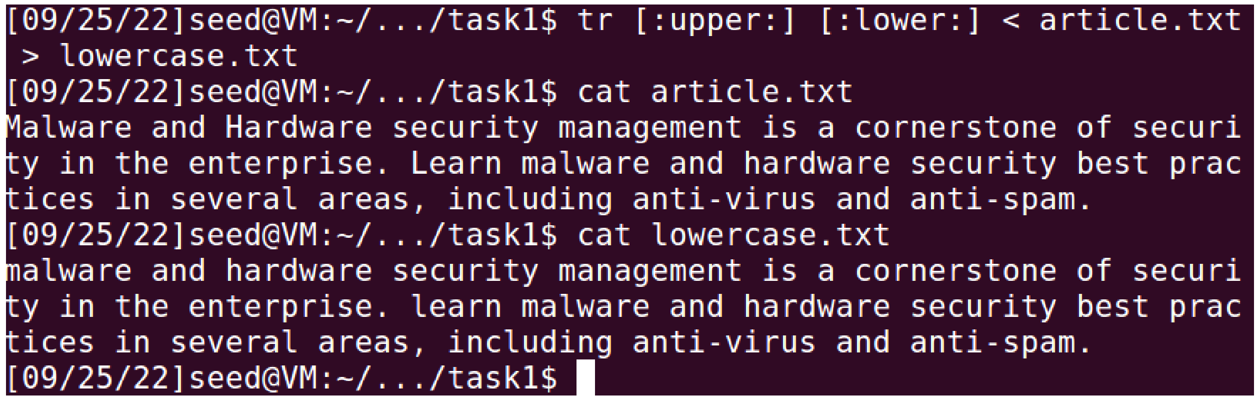
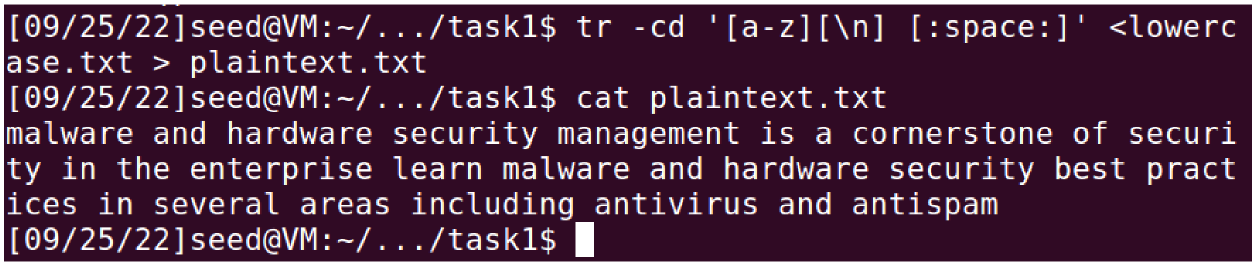
Task 1: Frequency Analysis

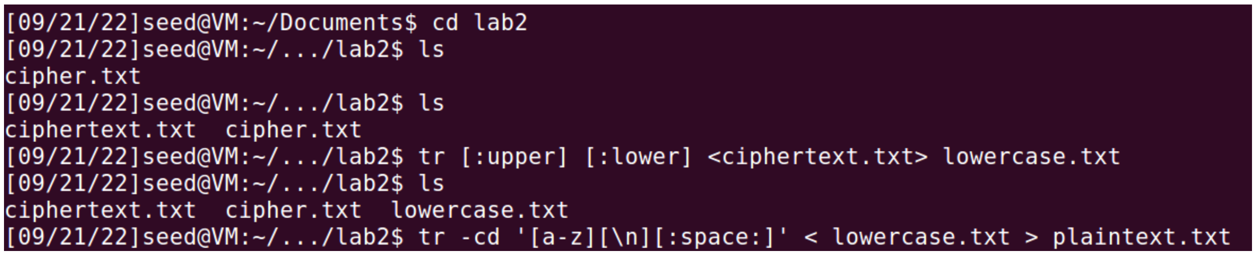
For task1 we used our own article.
Step 1: Encrypting the file and simplification made to it.



```
[09/25/22]seed@VM:~/.../task1$ tr [:upper:] [:lower:] < article.txt
 > lowercase.txt
[09/25/22]seed@VM:~/.../task1$ cat article.txt
Malware and Hardware security management is a cornerstone of securi
ty in the enterprise. Learn malware and hardware security best prac
tices in several areas, including anti-virus and anti-spam.
[09/25/22]seed@VM:~/.../task1$ cat lowercase.txt
malware and hardware security management is a cornerstone of securi
ty in the enterprise. learn malware and hardware security best prac
tices in several areas, including anti-virus and anti-spam.
[09/25/22]seed@VM:~/.../task1$
```

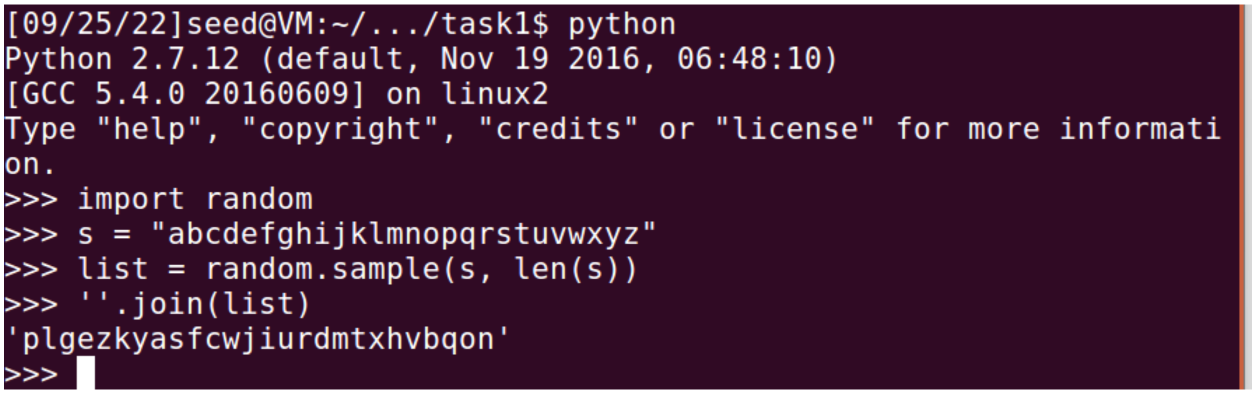


```
[09/25/22]seed@VM:~/.../task1$ tr -cd '[a-z][\n] [:space:]' <lowerc
ase.txt > plaintext.txt
[09/25/22]seed@VM:~/.../task1$ cat plaintext.txt
malware and hardware security management is a cornerstone of securi
ty in the enterprise learn malware and hardware security best pract
ices in several areas including antivirus and antispam
[09/25/22]seed@VM:~/.../task1$
```



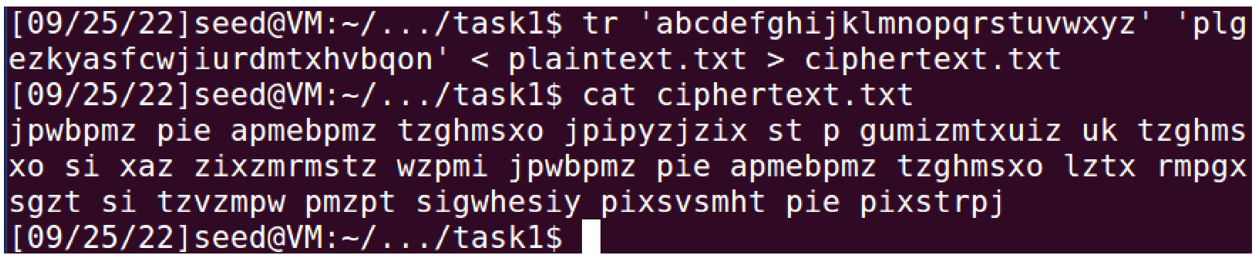
```
[09/21/22]seed@VM:~/Documents$ cd lab2
[09/21/22]seed@VM:~/.../lab2$ ls
cipher.txt
[09/21/22]seed@VM:~/.../lab2$ ls
ciphertext.txt  cipher.txt
[09/21/22]seed@VM:~/.../lab2$ tr [:upper] [:lower] <ciphertext.txt> lowercase.txt
[09/21/22]seed@VM:~/.../lab2$ ls
ciphertext.txt  cipher.txt  lowercase.txt
[09/21/22]seed@VM:~/.../lab2$ tr -cd '[a-z][\n][:space:]' < lowercase.txt > plaintext.txt
```

Step 2: Generating encryption key in Python



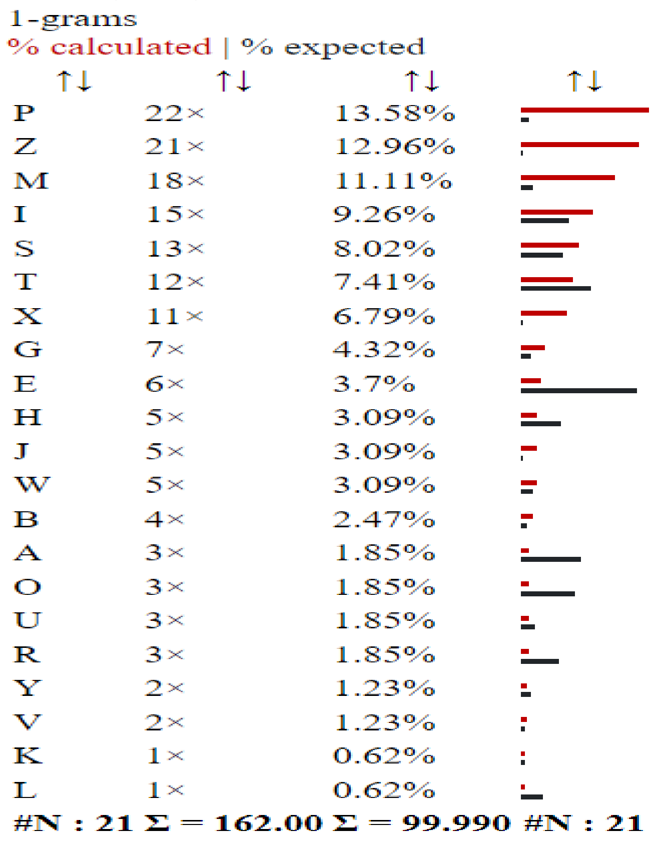
```
[09/25/22]seed@VM:~/.../task1$ python
Python 2.7.12 (default, Nov 19 2016, 06:48:10)
[GCC 5.4.0 20160609] on linux2
Type "help", "copyright", "credits" or "license" for more informati
on.
>>> import random
>>> s = "abcdefghijklmnopqrstuvwxyz"
>>> list = random.sample(s, len(s))
>>> ''.join(list)
'plgezkyasfcwjiurdmtxhvbqon'
>>>
```

Step 3: tr command to do the encryption of letters leaving the space and returning characters alone



```
[09/25/22]seed@VM:~/.../task1$ tr 'abcdefghijklmnopqrstuvwxyz' 'plg
ezkyasfcwjiurdmtxhvbqon' < plaintext.txt > ciphertext.txt
[09/25/22]seed@VM:~/.../task1$ cat ciphertext.txt
jpwbpmz pie apmebpmz tzghmsxo jpipyzjzix st p gumizmtxuiz uk tzghms
xo si xaz zixzmrmstz wzpmi jpwbpmz pie apmebpmz tzghmsxo lztx rmpgx
sgzt si tzvzmpw pmzpt sigwhesiy pixsvsmht pie pixstrpj
[09/25/22]seed@VM:~/.../task1$
```

Frequency Analysis for our own article:



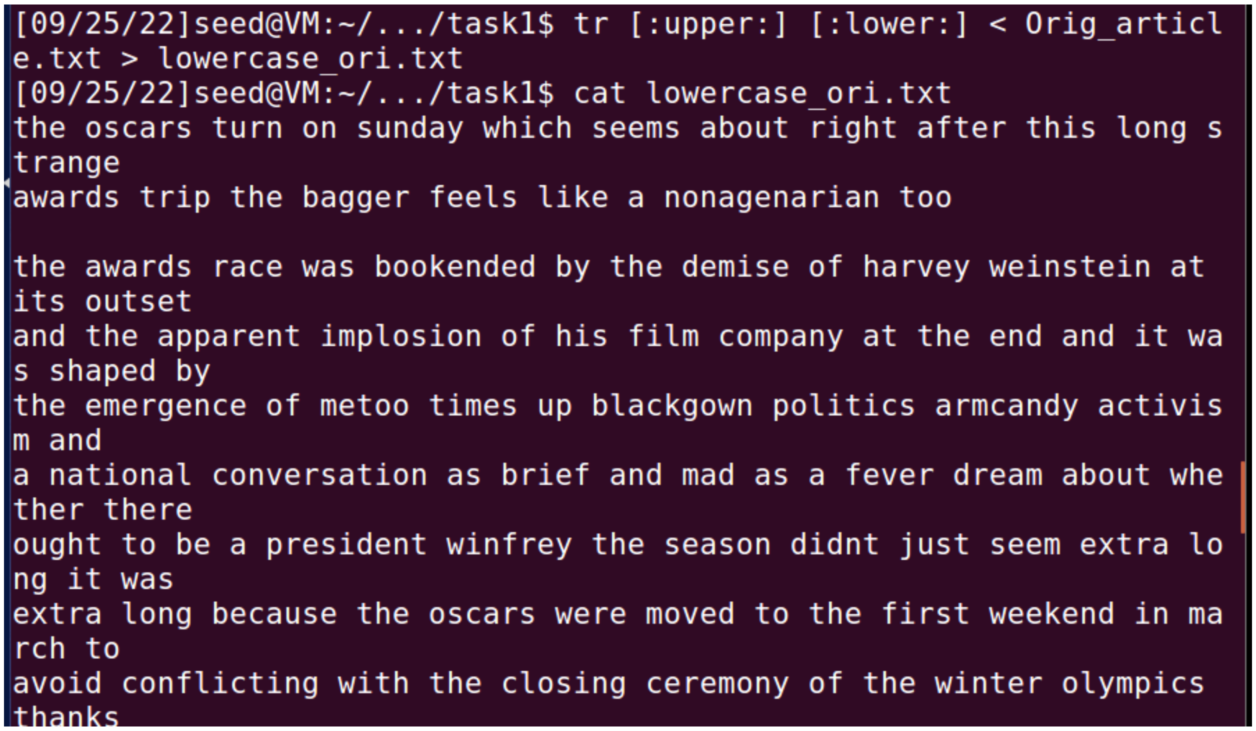
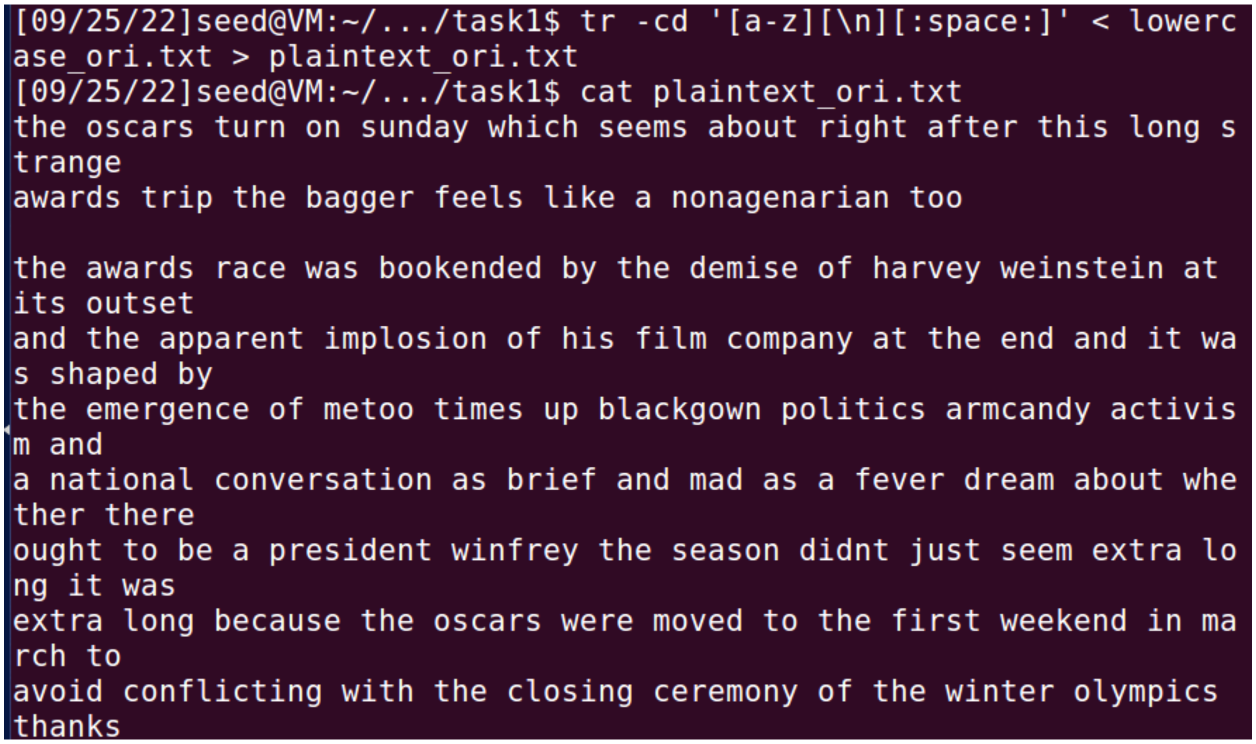
1-grams

