

Name: Bharath Karumudi
Lab: Secret-Key Encryption

Task 1: Frequency Analysis Against Monoalphabetic Substitution Cipher

Frequency analysis

ytm xqavhq yzhu xu qzupvd lmat qnacq vxgxy hmrty vbynh ytmq ixur qyhvurn vlvhpq yhme ytn gvrnh bnniq imsn v uxuvrnuvhmuu yxx ytn vlvhpq hvan lvg gxxsnupnp gd ytn pncmgn xb twhfd lnmugyntu vy myq xxyqny vup ytn veevhnuv mceixqmxu xb tmq bmic axcevd vy ytn nup vup my lvg qtvevp gd ytn ncnhrnuan xb cnyxx ymcng ze givarsklu eximymag vhacavpd vaynmfqc vup v uvyxuvi uxafnhqyvnxu vg qhmnbd vup cvp vg v bnfnh phvc vxgxy ltnyntuh ytnhx xxzry yx gn v ehnqmprnu lmbuhnd ytn qnvgxu pmppu ozgy qncc nkyhv ixur my lvg nkyhv ixur gnavzqn ytn xqavhq lnhn cxfnpx yz ytn bmhgy lnsup mu cvhat yx vxkmp axubimaymur lmyt ytn aixqmur anhncxud xb ytn lmuyhn xidcemaq ytvusq ednxuratvur xun gmr jzngymxu qzhxxupmurr ytmq dnvhg vavpncc vlvhpq mg txl xh mb ytn anhncxud lmi vphphng cnyxq ngenamivni vbynh ytn rxipnu rixgng lmat gnavch v ozgnavuy axcmurxzy evhyd bxh ymcng ze ytn cxfnccnq qenvhtnvpnp gd exlnhbzi txkldlxpx lxcmu ltx tnieng hvnq cmliimxug xb pxiihvq yx brmty qnkzvi twhvqgcnuy vhxzup ytn axzuyhd qmrurivngh qzeexhy rxipnu rixgng vyynupnng qlvvtvpn ytn cncqnfq mu givas qexhy np iveni emuq vup qxzupnp xbb vxgxy qnkmgq exlnh mcgvivuaq bhx ytn hnp avheny vup ytn qyvrrn xu ytn vmb n lvg avilng xxy vxgxy evd munjymd vbynh myg bxhcnuh vuatxh avyy qpvphn jzmy xuan qtn invhunp ytv ytn lvg csmurz bkh inqg ytvn v cvin axtxqy vup pzhrm ytn anhncxud uvyyvinn exhycv yxxs v gizuy vup qvymqgbdmur pmr v ytn viicvhn hxqyhn xb uxcmuvnp pmhnhayxhg txl azxip ytv ytn gn yxeenp vq my yzhuq xzy v yinvqy mu ynhcq xb ytn xqavhq my ehxqygid lxuy gn lxcnu mufxfnp mu ymcng ze qvmp ytv yvlytxzrt ytn rixgng qmrurumbnp ytn munymwymfng izvuzat ytdn unfnh muynupnnp my yx gn ozgy vu vlvhpq qnvgxu acvevmru xh xun ytv ygnavcn vqgxmavnpn xuid lmyt hnpanvheny waymxug muqyvnp v qexsnqlxvcu qvmp ytn rhxze mg lxhsmr qntmup aixqnp pxhqq vup tvq qmuan vcvqgnp cmiimxh xbh myq irnvi pbnuqnp bzup lmat vbynh ytn rixgng lvg blixpnp lmyt ytxzqvupq xb pxvymxu xb inqg bxhc enxein mu qxcm axzuyhmg ux avii yz lnhv givas rxluq lnuy xzy mu vpfvuan xb ytn xqavhq ytxzrt ytn cxfnccnq lmi viexqy anhymwid ytn hnbnhnuanq gnbxhn vup pzhrm ytn anhncxud ngenamivi qmuan faxvi cnyxq qzeexhyhng imsn vgtind opp izvhz phnu vup umaxin smpcvu vhn qatnpzinp ehnqnuynhg uxvynh bnvyzhn xb ytmq qnvgxu ux xun hnviid surxq ltx