14:01 pic_original.bmp
```

Decrypt the files:

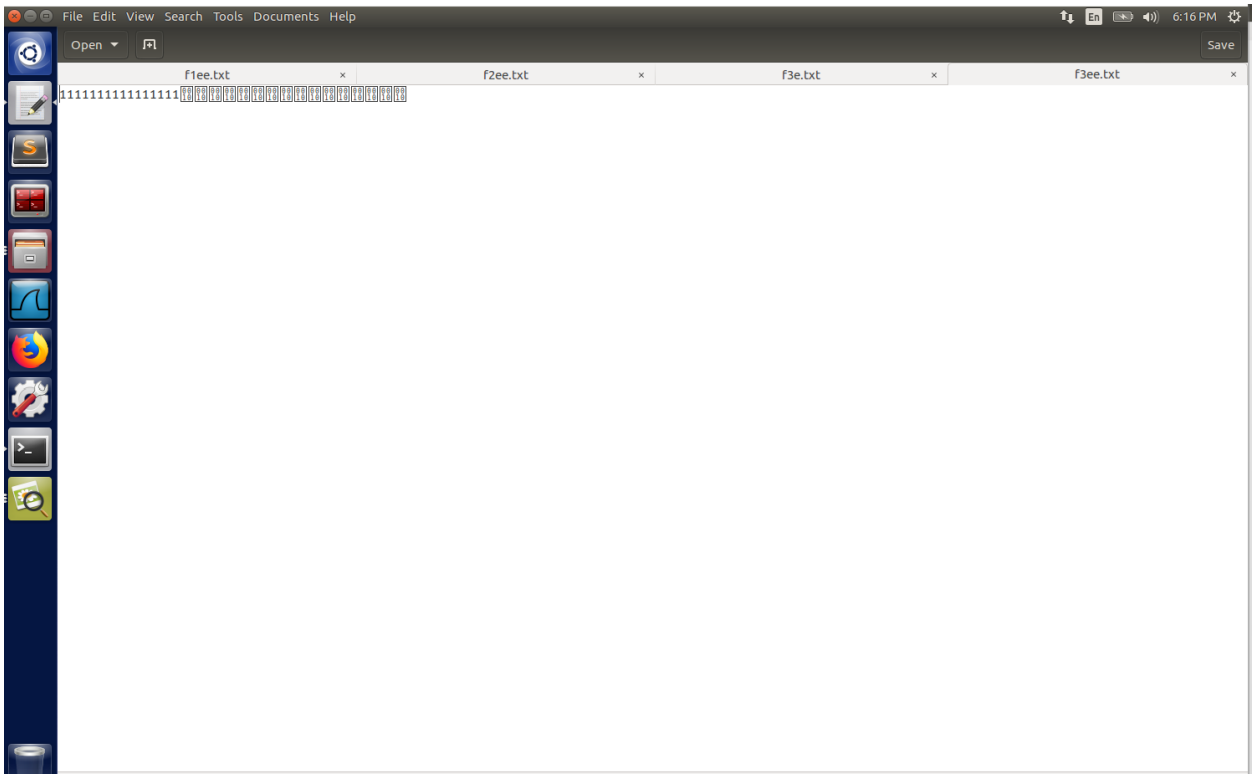
```
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-cbc -d -in f1e.txt -out f1ee.txt
-K 00112233445566778889aabbccddeeff -iv 0102030405060708 -nopad
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-cbc -d -in f2e.txt -out f2ee.txt
-K 00112233445566778889aabbccddeeff -iv 0102030405060708 -nopad
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-cbc -d -in f3e.txt -out f3ee.txt
-K 00112233445566778889aabbccddeeff -iv 0102030405060708 -nopad
[11/08/22]seed@VM:~/lab3$ ls -al *
-rw-rw-r-- 1 seed seed 2995056 Nov  8 14:27 cipher1.bin
-rw-rw-r-- 1 seed seed    4759 Nov  8 17:42 cipher.bin
-rw-rw-r-- 1 seed seed    4759 Nov  8 01:29 ciphertext.txt