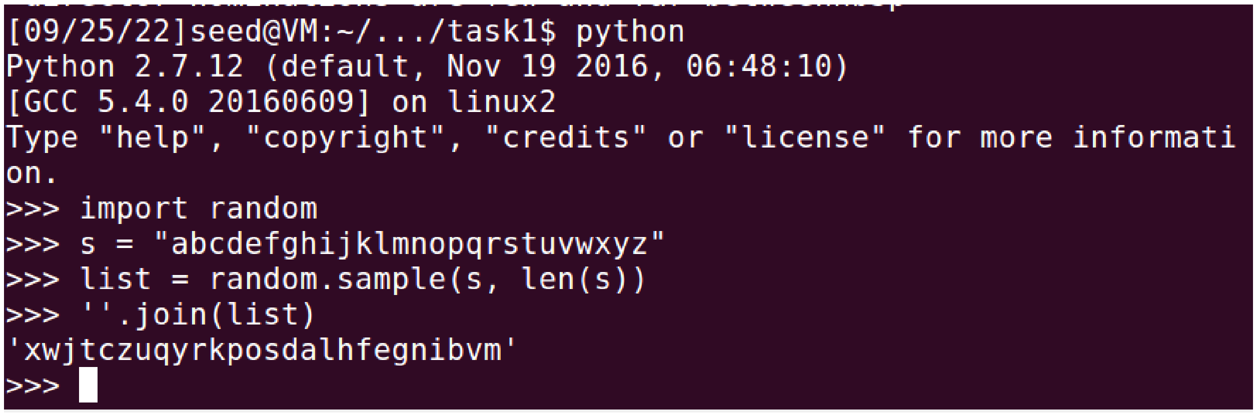
% calculated | % expected

↑↓	↑↓	↑↓	↑↓
P	22×	13.58%	
Z	21×	12.96%	
M	18×	11.11%	
I	15×	9.26%	
S	13×	8.02%	
T	12×	7.41%	
X	11×	6.79%	
G	7×	4.32%	
E	6×	3.7%	
H	5×	3.09%	
J	5×	3.09%	
W	5×	3.09%	
B	4×	2.47%	
A	3×	1.85%	
O	3×	1.85%	
U	3×	1.85%	
R	3×	1.85%	
Y	2×	1.23%	
V	2×	1.23%	
K	1×	0.62%	
L	1×	0.62%	
#N : 21	Σ = 162.00	Σ = 99.990	#N : 21

For Original article from the seedlabs:

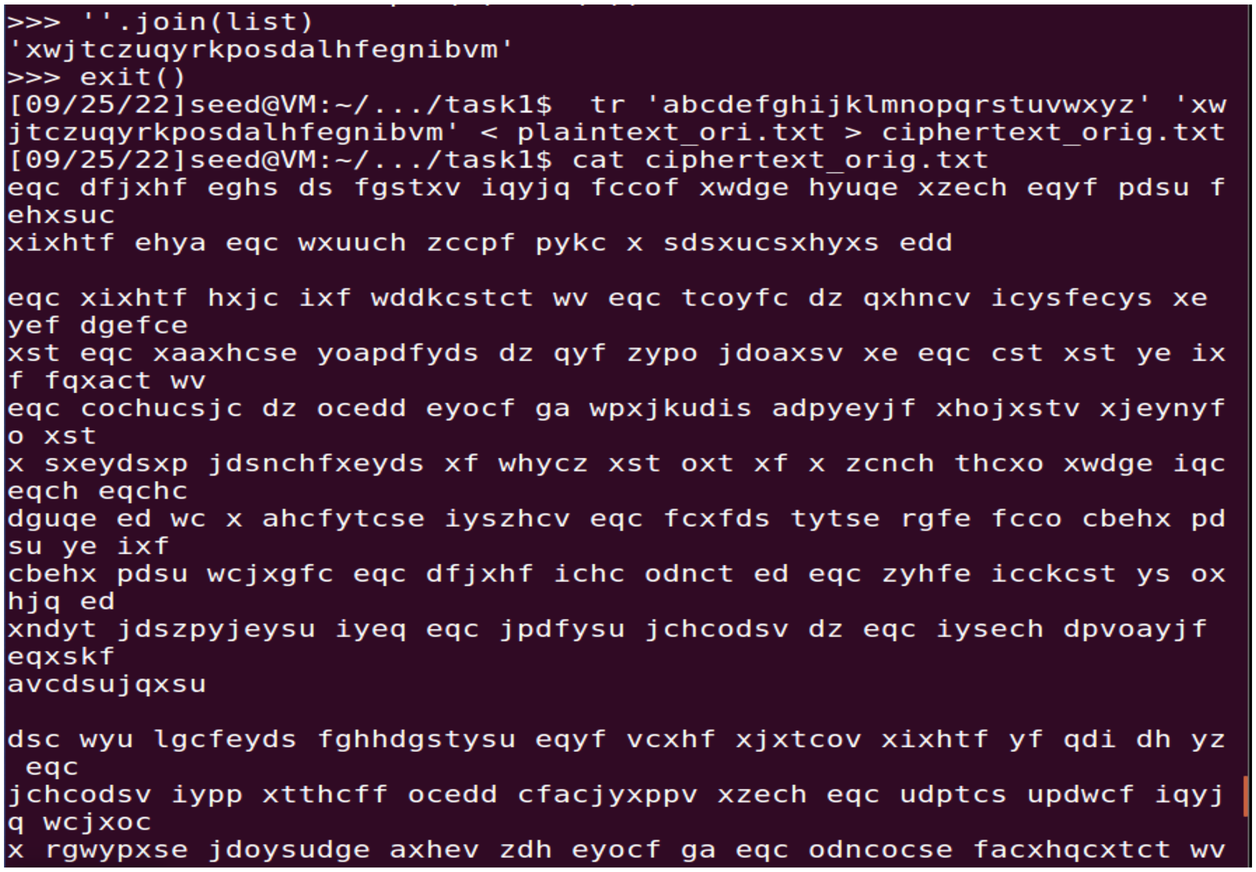
Step 1: Encrypting the file and simplification made to it.


```
[09/25/22]seed@VM:~/.../task1$ tr [:upper:] [:lower:] < Orig_articl
e.txt > lowercase_ori.txt
[09/25/22]seed@VM:~/.../task1$ cat lowercase_ori.txt
the oscars turn on sunday which seems about right after this long s
trange
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 wa
s shaped by
the emergence of metoo times up blackgown politics armcandy activis
m and
a national conversation as brief and mad as a fever dream about whe
ther there
ought to be a president winfrey the season didnt just seem extra lo
ng it was
extra long because the oscars were moved to the first weekend in ma
rch to
avoid conflicting with the closing ceremony of the winter olympics
thanks
```

```
[09/25/22]seed@VM:~/.../task1$ tr -cd '[a-z][\n][:space:]' < lowerc
ase_ori.txt > plaintext_ori.txt
[09/25/22]seed@VM:~/.../task1$ cat plaintext_ori.txt
the oscars turn on sunday which seems about right after this long s
trange
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 wa
s shaped by
the emergence of metoo times up blackgown politics armcandy activis
m and
a national conversation as brief and mad as a fever dream about whe
ther there
ought to be a president winfrey the season didnt just seem extra lo
ng it was
extra long because the oscars were moved to the first weekend in ma
rch to
avoid conflicting with the closing ceremony of the winter olympics
thanks
```
Step 2: Generating encryption key in Python



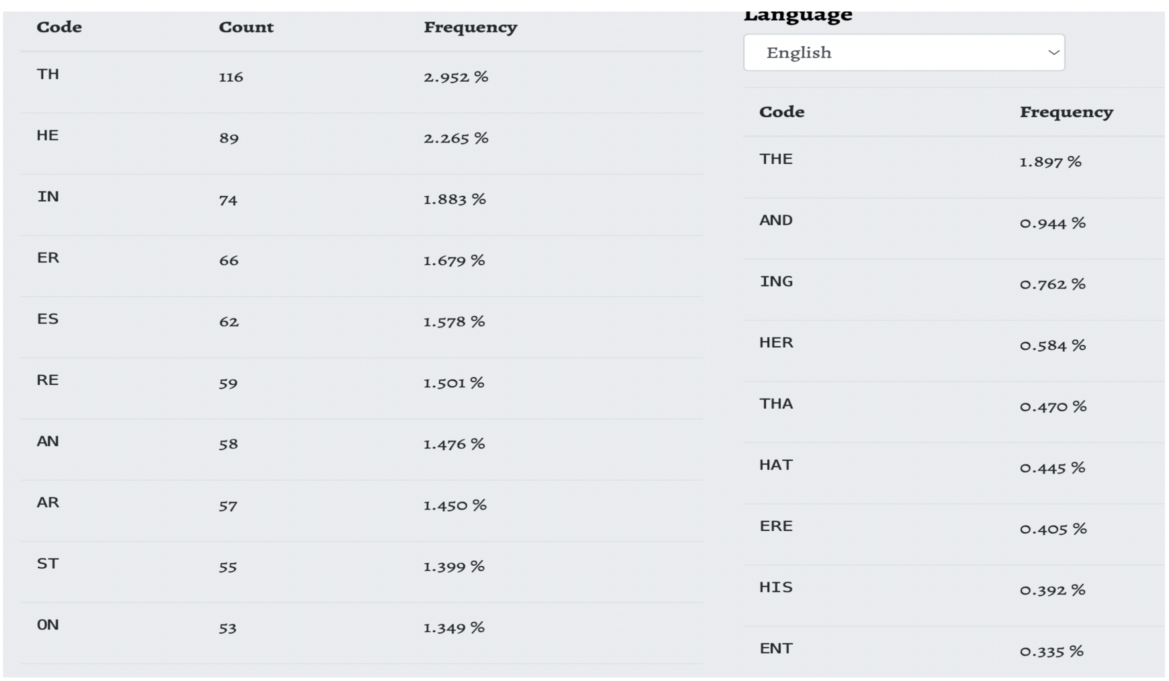
```
[09/25/22]seed@VM:~/.../task1$ python
Python 2.7.12 (default, Nov 19 2016, 06:48:10)
[GCC 5.4.0 20160609] on linux2
Type "help", "copyright", "credits" or "license" for more informati
on.
>>> import random
>>> s = "abcdefghijklmnopqrstuvwxyz"
>>> list = random.sample(s, len(s))
>>> ''.join(list)
'xwjtczuqyrkposdalhfegnibvm'
>>> 
```

Step 3: tr command to do the encryption of letters leaving the space and returning characters alone



```
>>> ''.join(list)
'xwjtczuqyrkposdalhfegnibvm'
>>> exit()
[09/25/22]seed@VM:~/.../task1$  tr 'abcdefghijklmnopqrstuvwxyz' 'xw
jtczuqyrkposdalhfegnibvm' < plaintext_ori.txt > ciphertext_orig.txt
[09/25/22]seed@VM:~/.../task1$ cat ciphertext_orig.txt
eqc dfjxhf eghs ds fgstxv iqyjq fccof xwdge hyuqe xzech eqyf pdsu f
ehxsuc
xixhtf ehya eqc wxuuch zccpf pykc x sdsxucsxhyxs edd

eqc xixhtf hxjc ixf wddkcstct wv eqc tcoyfc dz qxhncv icysfecys xe
yef dgefce
xst eqc xaaxhcse yoapdfyds dz qyf zypo jdoaxsv xe eqc cst xst ye ix
f fqxact wv
eqc cochucsjc dz ocedd eyocf ga wpxjkudis adpyeyjf xhojxstv xjeynyf
o xst
x sxeydsxp jdsnchfxeyds xf whycz xst oxt xf x zcnch thcxo xwdge iqc
eqch eqchc
dguqe ed wc x ahcfytcse iyszhcv eqc fcxfds tytse rgfe fcco cbehx pd
su ye ixf
cbehx pdsu wcjxgfc eqc dfjxhf ichc odnct ed eqc zyhfe icckcst ys ox
hjq ed
xndyt jdszpyjeysu iyeq eqc jpdfysu jchcodsv dz eqc iysech dpvoayjf
eqxskf
avcdsujqxsu

dsc wyu lgcfeyds fghhdgstysu eqyf vcxhf xjxtcov xixhtf yf qdi dh yz
 eqc
jchcodsv iypp xtthcff ocedd cfacjyxppv xzech eqc udptcs updwcf iqyj
q wcjxoc
x rgwypxse jdoysudge axhev zdh eyocf ga eqc odncocse facxhqcxtct wv
```

Frequency Text for original article: There were a lot of images of texts for frequency analysis but we added 2 screenshots.

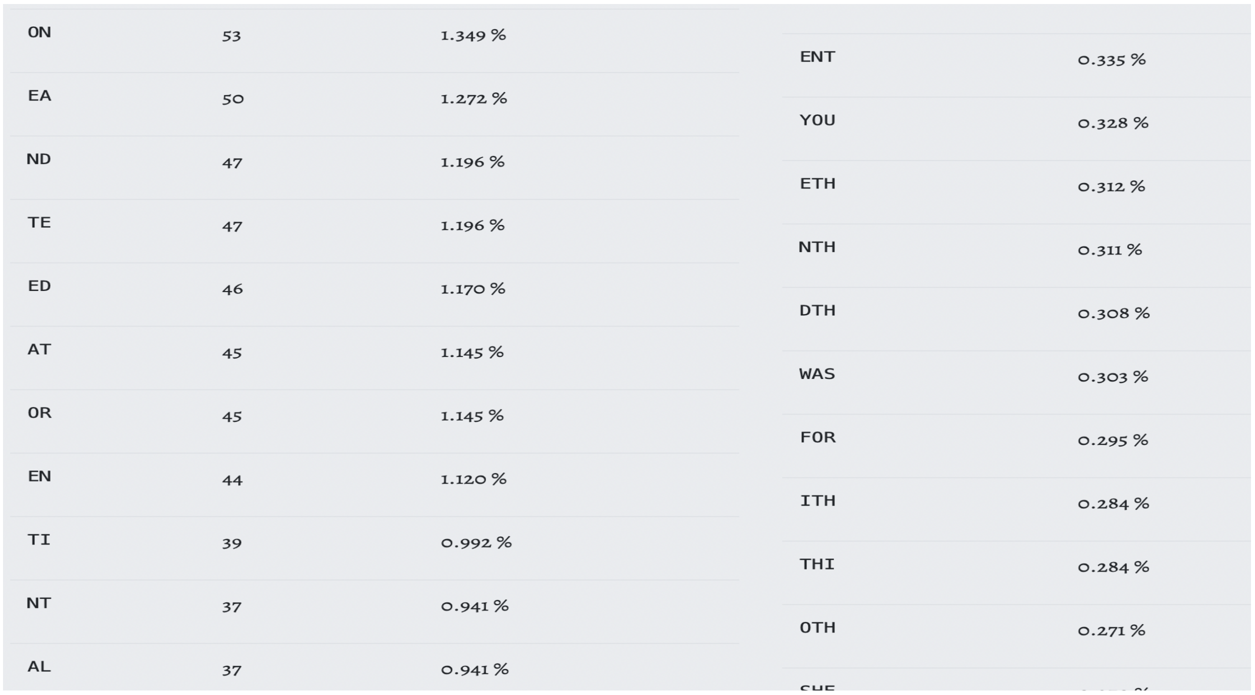


Code	Count	Frequency
TH	116	2.952 %
HE	89	2.265 %
IN	74	1.883 %
ER	66	1.679 %
ES	62	1.578 %
RE	59	1.501 %
AN	58	1.476 %
AR	57	1.450 %
ST	55	1.399 %
ON	53	1.349 %

Language

English

Code	Frequency
THE	1.897 %
AND	0.944 %
ING	0.762 %
HER	0.584 %
THA	0.470 %
HAT	0.445 %
ERE	0.405 %
HIS	0.392 %
ENT	0.335 %

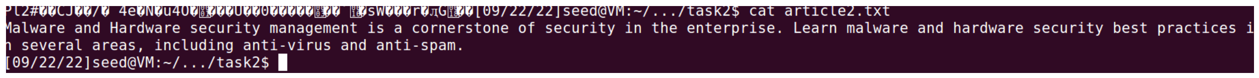


ON	53	1.349 %
EA	50	1.272 %
ND	47	1.196 %
TE	47	1.196 %
ED	46	1.170 %
AT	45	1.145 %
OR	45	1.145 %
EN	44	1.120 %
TI	39	0.992 %
NT	37	0.941 %
AL	37	0.941 %