mg rixmru yz lmu gnqy emayzhn vhrzvgid ytmq tveenug v ixy ytn ymcn muvhrzvgid ytn uvmigymnh uvhhvymfn xuid qnhfqn ytn vlvhpq tden cvatmun gzy xbnyu ytn enxein bxhnavgymur ytn hvan qxaviimp xqavhxixrmqy avu cwsn xuid npzavypn rznnqng ytn lvd ytn vavpncc yvqzivng ytn gmc lmuunh pxnqy tnie mu nfnhd ytnh avynrxhd ytn uxcmunn lmyt ytn cxqy fxyng lmuq gzy ytn gnqy emayzhn avynrxhd fxynhg vhn vgsnp yz imgy ytnhx yxe cxfmnp ytn ehnbnhnuymvi xphph mb v cxfmn rnqg cxhn ytvu enhanuy xb ytn bmhgeyeian fxynq my lmuq ltnu ux cxfmn cuvvrng ytv ytn xun lmyt ytn bnlnqy bmhgeyeian fxynq mg nimcmuvynp vup myq fxynq vhn hnmpcyhmgxng yx ytn cxfmnp ytvv rvhnunhp ytn nimcmuvynp gviixyg qnaxupeivan fxynq vup ytmq axymuzng zuymi v lmuunh ncnhrng my mg vli ynhmgid axubzqmr gzy veehnuuyd ytn axuqnuqzq bvfxhmyn axcnq xxy vtvpn mu ytn nup ytmq cnvuq ytvv nupxbqnvxu vlvhpq atvyyvhn mufvhmvqid mufxfnp yxhyzhznq genazivymxu vxgxy lmat bmic lxxzip cxqy imsnid gn fxynhg qnaxup xh ytmq bvfxhmyn vup ytnu njzvivid yxhyzhnp axuaizqmxuq vxgxy lmat bmic omtry ehnfmvi mu ylv yxqzqe gnylnnu gxdtxxp vup ytn nfnyuzvi lmuunh gmhpccu mu lmyt ixyg xb nkenhyq gnyymur ytu ytn hnfnvnuv xb ytmq qtxhy ytn ehmwu lnuy yx qexyimrty ivqy dnvh unvhid vlii ytn bxhnavgynhg pnaivhnp lv lv ivup ytn ehnqzeycmfn lmuunh vup bxh ylx vup v tvb cmuzuyg ytdn lnhx axhnhay qnbxhn vnu nfnixen qvzbv lvg hnfnvnp vup ytn hmrtbzli lmuunh cxxuiimrty lvg ahxlnp ytmq dnvh vlvhpq lyvatnbg vhn zuujzvild pmfmpnp gnylnnu ythnn gmiigxvpg xxyqmn nggmur cmgqzxn ytn bvfxhmyn vup ytn qtevn xb lvynh lmat mq ytn gvrnhq ehnpmaymxu lmyt v bnl bxhnavgymur v tvni cvhd lmu bxh rny xxy gzy vlii xb ytxqn bmicq tvfn tmgxhnavi xqavhxixrmqy avyvnhq vrvmuqy ytn qtevn xb lvynh tvq uxcmuvymxuq cxhn ytvu vud yxth bmic vup lvg viqx uvcnp ytn dnvhg gnqy gd ytn ehxpzanh vup pmhnhayxhg rzmpq dny my lvg ux yx uxcmuvynp bxh v qahnmu vayxhg rzmp lvhph bxh gnqy nucnqg vup ux bmic tvq lxi gnqy emayzhn lmytxzy ehnfmzxqid ivumpur vy ivqy ytn vayxhg uxcmuvymxu qmuan ghfvntvhy mu ytmq dnvh ytn gnqy nuqncgin qvr nupnp ze rxmr yx ythnn gmiigxvpg lmat mq qmrurumbavuy gnavzqn vayxhg cvsn ze ytn vavpnccdg ivhrgy ghuuat ytv ymic ltnin pmfmpnp viqx lxi ytn gnqy phvcv rxipnu rixgn vup ytn gnyv gzy myg bmicccvsnh cvhymu capxuvrt lvg ux yx uxcmuvynp bxh gnqy pmhnhayxh vup vevhy bhxc vrhx cxfmnp ytvv ivup gnqy emayzhn lmytxzy viqx nvhumur gnqy pmhnhayxh uxcmuvymxuq vhn bnl vup bvh gnlynunu