-rw-rw-r-- 1 seed seed      16 Nov  8 18:12 f1ee.txt
-rw-rw-r-- 1 seed seed      16 Nov  8 18:06 f1e.txt
-rw-rw-r-- 1 seed seed       5 Nov  8 17:50 f1.txt
-rw-rw-r-- 1 seed seed      16 Nov  8 18:12 f2ee.txt
-rw-rw-r-- 1 seed seed      16 Nov  8 18:06 f2e.txt
-rw-rw-r-- 1 seed seed      10 Nov  8 17:50 f2.txt
-rw-rw-r-- 1 seed seed      32 Nov  8 18:12 f3ee.txt
-rw-rw-r-- 1 seed seed      32 Nov  8 18:06 f3e.txt
-rw-rw-r-- 1 seed seed      16 Nov  8 17:50 f3.txt
-rw-rw-r-- 1 seed seed 2995056 Nov  8 14:30 new.bmp
-rw-rw-r-- 1 seed seed 2995046 Mar 15  2011 original.bmp
-rw-rw-r-- 1 seed seed    4759 Nov  8 02:32 out.txt
-rw-rw-r-- 1 seed seed  184974 Oct 26 14:01 pic_original.bmp
[11/08/22]seed@VM:~/lab3$
```

5 byte -> 16 byte:

10 byte-> 16 byte



16 byte -> 32 byte:

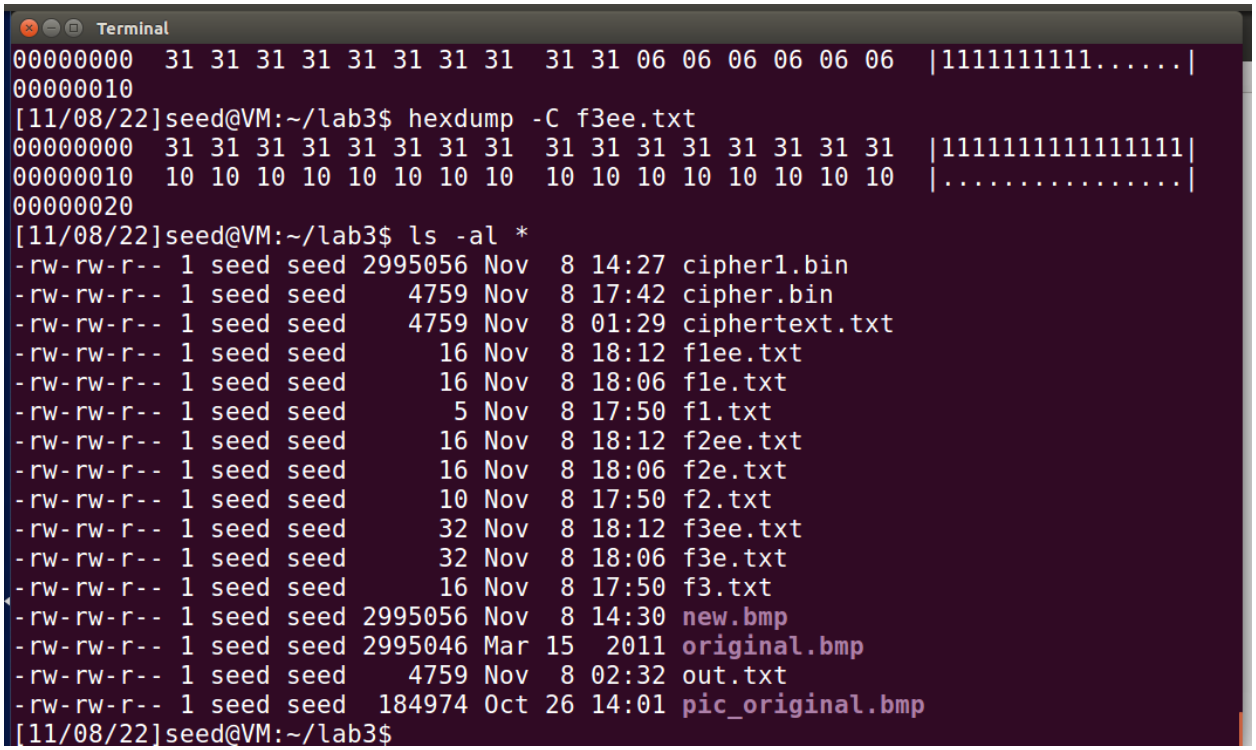


We could see the padding after hex dump

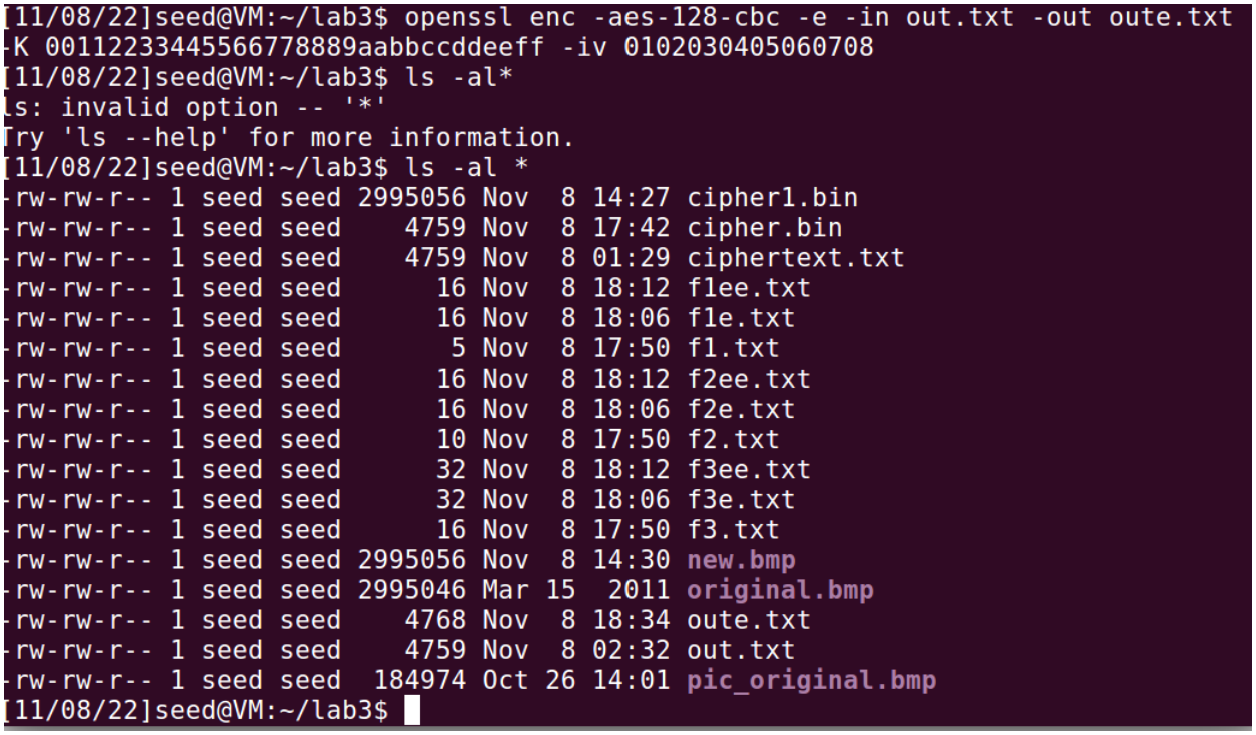
```
[11/08/22]seed@VM:~/lab3$ hexdump -C p1ee.txt
hexdump: p1ee.txt: No such file or directory
[11/08/22]seed@VM:~/lab3$ hexdump -C f1ee.txt
00000000  31 32 33 34 35 0b 0b 0b  0b 0b 0b 0b 0b 0b 0b 0b  |12345...........|
00000010
[11/08/22]seed@VM:~/lab3$ hexdump -C f2ee.txt
00000000  31 31 31 31 31 31 31 31  31 31 06 06 06 06 06 06  |1111111111......|
00000010
[11/08/22]seed@VM:~/lab3$ hexdump -C f3ee.txt
00000000  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  |1111111111111111|
00000010  10 10 10 10 10 10 10 10  10 10 10 10 10 10 10 10  |................|
00000020
[11/08/22]seed@VM:~/lab3$
```

Task 5: Error Propagation – Corrupted Cipher Text