ENT	0.335 %
YOU	0.328 %
ETH	0.312 %
NTH	0.311 %
DTH	0.308 %
WAS	0.303 %
FOR	0.295 %
ITH	0.284 %
THI	0.284 %
OTH	0.271 %

Task 2: Encryption using Different Ciphers and Modes

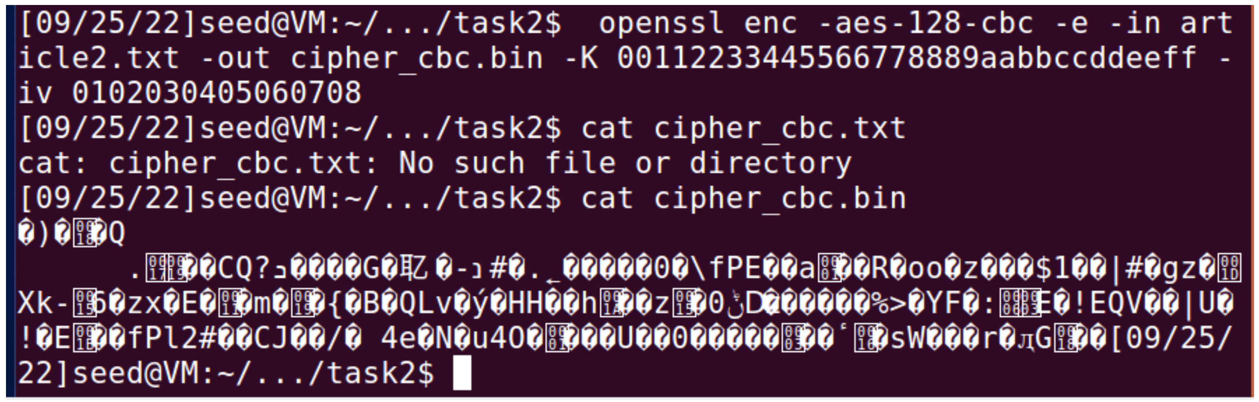
Name of the file with contents :



```
Pl2#��CJ��/� 4e�N�u4O����U��0�������� ��sW���r�лG���[09/22/22]seed@VM:~/.../task2$ cat article2.txt
Malware and Hardware security management is a cornerstone of security in the enterprise. Learn malware and hardware security best practices i
n several areas, including anti-virus and anti-spam.
[09/22/22]seed@VM:~/.../task2$
```

Command typed in for **aes-128-cbc:**

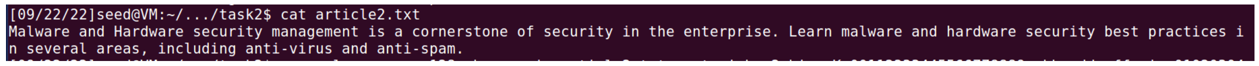
openssl enc -aes-128-cbc -e -in article2.txt -out cipher_cbc.bin -K 00112233445566778889aabbccddeeff -iv 0102030405060708



```
[09/25/22]seed@VM:~/.../task2$  openssl enc -aes-128-cbc -e -in art
icle2.txt -out cipher_cbc.bin -K 00112233445566778889aabbccddeeff -
iv 0102030405060708
[09/25/22]seed@VM:~/.../task2$ cat cipher_cbc.txt
cat: cipher_cbc.txt: No such file or directory
[09/25/22]seed@VM:~/.../task2$ cat cipher_cbc.bin
�)��Q
     .���CQ?ɹ����G�ⵎ�-ɹ#�._������0�\fPE��a��R�oo�z���$1��|#�gz��
Xk-��zx�E��m��{�B�QLv�ý�HH��h��z�0ْD������%>�YF�:��E�!EQV��|U�
!�E��fPl2#��CJ��/� 4e�N�u4O����U���������� ʿ�sW���r�лG���[09/25/
22]seed@VM:~/.../task2$
```

Based on -aes-128-ofb :

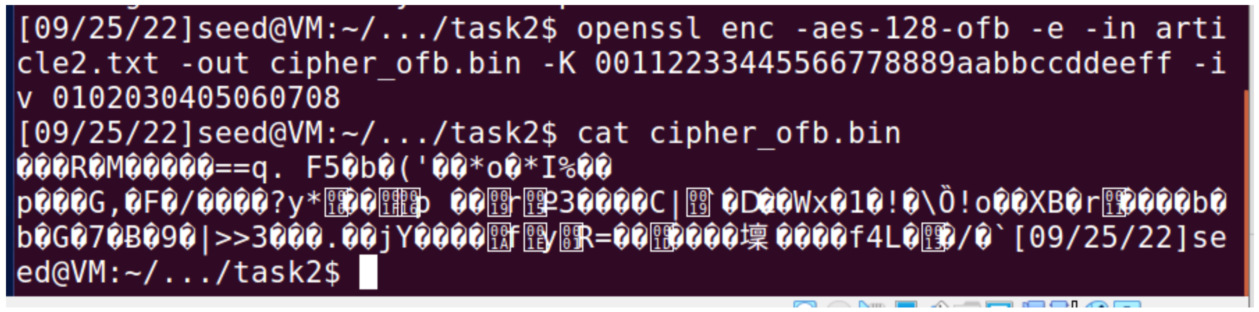
Name of the file with contents:



```
[09/22/22]seed@VM:~/.../task2$ cat article2.txt
Malware and Hardware security management is a cornerstone of security in the enterprise. Learn malware and hardware security best practices i
n several areas, including anti-virus and anti-spam.
```

Command typed in for -aes-128-ofb :

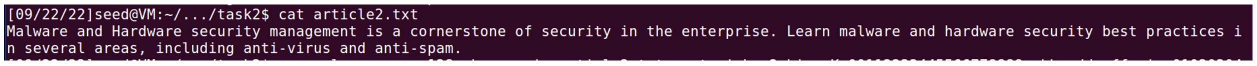
openssl enc -aes-128-ofb -e -in article2.txt -out cipher_ofb.bin -K 00112233445566778889aabbccddeeff -iv 0102030405060708



```
[09/25/22]seed@VM:~/.../task2$ openssl enc -aes-128-ofb -e -in arti
cle2.txt -out cipher_ofb.bin -K 00112233445566778889aabbccddeeff -i
v 0102030405060708
[09/25/22]seed@VM:~/.../task2$ cat cipher_ofb.bin
���R�M�����==q. F5�b�('��*o�*I%��
p���G,�F�/����?y*����b ���r�P3����C|� �D��Wx�1�!�\Ȍ!o��XB�r�����b�
b�G�7�B�9�|>>3���.��jY����f�y�R=�������壊����f4L���/�`[09/25/22]se
ed@VM:~/.../task2$
```

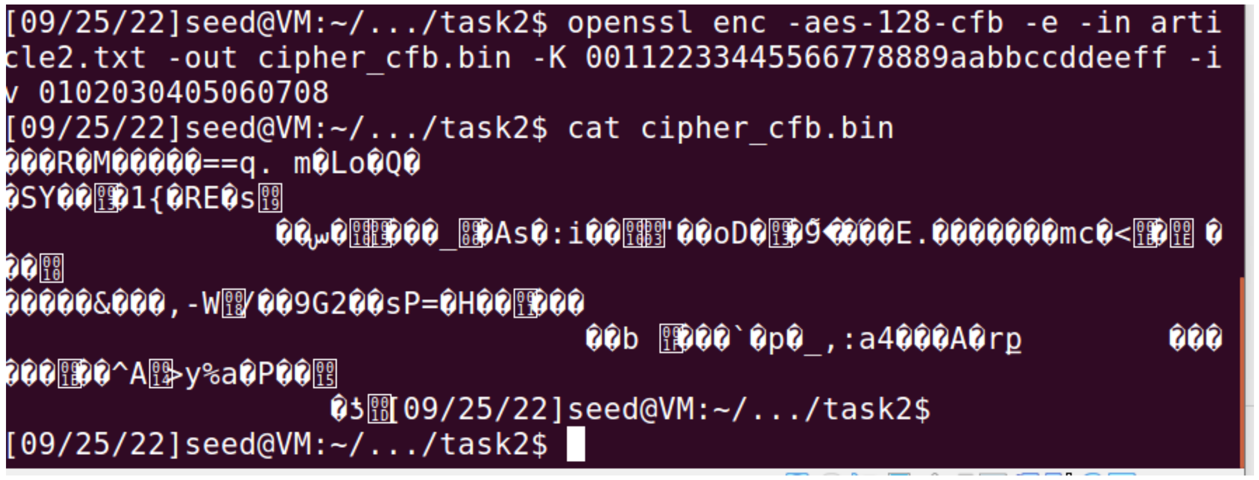
Based on -aes-128-cfb

Name of the file



```
[09/22/22]seed@VM:~/.../task2$ cat article2.txt
Malware and Hardware security management is a cornerstone of security in the enterprise. Learn malware and hardware security best practices i
n several areas, including anti-virus and anti-spam.
```

Command typed in:
openssl enc -aes-128-cfb -e -in article2.txt -out cipher_cfb.bin -K 00112233445566778899aabbccddeeff -iv 0102030405060708



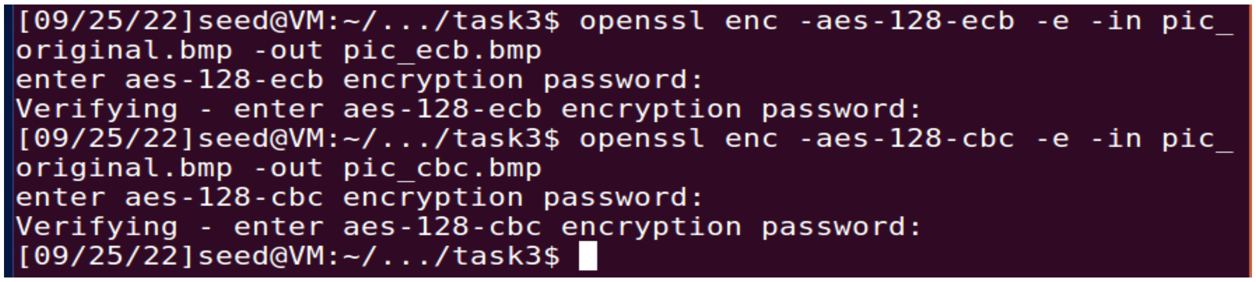
```
[09/25/22]seed@VM:~/.../task2$ openssl enc -aes-128-cfb -e -in arti
cle2.txt -out cipher_cfb.bin -K 00112233445566778899aabbccddeeff -i
v 0102030405060708
[09/25/22]seed@VM:~/.../task2$ cat cipher_cfb.bin
���R�M�����==q. m�Lo�Q�
�SY���1{�RE�s�
                ��ω�����_��As�:i����'��oD���ʛ����E.�������mc�<��� �
���
�����&���,-W�/��9G2��sP=�H�����
                                   ��b ����`�p�_,:a4���A�rp       ���
������^A�>y%a�P���
                    �ʢ�[09/25/22]seed@VM:~/.../task2$
[09/25/22]seed@VM:~/.../task2$ █
```

Task 3 : Encryption Mode – ECB vs. CBC

Changing original pic mode to ecb and cbc mode:

For encrypting original_pic .bmp file to ECB and CBC mode commands used:

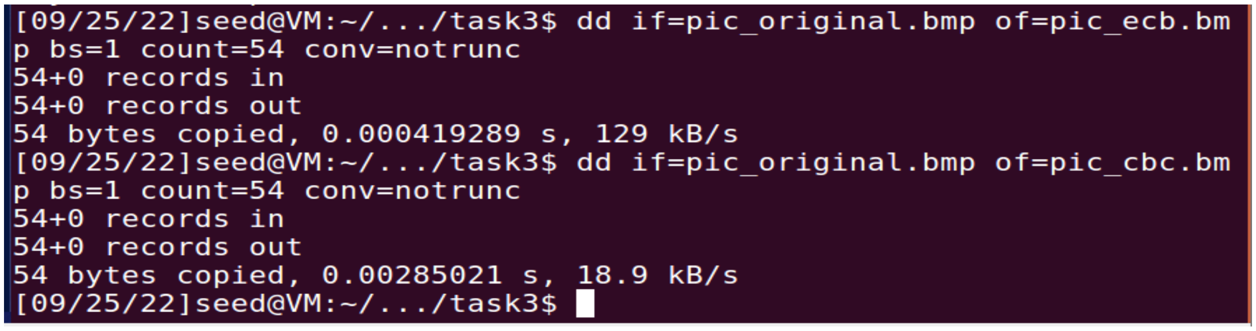
openssl enc -aes-128-ecb -e -in pic_original.bmp -out pic_ecb.bmp
openssl enc -aes-128-cbc -e -in pic_original.bmp -out pic_cbc.bmp



```
[09/25/22]seed@VM:~/.../task3$ openssl enc -aes-128-ecb -e -in pic_
original.bmp -out pic_ecb.bmp
enter aes-128-ecb encryption password:
Verifying - enter aes-128-ecb encryption password:
[09/25/22]seed@VM:~/.../task3$ openssl enc -aes-128-cbc -e -in pic_
original.bmp -out pic_cbc.bmp
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
[09/25/22]seed@VM:~/.../task3$ █
```

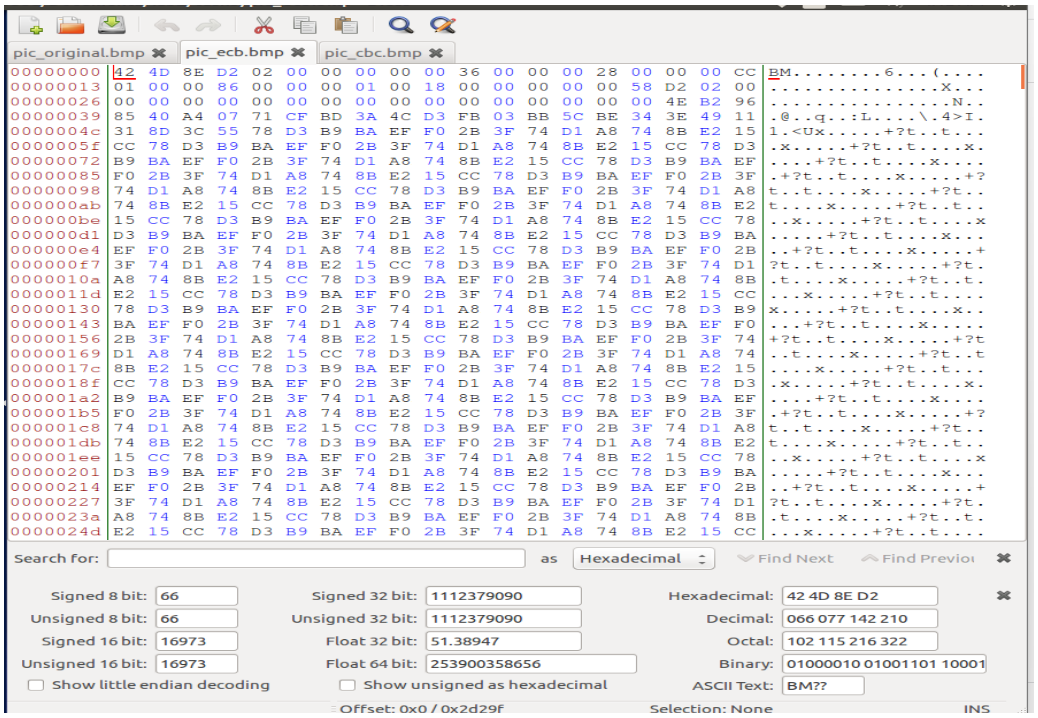
I have used dd if command to get 54 byte of pictures in both:

Commands used:
dd if=pic_original.bmp of=pic_ecb.bmp bs=1 count=54 conv=notrunc
dd if=pic_original.bmp of=pic_cbc.bmp bs=1 count=54 conv=notrunc



```
[09/25/22]seed@VM:~/.../task3$ dd if=pic_original.bmp of=pic_ecb.bm
p bs=1 count=54 conv=notrunc
54+0 records in
54+0 records out
54 bytes copied, 0.000419289 s, 129 kB/s
[09/25/22]seed@VM:~/.../task3$ dd if=pic_original.bmp of=pic_cbc.bm
p bs=1 count=54 conv=notrunc
54+0 records in
54+0 records out
54 bytes copied, 0.00285021 s, 18.9 kB/s
[09/25/22]seed@VM:~/.../task3$ 
```

Bless Hex Editor see:
For ECB:



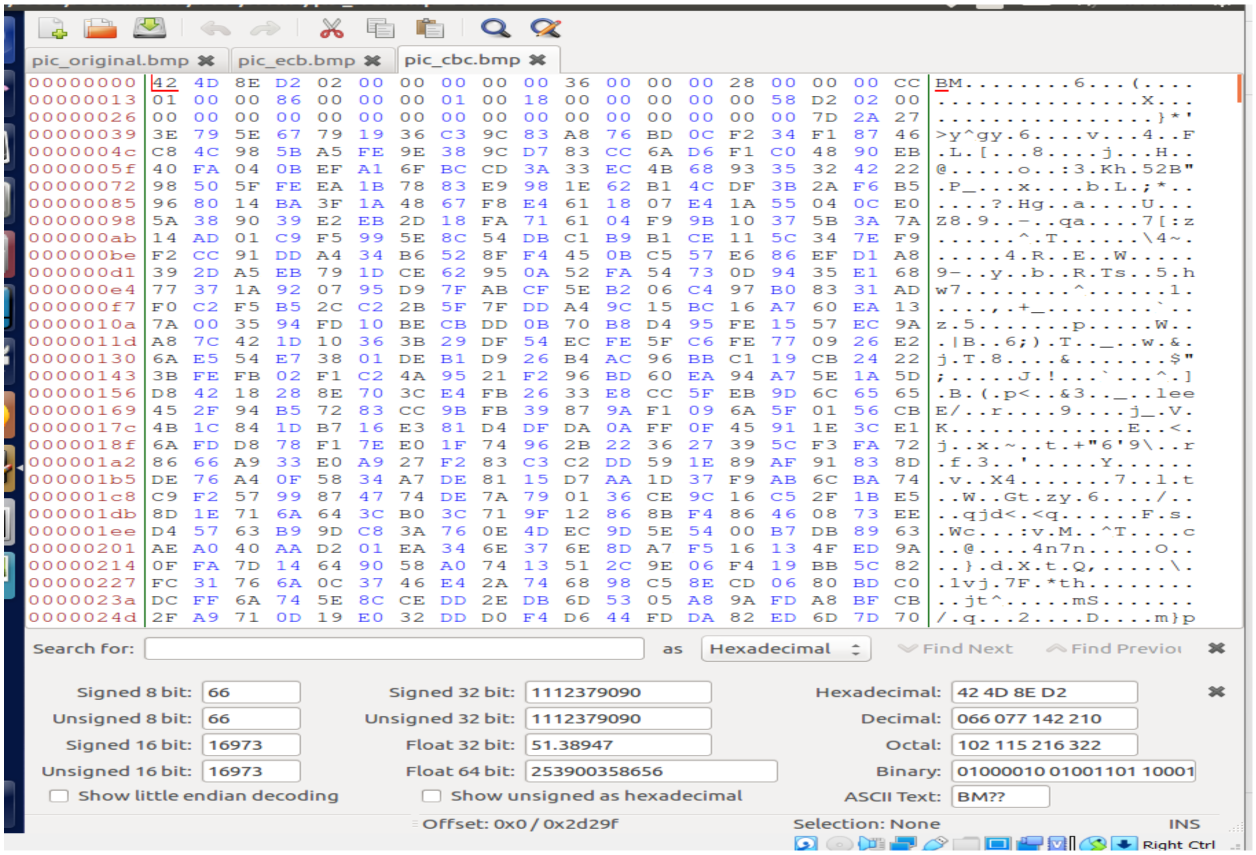
```
00000000 42 4D 8E D2 02 00 00 00 00 00 36 00 00 00 28 00 00 00 CC BM........6...(....
00000013 01 00 00 86 00 00 00 01 00 18 00 00 00 00 00 58 D2 02 00 ...............X...
00000026 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4E B2 96 ................N..
00000039 85 40 A4 07 71 CF BD 3A 4C D3 FB 03 BB 5C BE 34 3E 49 11 .@..q..:L....\.4>I.
0000004c 31 8D 3C 55 78 D3 B9 BA EF F0 2B 3F 74 D1 A8 74 8B E2 15 1.<Ux.....+?t..t...
0000005f CC 78 D3 B9 BA EF F0 2B 3F 74 D1 A8 74 8B E2 15 CC 78 D3 .x.....+?t..t....x.
00000072 B9 BA EF F0 2B 3F 74 D1 A8 74 8B E2 15 CC 78 D3 B9 BA EF ....+?t..t....x....
00000085 F0 2B 3F 74 D1 A8 74 8B E2 15 CC 78 D3 B9 BA EF F0 2B 3F .+?t..t....x.....+?
00000098 74 D1 A8 74 8B E2 15 CC 78 D3 B9 BA EF F0 2B 3F 74 D1 A8 t..t....x.....+?t..
000000ab 74 8B E2 15 CC 78 D3 B9 BA EF F0 2B 3F 74 D1 A8 74 8B E2 t....x.....+?t..t..
000000be 15 CC 78 D3 B9 BA EF F0 2B 3F 74 D1 A8 74 8B E2 15 CC 78 ..x.....+?t..t....x
000000d1 D3 B9 BA EF F0 2B 3F 74 D1 A8 74 8B E2 15 CC 78 D3 B9 BA .....+?t..t....x...
000000e4 EF F0 2B 3F 74 D1 A8 74 8B E2 15 CC 78 D3 B9 BA EF F0 2B ..+?t..t....x.....+
000000f7 3F 74 D1 A8 74 8B E2 15 CC 78 D3 B9 BA EF F0 2B 3F 74 D1 ?t..t....x.....+?t.
0000010a A8 74 8B E2 15 CC 78 D3 B9 BA EF F0 2B 3F 74 D1 A8 74 8B .t....x.....+?t..t.
0000011d E2 15 CC 78 D3 B9 BA EF F0 2B 3F 74 D1 A8 74 8B E2 15 CC ...x.....+?t..t....
00000130 78 D3 B9 BA EF F0 2B 3F 74 D1 A8 74 8B E2 15 CC 78 D3 B9 x.....+?t..t....x..
00000143 BA EF F0 2B 3F 74 D1 A8 74 8B E2 15 CC 78 D3 B9 BA EF F0 ...+?t..t....x.....
00000156 2B 3F 74 D1 A8 74 8B E2 15 CC 78 D3 B9 BA EF F0 2B 3F 74 +?t..t....x.....+?t
00000169 D1 A8 74 8B E2 15 CC 78 D3 B9 BA EF F0 2B 3F 74 D1 A8 74 ..t....x.....+?t..t
0000017c 8B E2 15 CC 78 D3 B9 BA EF F0 2B 3F 74 D1 A8 74 8B E2 15 ....x.....+?t..t...
0000018f CC 78 D3 B9 BA EF F0 2B 3F 74 D1 A8 74 8B E2 15 CC 78 D3 .x.....+?t..t....x.
000001a2 B9 BA EF F0 2B 3F 74 D1 A8 74 8B E2 15 CC 78 D3 B9 BA EF ....+?t..t....x....
000001b5 F0 2B 3F 74 D1 A8 74 8B E2 15 CC 78 D3 B9 BA EF F0 2B 3F .+?t..t....x.....+?
000001c8 74 D1 A8 74 8B E2 15 CC 78 D3 B9 BA EF F0 2B 3F 74 D1 A8 t..t....x.....+?t..
000001db 74 8B E2 15 CC 78 D3 B9 BA EF F0 2B 3F 74 D1 A8 74 8B E2 t....x.....+?t..t..
000001ee 15 CC 78 D3 B9 BA EF F0 2B 3F 74 D1 A8 74 8B E2 15 CC 78 ..x.....+?t..t....x
00000201 D3 B9 BA EF F0 2B 3F 74 D1 A8 74 8B E2 15 CC 78 D3 B9 BA .....+?t..t....x...
00000214 EF F0 2B 3F 74 D1 A8 74 8B E2 15 CC 78 D3 B9 BA EF F0 2B ..+?t..t....x.....+
00000227 3F 74 D1 A8 74 8B E2 15 CC 78 D3 B9 BA EF F0 2B 3F 74 D1 ?t..t....x.....+?t.
0000023a A8 74 8B E2 15 CC 78 D3 B9 BA EF F0 2B 3F 74 D1 A8 74 8B .t....x.....+?t..t.
0000024d E2 15 CC 78 D3 B9 BA EF F0 2B 3F 74 D1 A8 74 8B E2 15 CC ...x.....+?t..t....
```

Search for: as Hexadecimal

Signed 8 bit:	66	Signed 32 bit:	1112379090	Hexadecimal:	42 4D 8E D2
Unsigned 8 bit:	66	Unsigned 32 bit:	1112379090	Decimal:	066 077 142 210
Signed 16 bit:	16973	Float 32 bit:	51.38947	Octal:	102 115 216 322
Unsigned 16 bit:	16973	Float 64 bit:	253900358656	Binary:	01000010 01001101 10001
☐ Show little endian decoding		☐ Show unsigned as hexadecimal		ASCII Text:	BM??

Offset: 0x0 / 0x2d29f   Selection: None   INS

For CBC:



pic_original.bmp pic_ecb.bmp pic_cbc.bmp

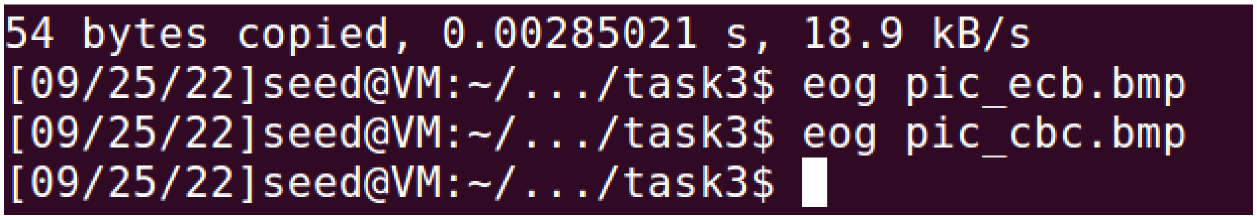
```
00000000 42 4D 8E D2 02 00 00 00 00 00 36 00 00 00 28 00 00 00 CC BM.........6...(....
00000013 01 00 00 86 00 00 00 01 00 18 00 00 00 00 00 58 D2 02 00 ...............X...
00000026 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7D 2A 27 ................}*'
00000039 3E 79 5E 67 79 19 36 C3 9C 83 A8 76 BD 0C F2 34 F1 87 46 >y^gy.6....v...4..F
0000004c C8 4C 98 5B A5 FE 9E 38 9C D7 83 CC 6A D6 F1 C0 48 90 EB .L.[...8....j...H..
0000005f 40 FA 04 0B EF A1 6F BC CD 3A 33 EC 4B 68 93 35 32 42 22 @.....o..:3.Kh.52B"
00000072 98 50 5F FE EA 1B 78 83 E9 98 1E 62 B1 4C DF 3B 2A F6 B5 .P_...x....b.L.;*..
00000085 96 80 14 BA 3F 1A 48 67 F8 E4 61 18 07 E4 1A 55 04 0C E0 ....?.Hg..a....U...
00000098 5A 38 90 39 E2 EB 2D 18 FA 71 61 04 F9 9B 10 37 5B 3A 7A Z8.9..-..qa....7[:z
000000ab 14 AD 01 C9 F5 99 5E 8C 54 DB C1 B9 B1 CE 11 5C 34 7E F9 ......^.T......\4~.
000000be F2 CC 91 DD A4 34 B6 52 8F F4 45 0B C5 57 E6 86 EF D1 A8 .....4.R..E..W.....
000000d1 39 2D A5 EB 79 1D CE 62 95 0A 52 FA 54 73 0D 94 35 E1 68 9-..y..b..R.Ts..5.h
000000e4 77 37 1A 92 07 95 D9 7F AB CF 5E B2 06 C4 97 B0 83 31 AD w7........^......1.
000000f7 F0 C2 F5 B5 2C C2 2B 5F 7F DD A4 9C 15 BC 16 A7 60 EA 13 ....,.+_..........`..
0000010a 7A 00 35 94 FD 10 BE CB DD 0B 70 B8 D4 95 FE 15 57 EC 9A z.5.......p.....W..
0000011d A8 7C 42 1D 10 36 3B 29 DF 54 EC FE 5F C6 FE 77 09 26 E2 .|B..6;).T.._..w.&.
00000130 6A E5 54 E7 38 01 DE B1 D9 26 B4 AC 96 BB C1 19 CB 24 22 j.T.8....&.......$"
00000143 3B FE FB 02 F1 C2 4A 95 21 F2 96 BD 60 EA 94 A7 5E 1A 5D ;.....J.!...`...^.]
00000156 D8 42 18 28 8E 70 3C E4 FB 26 33 E8 CC 5F EB 9D 6C 65 65 .B.(.p<..&3.._..lee
00000169 45 2F 94 B5 72 83 CC 9B FB 39 87 9A F1 09 6A 5F 01 56 CB E/..r....9....j_.V.
0000017c 4B 1C 84 1D B7 16 E3 81 D4 DF DA 0A FF 0F 45 91 1E 3C E1 K..............E..<.
0000018f 6A FD D8 78 F1 7E E0 1F 74 96 2B 22 36 27 39 5C F3 FA 72 j..x.~..t.+"6'9\..r
000001a2 86 66 A9 33 E0 A9 27 F2 83 C3 C2 DD 59 1E 89 AF 91 83 8D .f.3..'.....Y......
000001b5 DE 76 A4 0F 58 34 A7 DE 81 15 D7 AA 1D 37 F9 AB 6C BA 74 .v..X4.......7..l.t
000001c8 C9 F2 57 99 87 47 74 DE 7A 79 01 36 CE 9C 16 C5 2F 1B E5 ..W..Gt.zy.6..../..
000001db 8D 1E 71 6A 64 3C B0 3C 71 9F 12 86 8B F4 86 46 08 73 EE ..qjd<.<q......F.s.
000001ee D4 57 63 B9 9D C8 3A 76 0E 4D EC 9D 5E 54 00 B7 DB 89 63 .Wc...:v.M..^T....c
00000201 AE A0 40 AA D2 01 EA 34 6E 37 6E 8D A7 F5 16 13 4F ED 9A ..@....4n7n.....O..
00000214 0F FA 7D 14 64 90 58 A0 74 13 51 2C 9E 06 F4 19 BB 5C 82 ..}.d.X.t.Q,.....\.
00000227 FC 31 76 6A 0C 37 46 E4 2A 74 68 98 C5 8E CD 06 80 BD C0 .1vj.7F.*th........
0000023a DC FF 6A 74 5E 8C CE DD 2E DB 6D 53 05 A8 9A FD A8 BF CB ..jt^.....mS.......
0000024d 2F A9 71 0D 19 E0 32 DD D0 F4 D6 44 FD DA 82 ED 6D 7D 70 /.q...2....D....m}p
```

Search for: as Hexadecimal

Signed 8 bit:	66	Signed 32 bit:	1112379090	Hexadecimal:	42 4D 8E D2
Unsigned 8 bit:	66	Unsigned 32 bit:	1112379090	Decimal:	066 077 142 210
Signed 16 bit:	16973	Float 32 bit:	51.38947	Octal:	102 115 216 322
Unsigned 16 bit:	16973	Float 64 bit:	253900358656	Binary:	01000010 01001101 10001
☐ Show little endian decoding		☐ Show unsigned as hexadecimal		ASCII Text:	BM??

Offset: 0x0 / 0x2d29f Selection: None INS

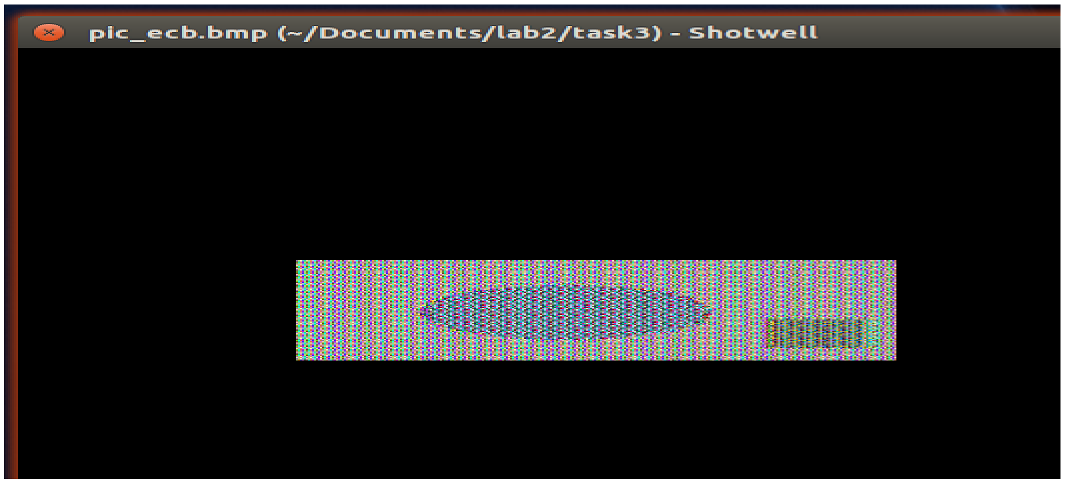
To see picture(here we called image viewer program called eog):



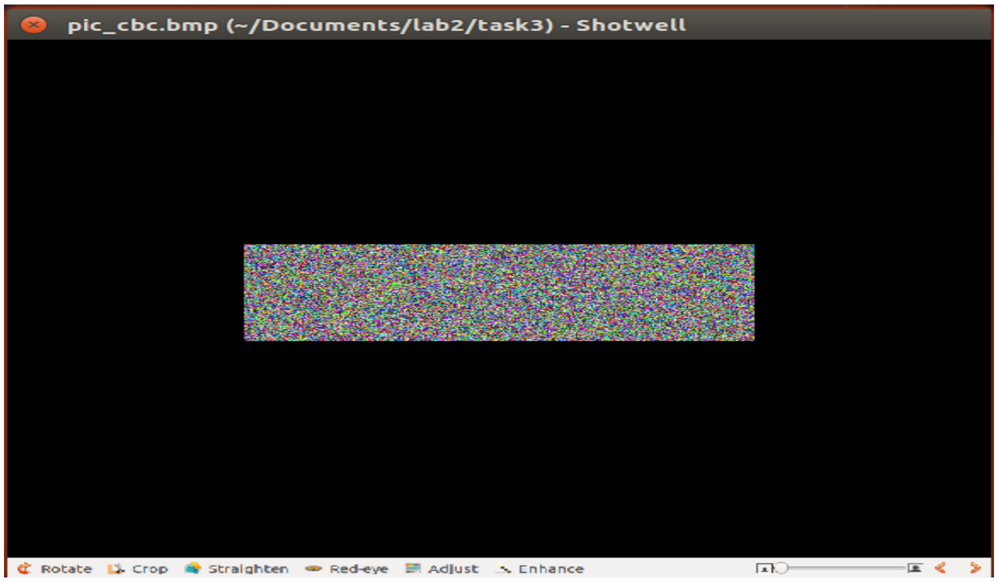
```
54 bytes copied, 0.00285021 s, 18.9 kB/s
[09/25/22]seed@VM:~/.../task3$ eog pic_ecb.bmp
[09/25/22]seed@VM:~/.../task3$ eog pic_cbc.bmp
[09/25/22]seed@VM:~/.../task3$ 
```

Final images:

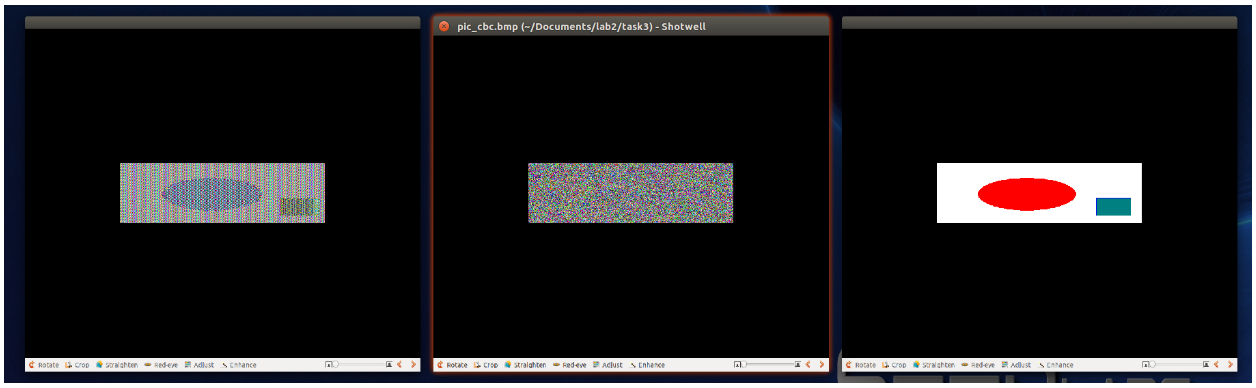
From ECB:



From CBC:



Comparison of all three images:

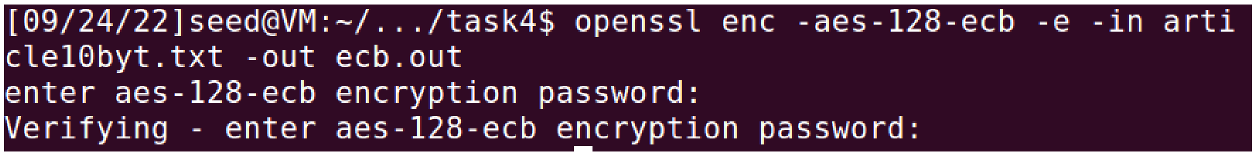


We here conclude that CBC to be used for encrypting data that might be in public and not use ECB encryption as we can see that we can see the image.