Removed spaces

3931 chars

Fig1: Cipher Text

Letter frequencies

```
n : 488
y : 373
v : 348
x : 291
u : 280
q : 276
H : 264
R : 235
t : 183
i : 166
p : 156
a : 116
c : 104
z : 95
l : 90
g : 83
b : 83
r : 82
e : 76
d : 59
f : 49
s : 19
j : 5
k : 5
o : 4
w : 1
```

Fig2: Occurrences of each letter (frequency)

2 letter sequences

```
yt => 116
tn => 89
mu => 74
nh => 66
nq => 62
hn => 59
vu => 58
vh => 57
gy => 55
xu => 53
nv => 50
up => 47
yn => 47
np => 46
vy => 45
xh => 45
nu => 44
ym => 39
uy => 37
vi => 37
yx => 36
vq => 35
uv => 34
gn => 32
my => 32
av => 31
xz => 30
ur => 29
na => 29
tv => 29
qn => 28
uq => 27
mq => 27
qv => 27
lv => 26
hq => 26
nc => 26
iv => 25
hm => 24
hy => 23
py => 23
zy => 23
tm => 23
cn => 22
xb => 22
cv => 22
lm => 22
xy => 22
qm => 22
mi => 22
fn => 22
qx => 21
ii => 21
un => 21
pn => 21
yv => 20
id => 20
ix => 20
an => 20
ny => 20
in => 20
en => 19
xc => 19
ux => 19
nn => 18
qq => 18
cx => 18
ma => 18
yq => 18
pm => 18
nx => 18
```

Fig3: Two letter frequencies

3 letter sequences

```
ytn => 79
vup => 30
ngy => 22
pyt => 20
mur => 20
ynh => 18
xzy => 16
nhn => 16
nuy => 14
ytv => 14
bxh => 14
gnq => 14
mxu => 14
vii => 13
vyn => 13
uvy => 12
lvq => 12
nvh => 12
tmq => 12
gvt => 12
muu => 11
upy => 11
xhy => 11
vym => 11
lmu => 11
ymu => 11
yxh => 11
tnv => 11
cmu => 11
hna => 10
tnh => 10
xuq => 10
myt => 10
ymx => 10
tvv => 10
vhp => 10
uyt => 9
ncx => 9
npy => 9
ynp => 9
mic => 9
hpg => 9
ytm => 9
lmy => 9
nvq => 9
dyt => 9
yzh => 9
nhq => 9
rty => 9
byt => 8
qmu => 8
tyt => 8
xby => 8
bmi => 8
vhn => 8
nav => 8
uxc => 8
uan => 8
vlv => 8
axu => 8
ltm => 8
qav => 8
avh => 8
hnp => 8
lvh => 8
nax => 8
cxf => 8
fxy => 8
tng => 8
xcm => 8
```

Fig4: Three letter frequencies

4 letter sequences

```
pytn => 14
upytn => 11
gnqy => 10
ymxu => 10
lmyt => 9
vhpq => 9
vupy => 9
ytnh => 9
ytvy => 9
muvy => 9
dytn => 8
ytng => 8
lvhp => 8
ytnv => 8
bmic => 8
ytmg => 8
vlvh => 8
xcmu => 8
cmuv => 8
mxuq => 8
yzhn => 7
yytn => 7
ngyt => 7
fxyn => 7
vymx => 7
ayxh => 7
uytn => 7
uxcm => 7
vynp => 7
mury => 7
xbty => 7
ltma => 7
tmat => 7
bytn => 6
gytv => 6
xytn => 6
nhnc => 6
mrty => 6
tytn => 6
ytna => 6
vgxz => 6
gxzy => 6
npyt => 6
qavh => 6
xgav => 6
uvym => 6
ytnc => 6
bxhn => 5
ixgn => 5
ynhq => 5
rixg => 5
viid => 5
uryt => 5
dnvh => 5
ytnx => 5
qvup => 5
ymur => 5
nhqv => 5
ytxz => 5
nvup => 5
xynq => 5
ytnn => 5
xfmn => 5
ylvq => 5
cxfm => 5
hytn => 5
uuhn => 5
yxhq => 5
ytnb => 5
gytn => 5
hncc => 5
```