1. Create a text file that is at least 1000 bytes long.
We would like to use out.txt from the task one, size is 4759

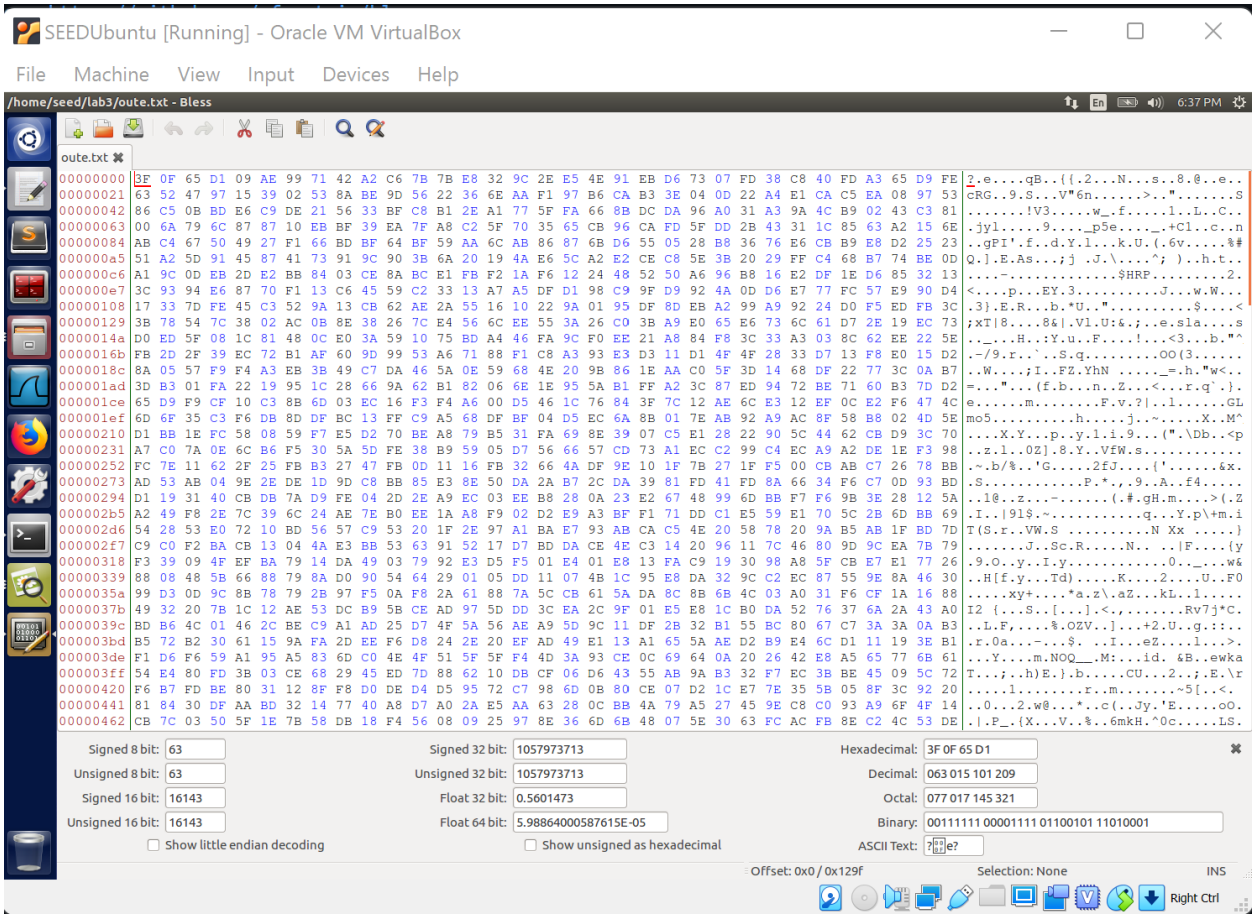


2. Encrypt the file using the AES-128 cipher oute.txt



3. Unfortunately, a single bit of the 55th byte in the encrypted file got corrupted. You can achieve this corruption using the bless hex editor.