Task 4 : Padding

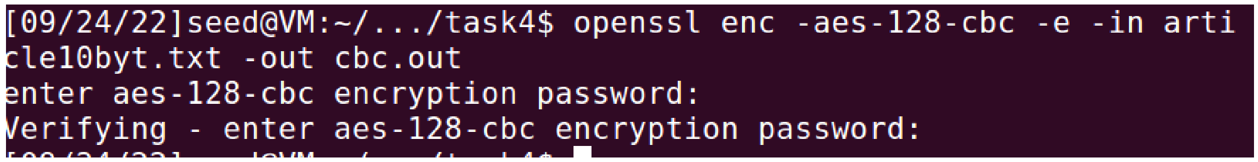
Use of AES ECB, CBC, CFB and OFB encryption

AES ECB encryption



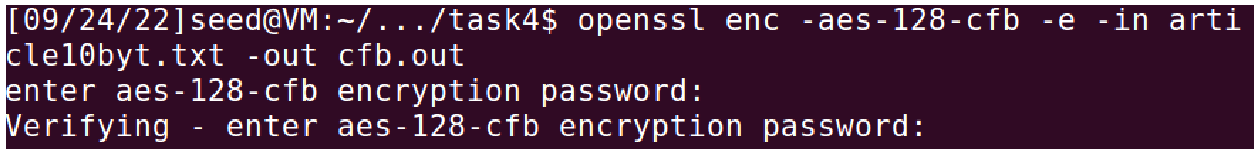
```
[09/24/22]seed@VM:~/.../task4$ openssl enc -aes-128-ecb -e -in arti
cle10byt.txt -out ecb.out
enter aes-128-ecb encryption password:
Verifying - enter aes-128-ecb encryption password:
```

CBC encryption



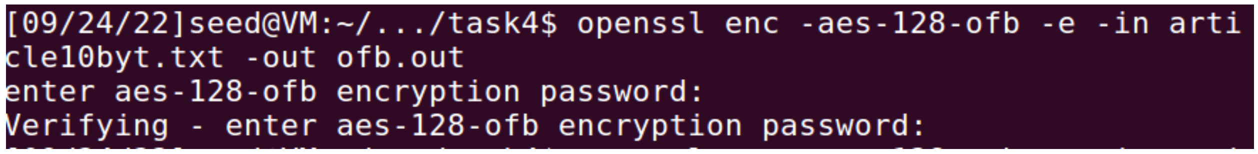
```
[09/24/22]seed@VM:~/.../task4$ openssl enc -aes-128-cbc -e -in arti
cle10byt.txt -out cbc.out
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
```

CFB encryption



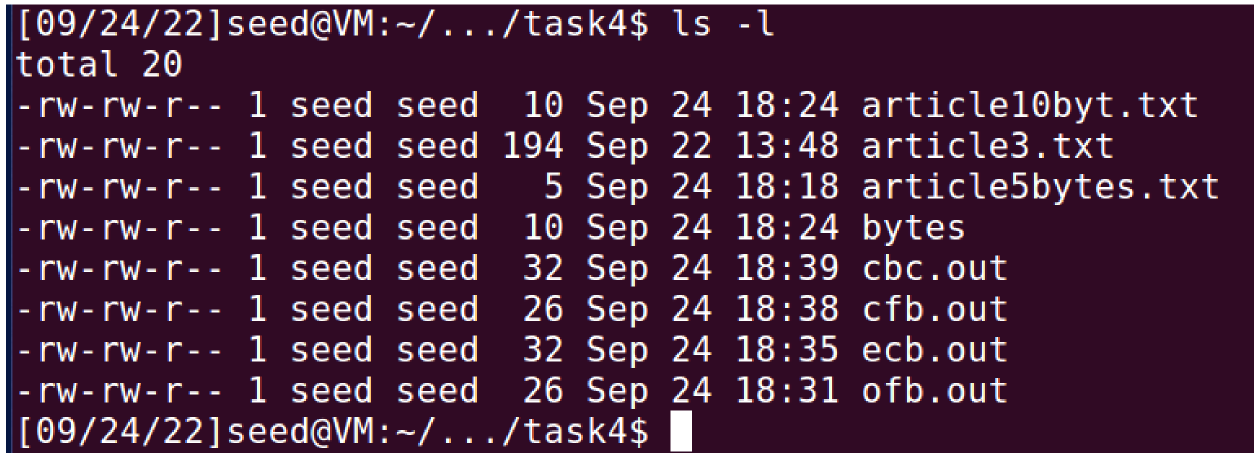
```
[09/24/22]seed@VM:~/.../task4$ openssl enc -aes-128-cfb -e -in arti
cle10byt.txt -out cfb.out
enter aes-128-cfb encryption password:
Verifying - enter aes-128-cfb encryption password:
```

OFB encryption

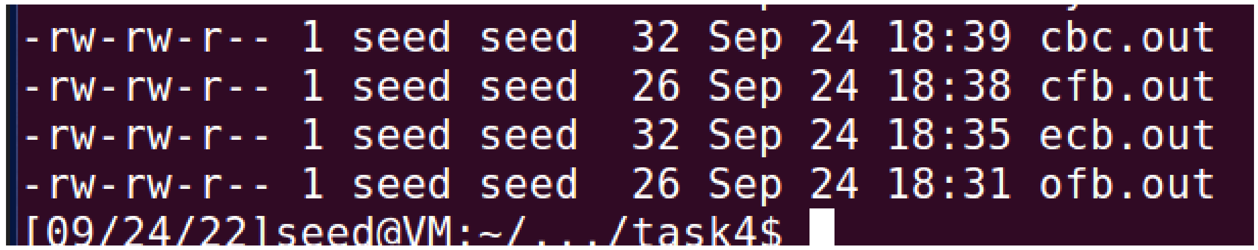


```
[09/24/22]seed@VM:~/.../task4$ openssl enc -aes-128-ofb -e -in arti
cle10byt.txt -out ofb.out
enter aes-128-ofb encryption password:
Verifying - enter aes-128-ofb encryption password:
```

Comparison of all four modes:



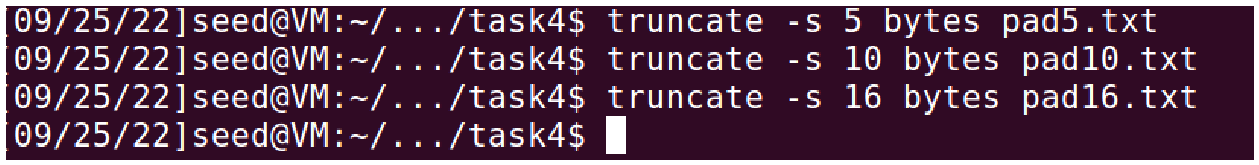
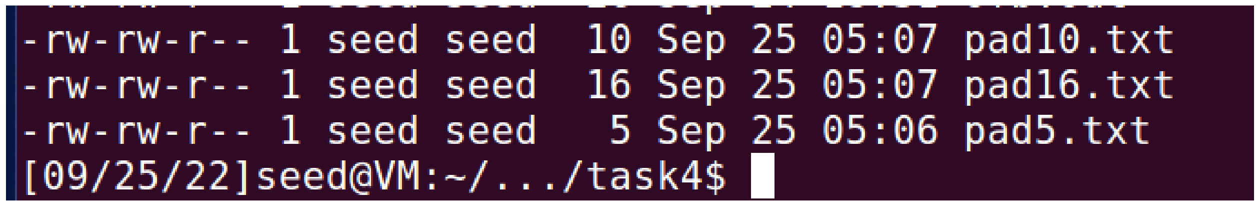
```
[09/24/22]seed@VM:~/.../task4$ ls -l
total 20
-rw-rw-r-- 1 seed seed  10 Sep 24 18:24 article10byt.txt
-rw-rw-r-- 1 seed seed 194 Sep 22 13:48 article3.txt
-rw-rw-r-- 1 seed seed   5 Sep 24 18:18 article5bytes.txt
-rw-rw-r-- 1 seed seed  10 Sep 24 18:24 bytes
-rw-rw-r-- 1 seed seed  32 Sep 24 18:39 cbc.out
-rw-rw-r-- 1 seed seed  26 Sep 24 18:38 cfb.out
-rw-rw-r-- 1 seed seed  32 Sep 24 18:35 ecb.out
-rw-rw-r-- 1 seed seed  26 Sep 24 18:31 ofb.out
[09/24/22]seed@VM:~/.../task4$
```



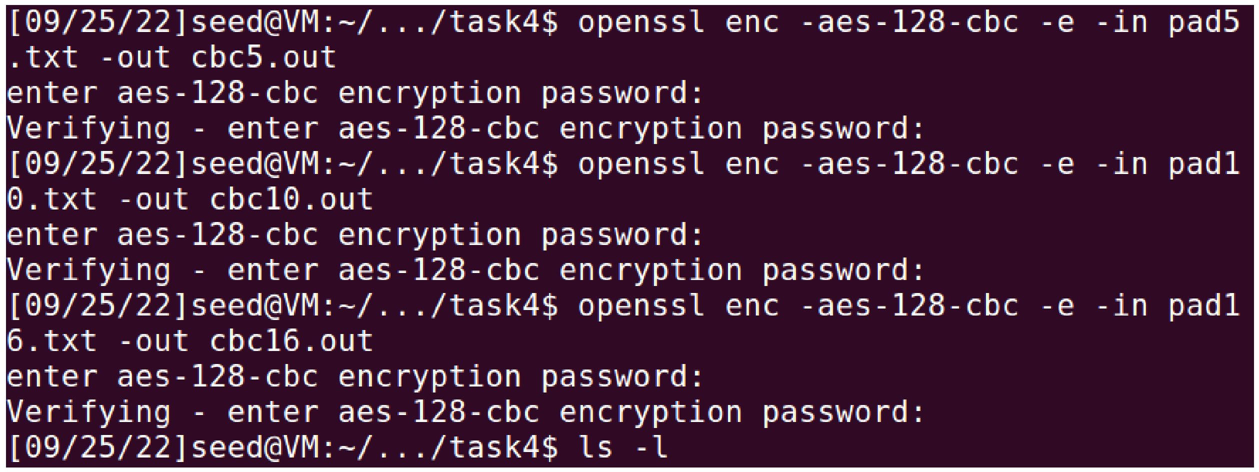
```
-rw-rw-r-- 1 seed seed  32 Sep 24 18:39 cbc.out
-rw-rw-r-- 1 seed seed  26 Sep 24 18:38 cfb.out
-rw-rw-r-- 1 seed seed  32 Sep 24 18:35 ecb.out
-rw-rw-r-- 1 seed seed  26 Sep 24 18:31 ofb.out
[09/24/22]seed@VM:~/.../task4$
```

We see CBC and ECB mode needing padding because they are block ciphers.
CFB and OFB do not need padding because these are stream ciphers. As OFB turns a block cipher into a synchronous stream cipher. As with CFB, the encryption and decryption processes are identical therefore no padding is required.

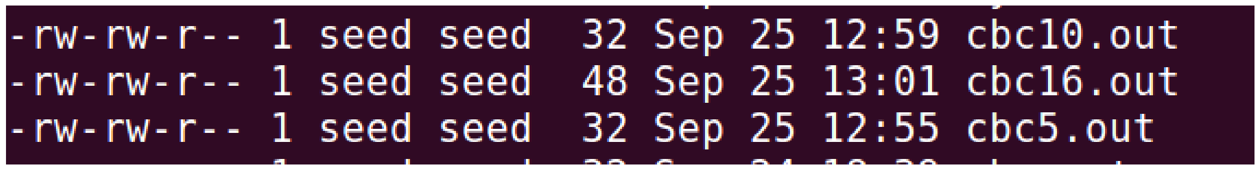
Different sizes of files :


```
[09/25/22]seed@VM:~/.../task4$ truncate -s 5 bytes pad5.txt
[09/25/22]seed@VM:~/.../task4$ truncate -s 10 bytes pad10.txt
[09/25/22]seed@VM:~/.../task4$ truncate -s 16 bytes pad16.txt
[09/25/22]seed@VM:~/.../task4$
```

```
-rw-rw-r-- 1 seed seed  10 Sep 25 05:07 pad10.txt
-rw-rw-r-- 1 seed seed  16 Sep 25 05:07 pad16.txt
-rw-rw-r-- 1 seed seed   5 Sep 25 05:06 pad5.txt
[09/25/22]seed@VM:~/.../task4$
```

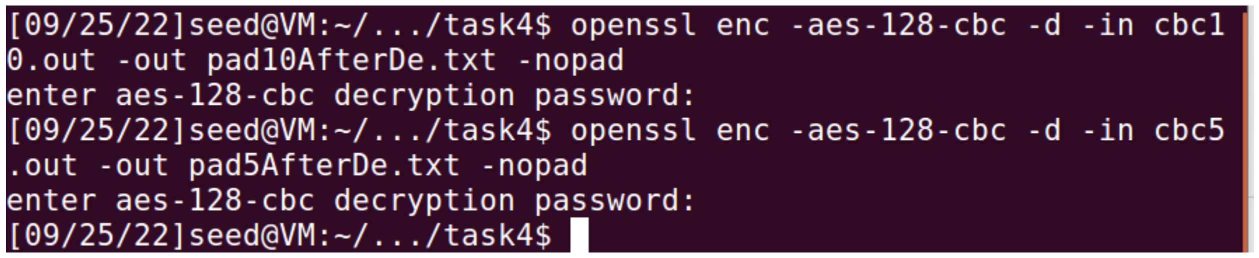
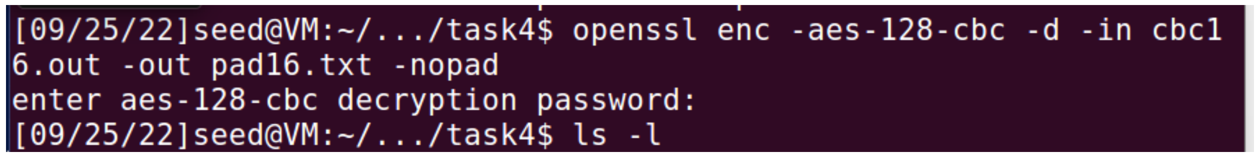
Encryption of 5, 10,16 bytes with CBC modes:


```
[09/25/22]seed@VM:~/.../task4$ openssl enc -aes-128-cbc -e -in pad5
.txt -out cbc5.out
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
[09/25/22]seed@VM:~/.../task4$ openssl enc -aes-128-cbc -e -in pad1
0.txt -out cbc10.out
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
[09/25/22]seed@VM:~/.../task4$ openssl enc -aes-128-cbc -e -in pad1
6.txt -out cbc16.out
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
[09/25/22]seed@VM:~/.../task4$ ls -l
```

After encryption with cbc to all files to see size of padding added:

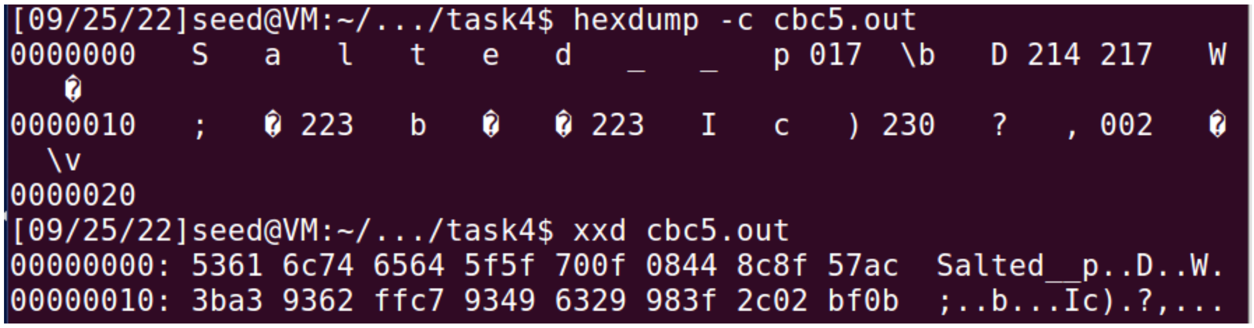

```
-rw-rw-r-- 1 seed seed  32 Sep 25 12:59 cbc10.out
-rw-rw-r-- 1 seed seed  48 Sep 25 13:01 cbc16.out
-rw-rw-r-- 1 seed seed  32 Sep 25 12:55 cbc5.out
```

Decryption without losing padding added to it:


```
[09/25/22]seed@VM:~/.../task4$ openssl enc -aes-128-cbc -d -in cbc1
0.out -out pad10AfterDe.txt -nopad
enter aes-128-cbc decryption password:
[09/25/22]seed@VM:~/.../task4$ openssl enc -aes-128-cbc -d -in cbc5
.out -out pad5AfterDe.txt -nopad
enter aes-128-cbc decryption password:
[09/25/22]seed@VM:~/.../task4$
```

```
[09/25/22]seed@VM:~/.../task4$ openssl enc -aes-128-cbc -d -in cbc1
6.out -out pad16.txt -nopad
enter aes-128-cbc decryption password:
[09/25/22]seed@VM:~/.../task4$ ls -l
```

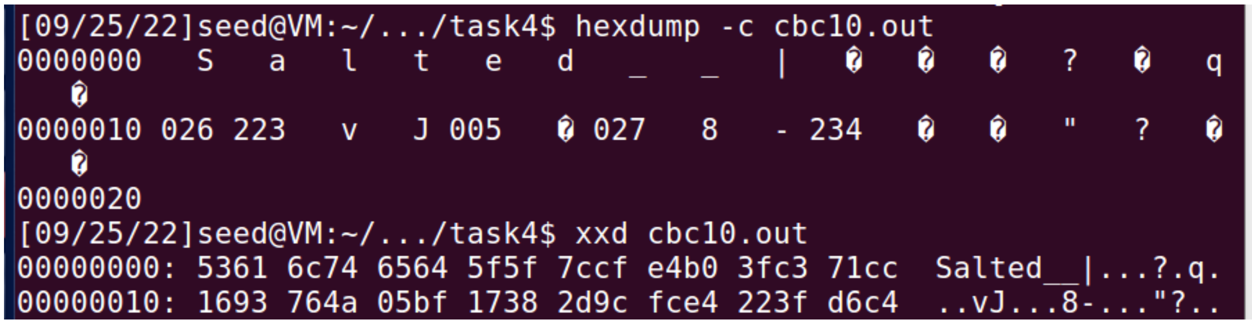
Padding to see:

For 5 bytes file



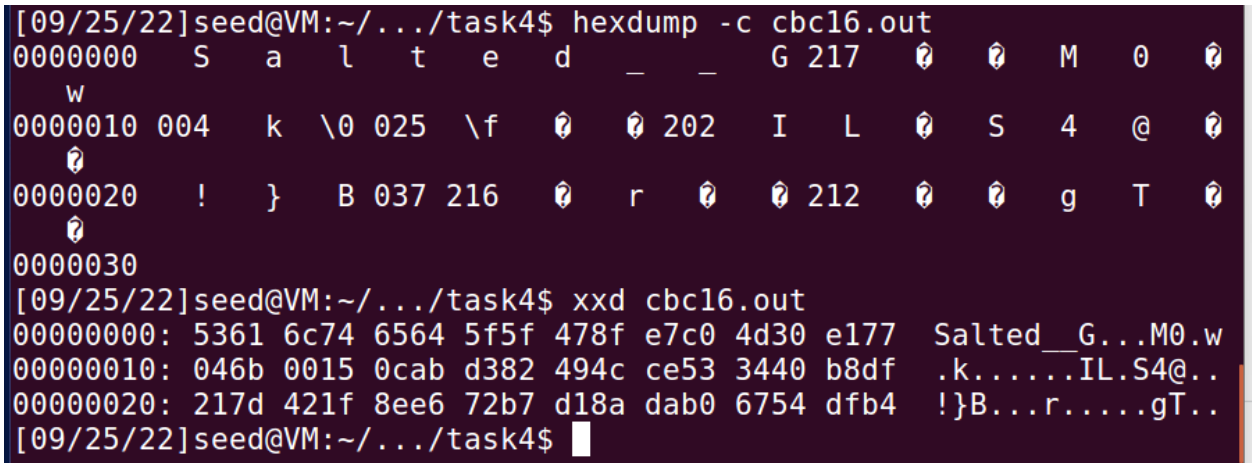
```
[09/25/22]seed@VM:~/.../task4$ hexdump -c cbc5.out
0000000   S   a   l   t   e   d   _   _   p 017  \b   D 214 217   W
   �
0000010   ;   � 223   b   �   � 223   I   c   ) 230   ?   , 002   �
  \v
0000020
[09/25/22]seed@VM:~/.../task4$ xxd cbc5.out
00000000: 5361 6c74 6564 5f5f 700f 0844 8c8f 57ac  Salted__p..D..W.
00000010: 3ba3 9362 ffc7 9349 6329 983f 2c02 bf0b  ;..b...Ic).?,...
```

For 10 bytes file



```
[09/25/22]seed@VM:~/.../task4$ hexdump -c cbc10.out
0000000   S   a   l   t   e   d   _   _   |   �   �   �   ?   �   q
   �
0000010 026 223   v   J 005   � 027   8   - 234   �   �   "   ?   �
   �
0000020
[09/25/22]seed@VM:~/.../task4$ xxd cbc10.out
00000000: 5361 6c74 6564 5f5f 7ccf e4b0 3fc3 71cc  Salted__|...?.q.
00000010: 1693 764a 05bf 1738 2d9c fce4 223f d6c4  ..vJ...8-..."?..
```

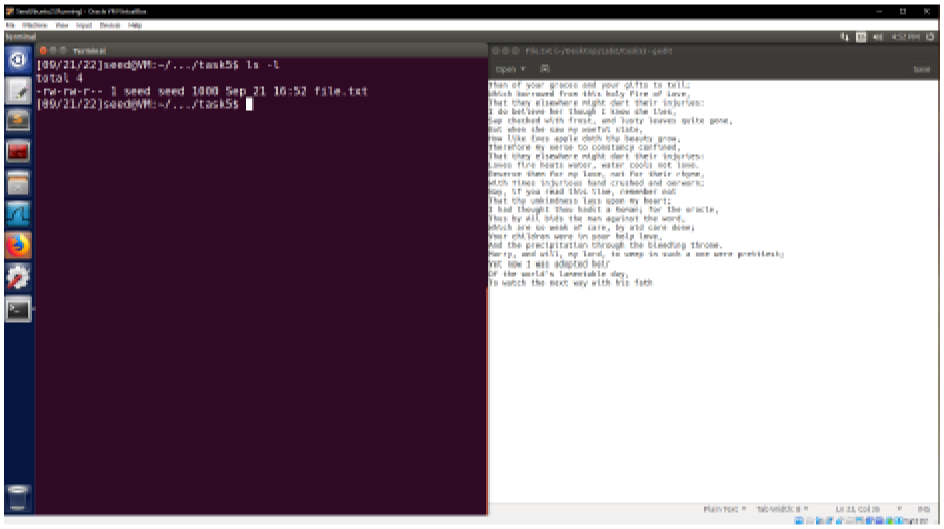
For 16 bytes file



```
[09/25/22]seed@VM:~/.../task4$ hexdump -c cbc16.out
0000000   S   a   l   t   e   d   _   _   G 217   �   �   M   0   �
   w
0000010 004   k  \0 025  \f   �   � 202   I   L   �   S   4   @   �
   �
0000020   !   }   B 037 216   �   r   �   � 212   �   �   g   T   �
   �
0000030
[09/25/22]seed@VM:~/.../task4$ xxd cbc16.out
00000000: 5361 6c74 6564 5f5f 478f e7c0 4d30 e177  Salted__G...M0.w
00000010: 046b 0015 0cab d382 494c ce53 3440 b8df  .k......IL.S4@..
00000020: 217d 421f 8ee6 72b7 d18a dab0 6754 dfb4  !}B...r.....gT..
[09/25/22]seed@VM:~/.../task4$
```

Task 5 : Error Propagation– Corrupted Cipher Text

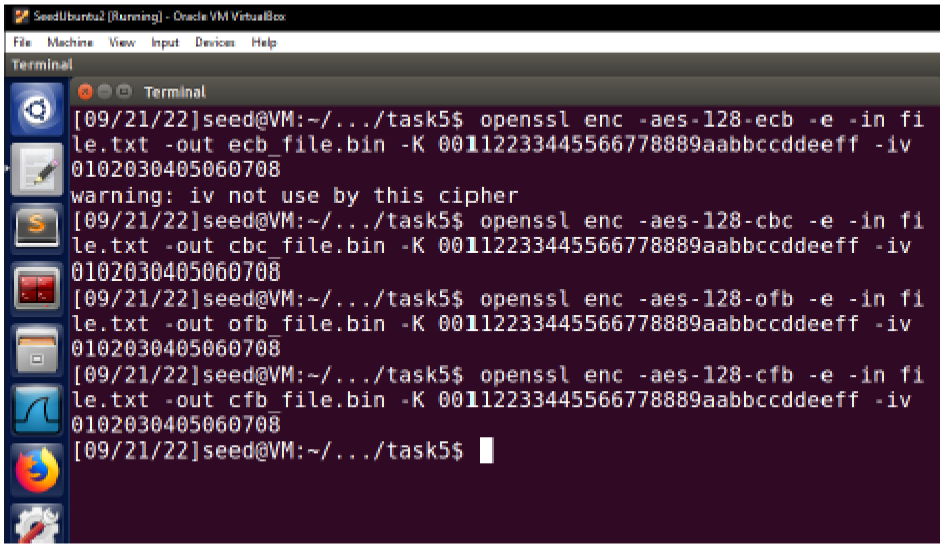
Creating a text file with 1000 bytes. I just copied it from the web.



```
[09/21/22]seed@VM:~/.../task5$ ls -l
total 4
-rw-rw-r-- 1 seed seed 1000 Sep 21 16:52 file.txt
[09/21/22]seed@VM:~/.../task5$
```

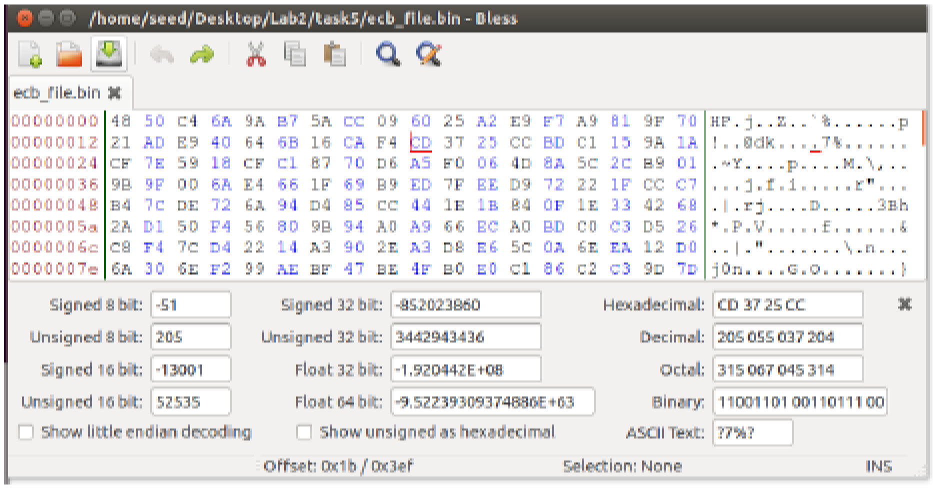
```
Then of your graces and your gifts to tell;
Which borrowed from this holy fire of Love,
That they elsewhere might dart their injuries:
I do believe her though I know she lies,
Sap checked with frost, and lusty leaves quite gone,
But when she saw my woeful state,
How like Eves apple doth thy beauty grow,
Therefore my verse to constancy confined,
That they elsewhere might dart their injuries:
Loves fire heats water, water cools not love.
Reserve them for my love, not for their rhyme,
With times injurious hand crushed and oerworn;
Nay, if you read this line, remember not
That thy unkindness lays upon my heart;
I had thought thou hadst a Roman; for the oracle,
Thus by all bids the man against the word,
Which are so weak of care, by old care done;
Your children were in your holy love,
And the precipitation through the bleeding throne.
Marry, and will, my lord, to weep in such a one were prettiest;
Yet now I was adopted heir
Of the world's lamentable day,
To watch the next way with his faith
```

Encrypting file with 4 types that is ecb,cbc,ofb,cfb modes

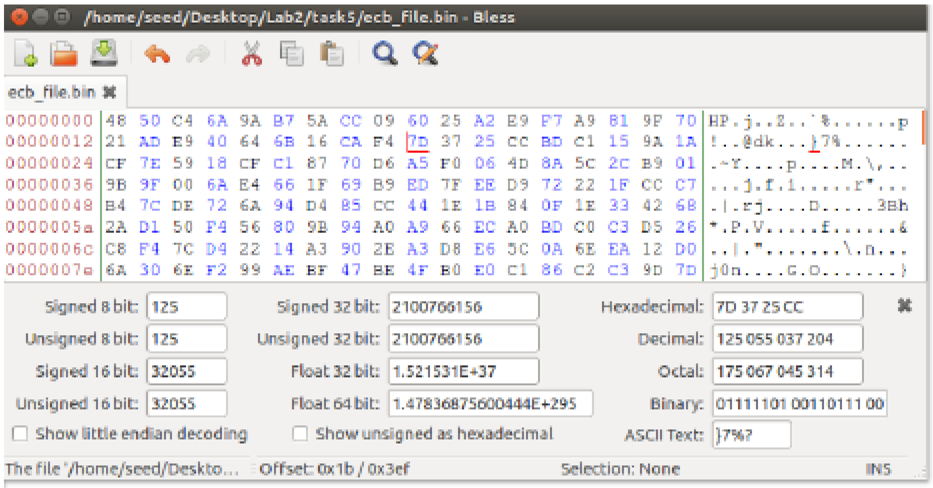


```
[09/21/22]seed@VM:~/.../task5$ openssl enc -aes-128-ecb -e -in fi
le.txt -out ecb_file.bin -K 00112233445566778889aabbccddeeff -iv
0102030405060708
warning: iv not use by this cipher
[09/21/22]seed@VM:~/.../task5$ openssl enc -aes-128-cbc -e -in fi
le.txt -out cbc_file.bin -K 00112233445566778889aabbccddeeff -iv
0102030405060708
[09/21/22]seed@VM:~/.../task5$ openssl enc -aes-128-ofb -e -in fi
le.txt -out ofb_file.bin -K 00112233445566778889aabbccddeeff -iv
0102030405060708
[09/21/22]seed@VM:~/.../task5$ openssl enc -aes-128-cfb -e -in fi
le.txt -out cfb_file.bin -K 00112233445566778889aabbccddeeff -iv
0102030405060708
[09/21/22]seed@VM:~/.../task5$
```

Changing the 55 bit for each file. Showing original then altered. This is for ECB where I show where the 55th byte is and change it to something.