Fig5: Four letter frequencies

5 letter sequences

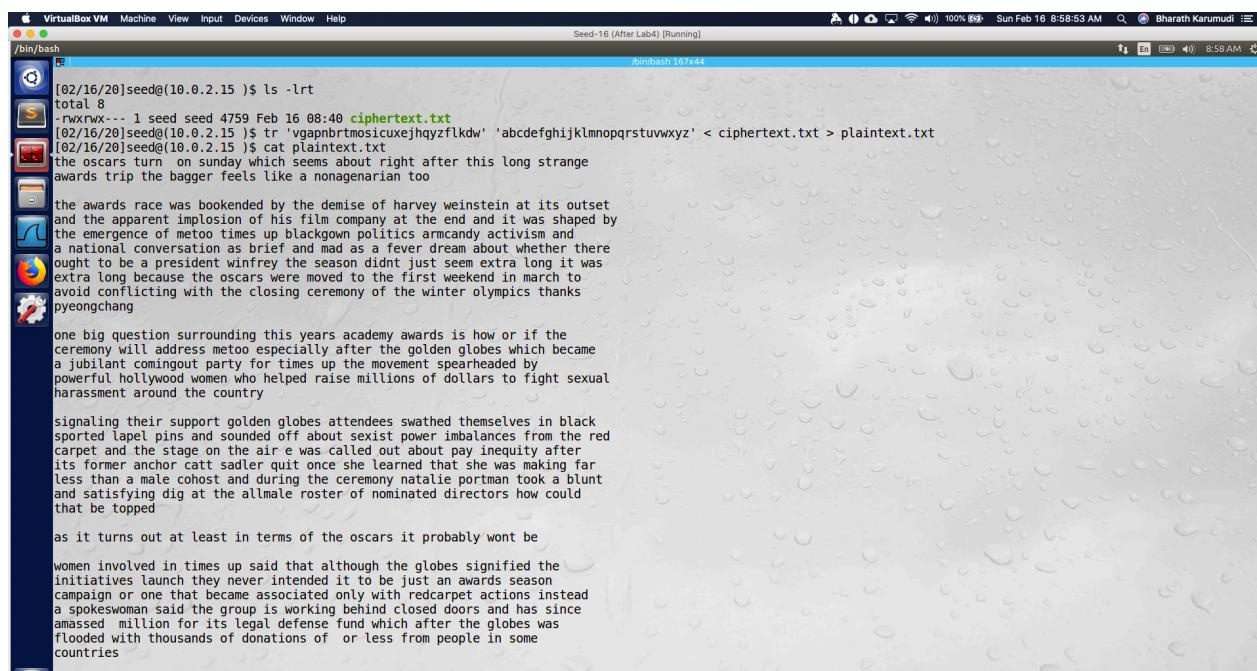
```
vupyt => 9  
upytn => 9  
cmuvy => 8  
vlvhp => 8  
vymxu => 7  
lvhpq => 7  
uxcmu => 7  
ltmat => 7  
xcmuv => 6  
xqavh => 6  
ymxuq => 6  
vgxzv => 6  
muryt => 5  
rixgn => 5  
uvynp => 5  
xbytn => 5  
muvyn => 5  
ayxhq => 5  
nhncx => 5  
lmuun => 5  
uvymx => 5  
muunh => 5  
fxynq => 5  
cxfmn => 5  
nayxh => 4  
gytvv => 4  
nfxyn => 4  
nlmyt => 4  
nbxhn => 4  
ngyem => 4  
yemay => 4  
emayz => 4  
mayzh => 4  
gyema => 4  
hnayx => 4  
ayzhn => 4  
ngytn => 4  
gnqye => 4  
ixgnd => 4  
mylvq => 4  
qnvxq => 4  
nvqxu => 4  
muvym => 4  
vbynh => 4  
tnxqa => 4  
nxqav => 4  
gavhq => 4  
lmtyt => 4  
mytyt => 4  
urytn => 4  
npytn => 4  
pmhna => 4  
ytncx => 4  
ytnxq => 4  
anhnc => 4  
hncxu => 4  
ncxud => 4  
mhnay => 4
```

Fig6: Five Letter Frequencies

6 letter sequences

```
vupytn => 8
vlvhpg => 7
xcmuvy => 6
uxcmuv => 6
lmuunh => 5
muvynp => 5
cmuvyn => 5
uvymxu => 5
ngyema => 4
gnqyem => 4
vymxug => 4
hnayxh => 4
gyemay => 4
yemayz => 4
nxqavh => 4
mayzhn => 4
emayzh => 4
mhayyx => 4
pmhnay => 4
rixgng => 4
hncxud => 4
nhncxu => 4
anhncx => 4
murytn => 4
ytnxqa => 4
qnvqku => 4
xqavhg => 4
tnxqav => 4
lmtyyt => 4
```

Fig7: Six letter frequencies



The screenshot shows a terminal window titled 'Seed-16 (After Lab4) [Running]' running on a VirtualBox VM. The terminal displays the following command sequence and output:

```
[02/16/20]seed@(10.0.2.15)$ ls -lrt
total 8
-rwxrwx--- 1 seed seed 4759 Feb 16 08:40 ciphertext.txt
[02/16/20]seed@(10.0.2.15)$ tr 'vgapnbrtmosiculejhqyzflkdw' 'abcdefghijklmnopqrstuvwxyz' < ciphertext.txt > plaintext.txt
[02/16/20]seed@(10.0.2.15)$ cat plaintext.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 blacktown politics armchair 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
spotted 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 cohort 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
```

Fig8a: Plaintext

The screenshot shows a terminal window titled 'VirtualBox VM' running on a Mac OS X desktop. The terminal window has a light gray background with a subtle water droplet pattern. It displays a single line of text in black font. The text is a decrypted article about the Academy Awards, starting with 'no call to wear black gowns went out in advance of the oscars though the movement will almost certainly be referenced before and during the ceremony especially since vocal metoo supporters like ashley judd laura dern and nicole kidman are scheduled presenters'. The terminal window includes standard Mac OS X window controls (red, yellow, green) and a status bar at the bottom.