CBC:



A line was broken and extra content are fine:

```
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-cbc -d -in oute.txt -out outd.txt
 -K 00112233445566778889aabbccddeeff -iv 0102030405060708
[11/08/22]seed@VM:~/lab3$ cat outd.txt
the oscars turn  on sunday which seems about right after this long strange
awards trip the bagger feels like a nonagenarian too

the awards race was bookended by the demise of harvey weinstein at its outset
and the apparent implosion of his film company at the end and it was shaped by
the emergence of m=B8~[k[vackg[wn politics[[o[v[[w[[[m[[[sm an[[a national
 conversation as brief and mad as a fever dream about whether there
ought to be a president winfrey the season didnt just seem extra long it was
extra long because the oscars were moved to the first weekend in march to
avoid conflicting with the closing ceremony of the winter olympics thanks
pyeongchang
```

ECB:
Several lines are affected

```
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-ecb -d -in oute.txt -out outd.txt
  -K 00112233445566778889aabbccddeeff -iv 0102030405060708
warning: iv not use by this cipher
[11/08/22]seed@VM:~/lab3$ cat outd.txt
the oscars turn  on sunday which seems about right after this long strange
awards trip the baggeX@)@@@
                                 ▯▯@@▯▯/onagenarian too

the awards race was bookended by the demise of harvey weinstein at its outset
and the apparent implosion of his film company at the end and it was shaped by
```

CBC:Can’t decrypt

```
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-cbc -e -in out.txt -out oute.txt
-K 00112233445566778889aabbccddeeff -iv 0102030405060708
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-cbc -d -in oute.txt -out outd.txt
 -K 00112233445566778889aabbccddeeff -iv 0102030405060708
bad decrypt
3070551744:error:0606506D:digital envelope routines:EVP_DecryptFinal_ex:wrong fi
nal block length:evp_enc.c:518:
[11/08/22]seed@VM:~/lab3$
```

CFB:
All lines affected:

```
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-cfb -d -in oute.txt -out outd.txt
 -K 00112233445566778889aabbccddeeff -iv 0102030405060708
[11/08/22]seed@VM:~/lab3$ cat outd.txt
the oscars turn  on sunday which seems ab@v@@/@n@ @@i@@@V@@=@@@f@@3@lv▫@@@@@@*@@
x@"@@@@@@au@@@@@@@D@@@(@3e@;s3@@@@@2@@R@@L@@@`@)Ì@h@k@@@@C
                                                        @@9@'$@@0w@@'Kv@{j@B
u<?@t@@@@@a@@@#@1@@@@@@r@Q@(I@@N@@Q@E~@jd1@>@@@@@@@j{@@%@`@P@Q@@7L@_/@@ú@@@ F@t@@
@@@'S@(@b?x@@RY@Q@@N3O@@@@L@)@&@@2@@@@@K@g@jc@OG@08Z@@@@u@@@@@@@
~f{M
    @@~@@s@@@@@@@gC@@@@i@@@@@)tlqQ@e@-@@q@@@N@@P杳qP|@@@@@9@@@@@@f@e@J@l@@H$@@@@
@@@@
  @f@U@A6@@@@.[@@@@w@@%@@@@b@@&@v>@@@d@P@@/&     @@Vq@@n;%@F@@@@@@@FE@@s@@y@@@@n@@@
-0@@@@@0@@@/x@TA@@{@@@@@>ž<@@@$5@@3@U@@@@@<@@@+`@W3@qd@@y@;@@,@@@@4м@@@u`@-P@@@@@@&
@@I@@V@#@t@6@@@@ L@@@U@~@@@YBj@{u@(@8#@wu {Q@3X@@@TQ@X@f@I@@T@@@@RO(@%@@@@@VzF@@@)@
```

OFB:
Barely anything is affected

```
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-ofb -e -in out.txt -out oute.txt
-K 00112233445566778889aabbccddeeff -iv 0102030405060708
[11/08/22]seed@VM:~/lab3$ openssl enc -aes-128-ofb -d -in oute.txt -out outd.tx
 -K 00112233445566778889aabbccddeeff -iv 0102030405060708
[11/08/22]seed@VM:~/lab3$ cat outd.txt
the oscars turn  on sunday which seems about right after this long strange
awards trip the bagger feels like a nonagjnarian too

the awards race was bookended by the demise of harvey weinstein at its outset
and the apparent implosion of his film company at the end and it was shaped by
the emergence of metoo times up blackgown politics armcandy activism and
a national conversation as brief and mad as a fever dream about whether there
ought to be a president winfrey the season didnt just seem extra long it was
extra long because the oscars were moved to the first weekend in march to
avoid conflicting with the closing ceremony of the winter olympics thanks
```