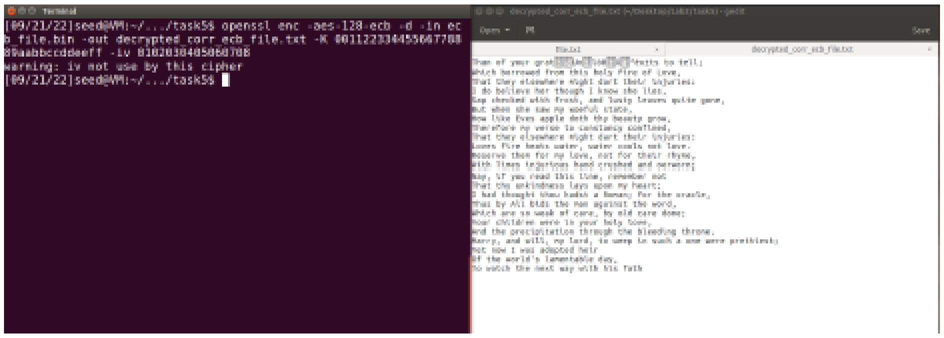


```
/home/seed/Desktop/Lab2/task5/ecb_file.bin - Bless
ecb_file.bin
00000000 48 50 C4 6A 9A B7 5A CC 09 60 25 A2 E9 F7 A9 81 9F 70 HP.j..Z..`%......p
00000012 21 AD E9 40 64 6B 16 CA F4 CD 37 25 CC BD C1 15 9A 1A !..@dk....7%......
00000024 CF 7E 59 18 CF C1 87 70 D6 A5 F0 06 4D 8A 5C 2C B9 01 .~Y....p....M.\,..
00000036 9B 9F 00 6A E4 66 1F 69 B9 ED 7F EE D9 72 22 1F CC C7 ...j.f.i.....r"...
00000048 B4 7C DE 72 6A 94 D4 85 CC 44 1E 1B 84 0F 1E 33 42 68 .|.rj....D.....3Bh
0000005a 2A D1 50 F4 56 80 9B 94 A0 A9 66 EC A0 BD C0 C3 D5 26 *.P.V.....f......&
0000006c C8 F4 7C D4 22 14 A3 90 2E A3 D8 E6 5C 0A 6E EA 12 D0 ..|."......\.n...
0000007e 6A 30 6E F2 99 AE BF 47 BE 4F B0 E0 C1 86 C2 C3 9D 7D j0n....G.O.......}

Signed 8 bit: -51          Signed 32 bit: -852023860              Hexadecimal: CD 37 25 CC
Unsigned 8 bit: 205        Unsigned 32 bit: 3442943436            Decimal: 205 055 037 204
Signed 16 bit: -13001      Float 32 bit: -1.920442E+08            Octal: 315 067 045 314
Unsigned 16 bit: 52535     Float 64 bit: -9.52239309374886E+63    Binary: 11001101 00110111 00
Show little endian decoding   Show unsigned as hexadecimal        ASCII Text: ?7%?
Offset: 0x1b / 0x3ef       Selection: None       INS
```



```
/home/seed/Desktop/Lab2/task5/ecb_file.bin - Bless
ecb_file.bin
00000000 48 50 C4 6A 9A B7 5A CC 09 60 25 A2 E9 F7 A9 81 9F 70 HP.j..Z..`%......p
00000012 21 AD E9 40 64 6B 16 CA F4 7D 37 25 CC BD C1 15 9A 1A !..@dk...}7%......
00000024 CF 7E 59 18 CF C1 87 70 D6 A5 F0 06 4D 8A 5C 2C B9 01 .~Y....p....M.\,..
00000036 9B 9F 00 6A E4 66 1F 69 B9 ED 7F EE D9 72 22 1F CC C7 ...j.f.i.....r"...
00000048 B4 7C DE 72 6A 94 D4 85 CC 44 1E 1B 84 0F 1E 33 42 68 .|.rj....D.....3Bh
0000005a 2A D1 50 F4 56 80 9B 94 A0 A9 66 EC A0 BD C0 C3 D5 26 *.P.V.....f......&
0000006c C8 F4 7C D4 22 14 A3 90 2E A3 D8 E6 5C 0A 6E EA 12 D0 ..|."......\.n...
0000007e 6A 30 6E F2 99 AE BF 47 BE 4F B0 E0 C1 86 C2 C3 9D 7D j0n....G.O.......}

Signed 8 bit: 125          Signed 32 bit: 2100766156              Hexadecimal: 7D 37 25 CC
Unsigned 8 bit: 125        Unsigned 32 bit: 2100766156            Decimal: 125 055 037 204
Signed 16 bit: 32055       Float 32 bit: 1.521531E+37             Octal: 175 067 045 314
Unsigned 16 bit: 32055     Float 64 bit: 1.47836875600444E+295    Binary: 01111101 00110111 00
Show little endian decoding   Show unsigned as hexadecimal        ASCII Text: }7%?
The file '/home/seed/Deskto...   Offset: 0x1b / 0x3ef   Selection: None   INS
```

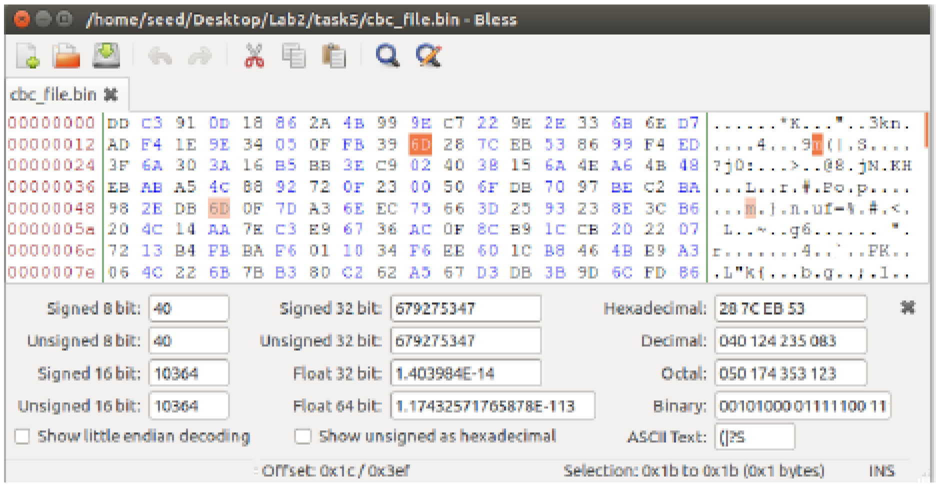
File after decryption. Here the 1st line has some data missing as it was altered but for the most part all of the data is not altered and can make the most of what was original..



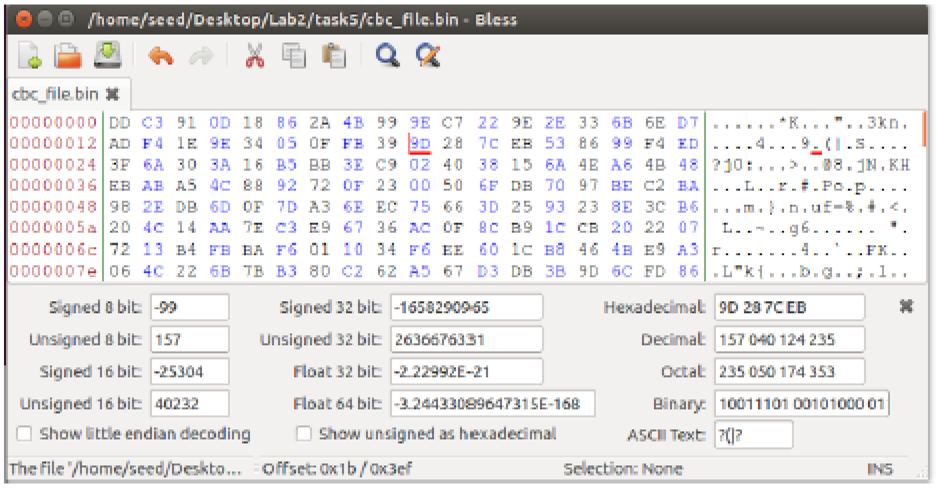
```
[09/21/22]seed@VM:~/.../task5$ openssl enc -aes-128-ecb -d -in ecb_file.bin -out decrypted_corr_ecb_file.txt -K 00112233445566778899aabbccddeeff -iv 0102030405060708
warning: iv not use by this cipher
[09/21/22]seed@VM:~/.../task5$
```

```
Than of your gra[illegible]tests to tell;
Which borrowed from this holy fire of love,
That they elsewhere might dart their injuries:
I do believe her though I know she lies,
Sap checked with frost, and lusty leaves quite gone,
But when she saw my woeful state,
How like Eve's apple doth thy beauty grow,
Therefore my verse to constancy confined,
That they elsewhere might dart their injuries:
Loves fire heats water, water cools not love.
Reserve them for my love, not for their rhyme,
With Times injurious hand crushed and overworn;
Nay, if you read this line, remember not
That the unkindness lays upon my heart:
I had thought thou hadst a Romany for the oracle,
Thus by All bids the man against the word,
Which are so weak of care, by old care done:
Your children were in your holy love,
And the precipitation through the bleeding throne.
Marry, and will, my lord, to weep in such a one were prettiest;
Not now I was adopted heir
Of the world's lamentable day,
To watch the next way with his faith
```

CBC file changing the 55th bit for the file after it was encrypted

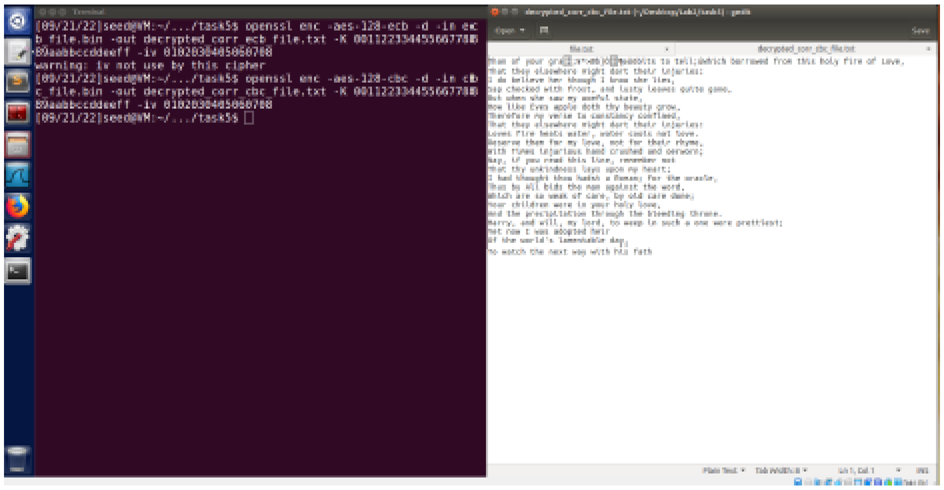


```
/home/seed/Desktop/Lab2/task5/cbc_file.bin - Bless
cbc_file.bin

00000000 DD C3 91 0D 18 86 2A 4B 99 9E C7 22 9E 2E 33 6B 6E D7  ......*K..."..3kn.
00000012 AD F4 1E 9E 34 05 0F FB 39 6D 28 7C EB 53 86 99 F4 ED  ....4...9m(|.S....
00000024 3F 6A 30 3A 16 B5 BB 3E C9 02 40 38 15 6A 4E A6 4B 48  ?j0:...>..@8.jN.KH
00000036 EB AB A5 4C 88 92 72 0F 23 00 50 6F DB 70 97 BE C2 BA  ...L..r.#.Po.p....
00000048 98 2E DB 6D 0F 7D A3 6E EC 75 66 3D 25 93 23 8E 3C B6  ...m.}.n.uf=%.#.<.
0000005a 20 4C 14 AA 7E C3 E9 67 36 AC 0F 8C B9 1C CB 20 22 D7   L..~..g6...... ".
0000006c 72 13 B4 FB BA F6 01 10 34 F6 EE 60 1C B8 46 4B E9 A3  r.......4..`..FK..
0000007e 06 4C 22 6B 7B B3 80 C2 62 A5 67 D3 DB 3B 9D 6C FD B6  .L"k{...b.g..;.l..

Signed 8 bit: 40          Signed 32 bit: 679275347            Hexadecimal: 28 7C EB 53
Unsigned 8 bit: 40        Unsigned 32 bit: 679275347          Decimal: 040 124 235 083
Signed 16 bit: 10364      Float 32 bit: 1.403984E-14          Octal: 050 174 353 123
Unsigned 16 bit: 10364    Float 64 bit: 1.17432571765878E-113 Binary: 00101000 01111100 11
Show little endian decoding   Show unsigned as hexadecimal    ASCII Text: (|?S
Offset: 0x1c / 0x3ef      Selection: 0x1b to 0x1b (0x1 bytes)   INS
```



```
/home/seed/Desktop/Lab2/task5/cbc_file.bin - Bless
cbc_file.bin

00000000 DD C3 91 0D 18 86 2A 4B 99 9E C7 22 9E 2E 33 6B 6E D7  ......*K..."..3kn.
00000012 AD F4 1E 9E 34 05 0F FB 39 9D 28 7C EB 53 86 99 F4 ED  ....4...9.(|.S....
00000024 3F 6A 30 3A 16 B5 BB 3E C9 02 40 38 15 6A 4E A6 4B 48  ?j0:...>..@8.jN.KH
00000036 EB AB A5 4C 88 92 72 0F 23 00 50 6F DB 70 97 BE C2 BA  ...L..r.#.Po.p....
00000048 98 2E DB 6D 0F 7D A3 6E EC 75 66 3D 25 93 23 8E 3C B6  ...m.}.n.uf=%.#.<.
0000005a 20 4C 14 AA 7E C3 E9 67 36 AC 0F 8C B9 1C CB 20 22 D7   L..~..g6...... ".
0000006c 72 13 B4 FB BA F6 01 10 34 F6 EE 60 1C B8 46 4B E9 A3  r.......4..`..FK..
0000007e 06 4C 22 6B 7B B3 80 C2 62 A5 67 D3 DB 3B 9D 6C FD B6  .L"k{...b.g..;.l..

Signed 8 bit: -99         Signed 32 bit: -1658290965          Hexadecimal: 9D 28 7C EB
Unsigned 8 bit: 157       Unsigned 32 bit: 2636676331         Decimal: 157 040 124 235
Signed 16 bit: -25304     Float 32 bit: -2.22992E-21          Octal: 235 050 174 353
Unsigned 16 bit: 40232    Float 64 bit: -3.24433089647315E-168 Binary: 10011101 00101000 01
Show little endian decoding   Show unsigned as hexadecimal    ASCII Text: ?(|?
The File '/home/seed/Deskto...  Offset: 0x1b / 0x3ef   Selection: None   INS
```

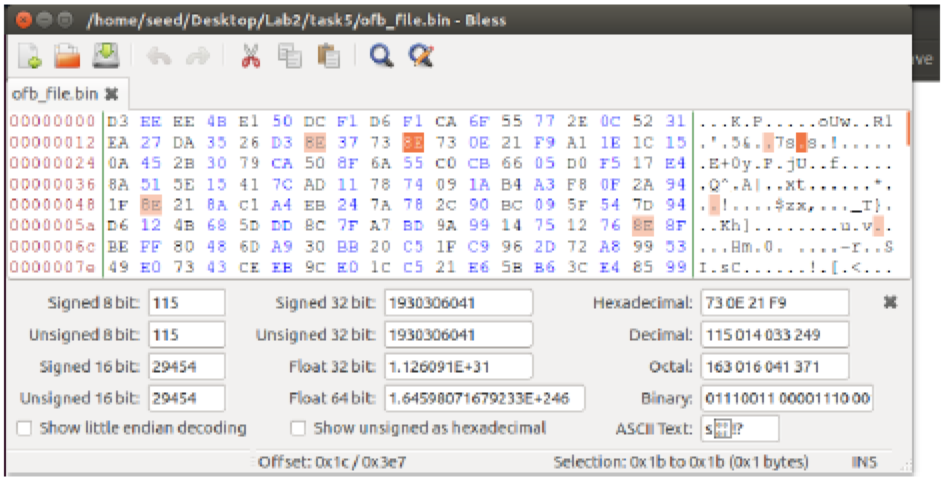
After decrypting it with the corrupted bit for the cbc it looks as though it is a little less ideal then ecb as with cbc there is less that we are able to tell what the original text was about.



```
[09/21/22]seed@VM:~/.../task5$ openssl enc -aes-128-ecb -d -in ec
b_file.bin -out decrypted_corr_ecb_file.txt -K 00112233445566778B
89aabbccddeeff -iv 0102030405060708
warning: iv not use by this cipher
[09/21/22]seed@VM:~/.../task5$ openssl enc -aes-128-cbc -d -in cb
c_file.bin -out decrypted_corr_cbc_file.txt -K 00112233445566778B
89aabbccddeeff -iv 0102030405060708
[09/21/22]seed@VM:~/.../task5$ 
```

```
decrypted_corr_cbc_file.txt (~/Desktop/Lab1/task5) - gedit
file.txt    decrypted_corr_cbc_file.txt

[illegible]
```

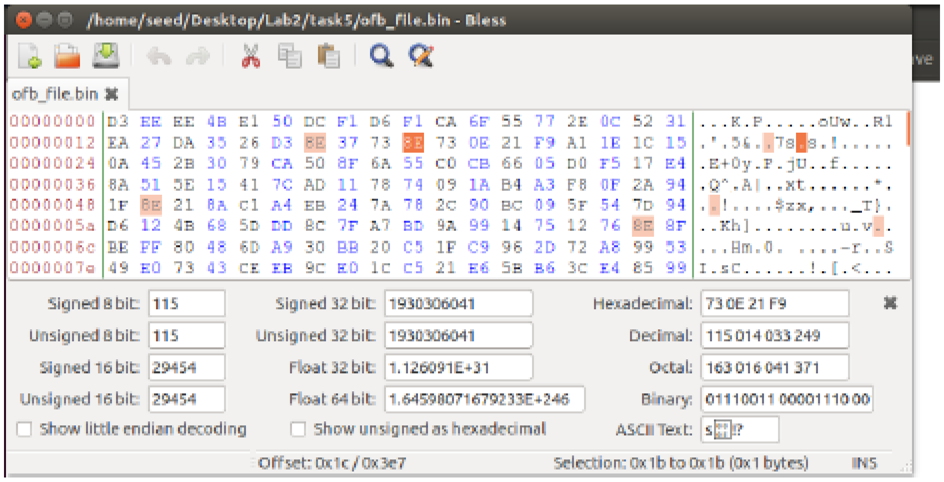
Ofb file changing the 55 bit on the file that was encrypted


/home/seed/Desktop/Lab2/task5/ofb_file.bin - Bless

ofb_file.bin

```
00000000 D3 EE EE 4B E1 50 DC F1 D6 F1 CA 6F 55 77 2E 0C 52 31 ...K.P.....oUw..R1
00000012 EA 27 DA 35 26 D3 8E 37 73 8E 73 0E 21 F9 A1 1E 1C 15 .'.5&..7s.s.!.....
00000024 0A 45 2B 30 79 CA 50 8F 6A 55 C0 CB 66 05 D0 F5 17 E4 .E+0y.P.jU..f.....
00000036 8A 51 5E 15 41 7C AD 11 78 74 09 1A B4 A3 F8 0F 2A 94 .Q^.A|..xt......*.
00000048 1F 8E 21 8A C1 A4 EB 24 7A 78 2C 90 BC 09 5F 54 7D 94 ..!....$zx,..._T}.
0000005a D6 12 4B 68 5D DD 8C 7F A7 BD 9A 99 14 75 12 76 8E 8F ..Kh]........u.v..
0000006c BE FF 80 48 6D A9 30 BB 20 C5 1F C9 96 2D 72 A8 99 53 ...Hm.0. ....-r..S
0000007e 49 E0 73 43 CE EB 9C ED 1C C5 21 E6 5B B6 3C E4 85 99 I.sC......!.[.<...
```

```
Signed 8 bit: 115          Signed 32 bit: 1930306041               Hexadecimal: 73 0E 21 F9
Unsigned 8 bit: 115        Unsigned 32 bit: 1930306041             Decimal: 115 014 033 249
Signed 16 bit: 29454       Float 32 bit: 1.126091E+31              Octal: 163 016 041 371
Unsigned 16 bit: 29454     Float 64 bit: 1.64598071679233E+246     Binary: 01110011 00001110 00
[ ] Show little endian decoding   [ ] Show unsigned as hexadecimal   ASCII Text: s..!?
Offset: 0x1c / 0x3e7     Selection: 0x1b to 0x1b (0x1 bytes)     INS
```



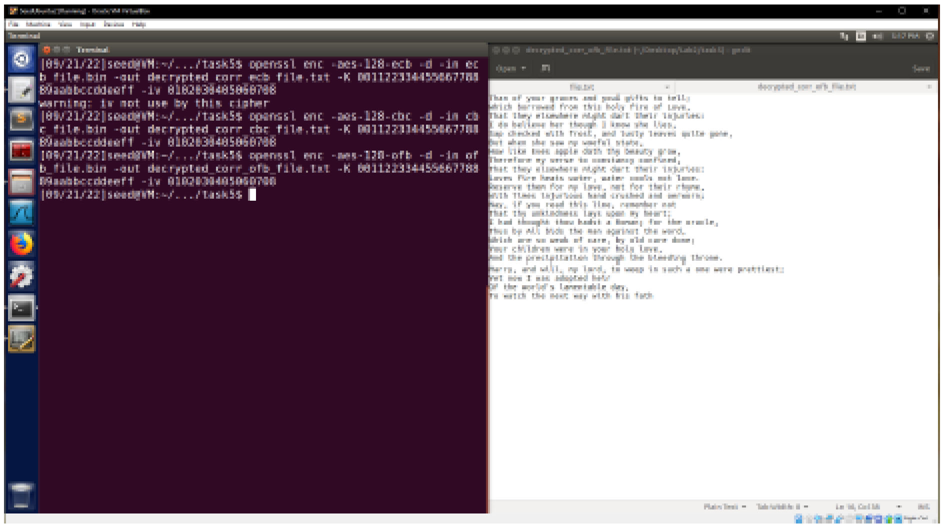
/home/seed/Desktop/Lab2/task5/ofb_file.bin - Bless

ofb_file.bin

```
00000000 D3 EE EE 4B E1 50 DC F1 D6 F1 CA 6F 55 77 2E 0C 52 31 ...K.P.....oUw..R1
00000012 EA 27 DA 35 26 D3 8E 37 73 8E 73 0E 21 F9 A1 1E 1C 15 .'.5&..7s.s.!.....
00000024 0A 45 2B 30 79 CA 50 8F 6A 55 C0 CB 66 05 D0 F5 17 E4 .E+0y.P.jU..f.....
00000036 8A 51 5E 15 41 7C AD 11 78 74 09 1A B4 A3 F8 0F 2A 94 .Q^.A|..xt......*.
00000048 1F 8E 21 8A C1 A4 EB 24 7A 78 2C 90 BC 09 5F 54 7D 94 ..!....$zx,..._T}.
0000005a D6 12 4B 68 5D DD 8C 7F A7 BD 9A 99 14 75 12 76 8E 8F ..Kh]........u.v..
0000006c BE FF 80 48 6D A9 30 BB 20 C5 1F C9 96 2D 72 A8 99 53 ...Hm.0. ....-r..S
0000007e 49 E0 73 43 CE EB 9C ED 1C C5 21 E6 5B B6 3C E4 85 99 I.sC......!.[.<...
```

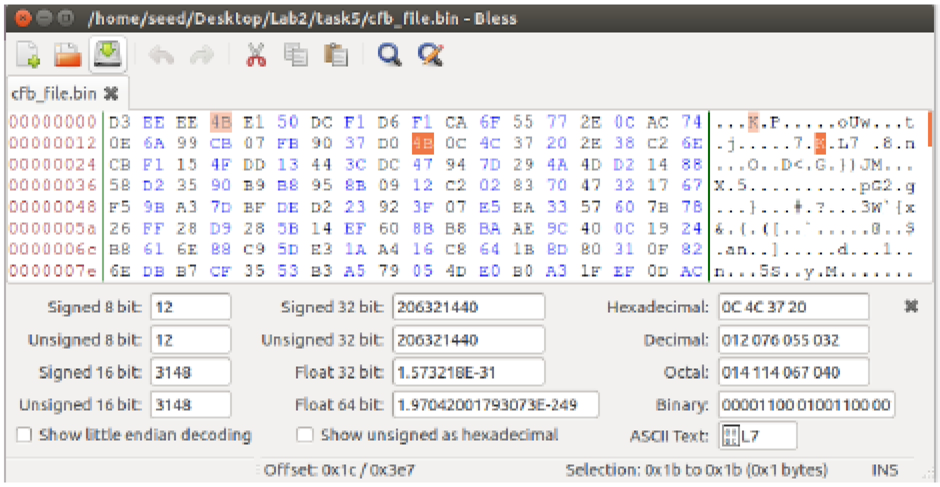
```
Signed 8 bit: 115          Signed 32 bit: 1930306041               Hexadecimal: 73 0E 21 F9
Unsigned 8 bit: 115        Unsigned 32 bit: 1930306041             Decimal: 115 014 033 249
Signed 16 bit: 29454       Float 32 bit: 1.126091E+31              Octal: 163 016 041 371
Unsigned 16 bit: 29454     Float 64 bit: 1.64598071679233E+246     Binary: 01110011 00001110 00
[ ] Show little endian decoding   [ ] Show unsigned as hexadecimal   ASCII Text: s..!?
Offset: 0x1c / 0x3e7     Selection: 0x1b to 0x1b (0x1 bytes)     INS
```

After decryption one thing was altered by the process of changing the bit and decryption which was the A instead of an r.

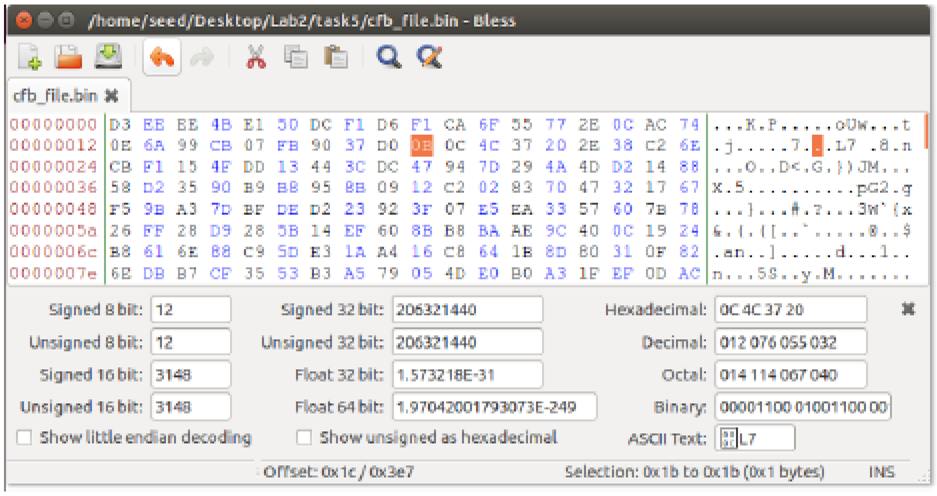


```
[09/21/22]seed@VM:~/.../task5$ openssl enc -aes-128-ecb -d -in ec
b_file.bin -out decrypted_corr_ecb_file.txt -K 00112233445566778
89aabbccddeeff -iv 0102030405060708
warning: iv not use by this cipher
[09/21/22]seed@VM:~/.../task5$ openssl enc -aes-128-cbc -d -in cb
c_file.bin -out decrypted_corr_cbc_file.txt -K 00112233445566778
89aabbccddeeff -iv 0102030405060708
[09/21/22]seed@VM:~/.../task5$ openssl enc -aes-128-ofb -d -in of
b_file.bin -out decrypted_corr_ofb_file.txt -K 00112233445566778
89aabbccddeeff -iv 0102030405060708
[09/21/22]seed@VM:~/.../task5$
```

```
Thee of your graces and good gifts to tell;
Which borrowed from this holy fire of love,
That they elsewhere might dart their injuries:
I do believe her though I know she lies,
Sap checked with frost, and lusty leaves quite gone,
But when she saw my woeful state,
How like Eves apple doth thy beauty grow,
Therefore my verse to constancy confined,
That they elsewhere might dart their injuries:
Loves fire heats water, water cools not love.
Reserve them for my love, not for their rhyme,
With Times injurious hand crushed and oerworn;
Nay, if you read this line, remember not
That thy unkindness lays upon my heart;
I had thought thou hadst a Roman; for the [illegible],
Thus by All this the man against the word.
Which are so weak of care, by old care done;
Your children were in your holy love.
And the precipitation through the bleeding throne.
Marry, and will, my lord, to weep in such a one were prettiest;
Yet now I am adopted heir
Of the world's lamentable day,
To watch the next way with his fate
```

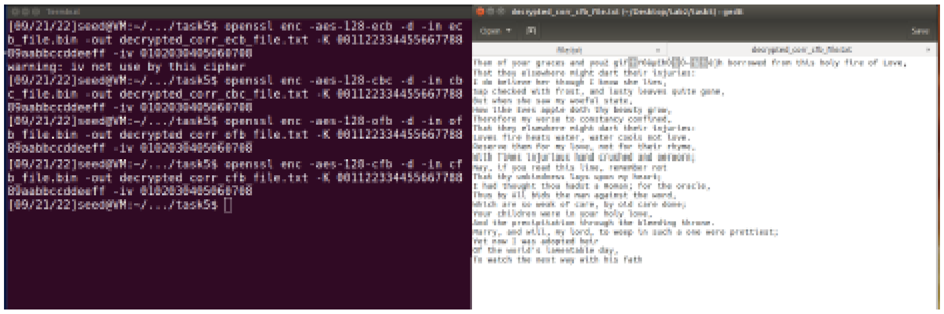


```
/home/seed/Desktop/Lab2/task5/cfb_file.bin - Bless

cfb_file.bin

00000000 D3 EE EE 4B E1 50 DC F1 D6 F1 CA 6F 55 77 2E 0C AC 74 ...K.P.....oUw...t
00000012 0E 6A 99 CB 07 FB 90 37 D0 4B 0C 4C 37 20 2E 38 C2 6E .j.....7.K.L7 .8.n
00000024 CB F1 15 4F DD 13 44 3C DC 47 94 7D 29 4A 4D D2 14 88 ...O..D<.G.})JM...
00000036 58 D2 35 90 B9 B8 95 8B 09 12 C2 02 83 70 47 32 17 67 X.5..........pG2.g
00000048 F5 9B A3 7D BF DE D2 23 92 3F 07 E5 EA 33 57 60 7B 78 ...}...#.?...3W`{x
0000005a 26 FF 28 D9 28 5B 14 EF 60 8B B8 BA AE 9C 40 0C 19 24 &.(.([..`.....@..$
0000006c B8 61 6E 88 C9 5D E3 1A A4 16 C8 64 1B 8D 80 31 0F 82 .an..].....d...1..
0000007e 6E DB B7 CF 35 53 B3 A5 79 05 4D E0 B0 A3 1F EF 0D AC n...5S..y.M.......

Signed 8 bit: 12          Signed 32 bit: 206321440                Hexadecimal: 0C 4C 37 20
Unsigned 8 bit: 12        Unsigned 32 bit: 206321440              Decimal: 012 076 055 032
Signed 16 bit: 3148       Float 32 bit: 1.573218E-31              Octal: 014 114 067 040
Unsigned 16 bit: 3148     Float 64 bit: 1.97042001793073E-249     Binary: 00001100 01001100 00
Show little endian decoding   Show unsigned as hexadecimal        ASCII Text: L7

Offset: 0x1c / 0x3e7        Selection: 0x1b to 0x1b (0x1 bytes)        INS
```



```
/home/seed/Desktop/Lab2/task5/cfb_file.bin - Bless

cfb_file.bin

00000000 D3 EE EE 4B E1 50 DC F1 D6 F1 CA 6F 55 77 2E 0C AC 74 ...K.P.....oUw...t
00000012 0E 6A 99 CB 07 FB 90 37 D0 0B 0C 4C 37 20 2E 38 C2 6E .j.....7...L7 .8.n
00000024 CB F1 15 4F DD 13 44 3C DC 47 94 7D 29 4A 4D D2 14 88 ...O..D<.G.})JM...
00000036 58 D2 35 90 B9 B8 95 8B 09 12 C2 02 83 70 47 32 17 67 X.5..........pG2.g
00000048 F5 9B A3 7D BF DE D2 23 92 3F 07 E5 EA 33 57 60 7B 78 ...}...#.?...3W`{x
0000005a 26 FF 28 D9 28 5B 14 EF 60 8B B8 BA AE 9C 40 0C 19 24 &.(.([..`.....@..$
0000006c B8 61 6E 88 C9 5D E3 1A A4 16 C8 64 1B 8D 80 31 0F 82 .an..].....d...1..
0000007e 6E DB B7 CF 35 53 B3 A5 79 05 4D E0 B0 A3 1F EF 0D AC n...5S..y.M.......

Signed 8 bit: 12          Signed 32 bit: 206321440                Hexadecimal: 0C 4C 37 20
Unsigned 8 bit: 12        Unsigned 32 bit: 206321440              Decimal: 012 076 055 032
Signed 16 bit: 3148       Float 32 bit: 1.573218E-31              Octal: 014 114 067 040
Unsigned 16 bit: 3148     Float 64 bit: 1.97042001793073E-249     Binary: 00001100 01001100 00
Show little endian decoding   Show unsigned as hexadecimal        ASCII Text: L7

Offset: 0x1c / 0x3e7        Selection: 0x1b to 0x1b (0x1 bytes)        INS
```

After decryption of the CFB file we are able to make out a lot of the file but the beginning portion of it not so much where the bit was changed. It is still corrupted and not much can be inferred from the data itself after decryption of it all.



```
[09/21/22]seed@VM:~/.../task5$ openssl enc -aes-128-ecb -d -in ec
b_file.bin -out decrypted_corr_ecb_file.txt -K 00112233445566778
899aabbccddeeff -iv 0102030405060708
warning: iv not use by this cipher
[09/21/22]seed@VM:~/.../task5$ openssl enc -aes-128-cbc -d -in cb
c_file.bin -out decrypted_corr_cbc_file.txt -K 00112233445566778
899aabbccddeeff -iv 0102030405060708
[09/21/22]seed@VM:~/.../task5$ openssl enc -aes-128-ofb -d -in of
b_file.bin -out decrypted_corr_ofb_file.txt -K 00112233445566778
899aabbccddeeff -iv 0102030405060708
[09/21/22]seed@VM:~/.../task5$ openssl enc -aes-128-cfb -d -in cf
b_file.bin -out decrypted_corr_cfb_file.txt -K 00112233445566778
899aabbccddeeff -iv 0102030405060708
[09/21/22]seed@VM:~/.../task5$ 
```

```
decrypted_corr_cfb_file.txt (~/Desktop/Lab2/task5) - gedit
Open   Save
file.txt    decrypted_corr_cfb_file.txt

Than of your graces and your gif[illegible]h borrowed from this holy fire of Love,
That they elsewhere might dart their injuries:
I do believe her though I know she lies,
Sap checked with frost, and lusty leaves quite gone,
But when she saw my woeful state,
How like Eve's apple doth thy beauty grow,
Therefore my verse to constancy confined,
That they elsewhere might dart their injuries:
Love's fire heats water, water cools not love.
Reserve them for my love, not for their rhyme,
With Time's injurious hand crushed and o'erworn;
Nay, if you read this line, remember not
That thy unkindness lays upon my heart;
I had thought thou hadst a woman; for the oracle,
Thus by all bids the man against the word,
Which are so weak of care, by old care done;
Your children were in your holy love,
And the precipitation through the bleeding throne.
Marry, and will, my lord, to weep in such a one were prettiest;
Yet now I was adopted heir
Of the world's lamentable day,
To watch the next way with his fath
```

CFB and OFB would have the most data recovered as they both do not have padding. Here the CFB file still has some data corrupted. It would still provide data corruption after it had been decrypted and the 55th bit had been changed. Both ECB and CBC did not show most data as it still shows its encryption info after the corruption due to which we think the encryption process is more secure in ECB and CBC.