Fig8b: Plaintext

Observation: The given cipher text was used and performed the frequency analysis on that and based on the analysis determined the key and translated the cipher to plain text.

Explanation: The given cipher was copied to the machine and using the tools [http://www.richkni.co.uk/php/crypta/freq.php] performed the frequency analysis on the text. Based on the analysis on the text and general English letter frequencies, determined the cipher was encrypted with "vgapnbrtmusicuxejhqyzflkdw" key and using the Linux translate command 'tr'; translated the article to plain text and then it was a readable text as shown in the figure.

Task 2: Encryption using Different Ciphers and Modes

```
[02/16/20]seed@[10.0.2.15]$ ls -lrt
total 16
-rwxrwx--- 1 seed seed 4759 Feb 16 08:40 ciphertext.txt
-rw-rw-r-- 1 seed seed 4759 Feb 16 08:58 plaintext.txt
[02/16/20]seed@[10.0.2.15]$ openssl enc -aes-128-ecb -e -in plaintext.txt -out cipher-aes-128-ecb.txt -K 0011223344556677889aabcccddeff
[02/16/20]seed@[10.0.2.15]$ ls -lrt
total 24
-rwxrwx--- 1 seed seed 4759 Feb 16 08:40 ciphertext.txt
-rw-rw-r-- 1 seed seed 4759 Feb 16 08:58 plaintext.txt
-rw-rw-r-- 1 seed seed 4768 Feb 16 09:17 cipher-aes-128-ecb.txt
[02/16/20]seed@[10.0.2.15]$ more cipher-aes-128-ecb.txt
-----BEGIN AES-128-CBC-HMAC-SHA1-----  
[REDACTED]  
-----END AES-128-CBC-HMAC-SHA1-----
[02/16/20]seed@[10.0.2.15]$ openssl enc -aes-128-ecb -d -in cipher-aes-128-ecb.txt -out plaintext-aes-128-ecb.txt -K 0011223344556677889aabcccddeff
[02/16/20]seed@[10.0.2.15]$ compare plaintext.txt plaintext-aes-128-ecb.txt
compare: improper image header 'plaintext.txt' @ error/txt.c/ReadTIXImage/439
[02/16/20]seed@[10.0.2.15]$ more plaintext-aes-128-ecb.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 blackown 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
spotted 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 cohort and during the ceremony natalie portman took a blunt
and satisfying dig at the allmale roster of nominated directors how could
```

Encrypted Cipher

Decrypted to Plain text

Fig1: Encryption and Decryption using ECB

```
[02/16/20]seed@[10.0.2.15]$ ls -lrt
total 16
-rwxrwx--- 1 seed seed 4759 Feb 16 08:40 ciphertext.txt
-rw-rw-r-- 1 seed seed 4759 Feb 16 08:58 plaintext.txt
-rw-rw-r-- 1 seed seed 4768 Feb 16 09:17 cipher-aes-128-ecb.txt
-rw-rw-r-- 1 seed seed 4759 Feb 16 09:19 plaintext-aes-128-ecb.txt
[02/16/20]seed@[10.0.2.15]$ openssl enc -aes-128-cbc -e -in plaintext.txt -out cipher-aes-128-cbc.txt -K 0011223344556677889aabcccddeff
[02/16/20]seed@[10.0.2.15]$ openssl enc -aes-128-cbc -e -in plaintext.txt -out cipher-aes-128-cbc.txt -K 0011223344556677889aabcccddeff -iv 0102030405060708
[02/16/20]seed@[10.0.2.15]$ ls -lrt
total 40
-rwxrwx--- 1 seed seed 4759 Feb 16 08:40 ciphertext.txt
-rw-rw-r-- 1 seed seed 4759 Feb 16 08:58 plaintext.txt
-rw-rw-r-- 1 seed seed 4768 Feb 16 09:17 cipher-aes-128-ecb.txt
-rw-rw-r-- 1 seed seed 4759 Feb 16 09:19 plaintext-aes-128-ecb.txt
-rw-rw-r-- 1 seed seed 4768 Feb 16 09:23 cipher-aes-128-cbc.txt
[02/16/20]seed@[10.0.2.15]$ more cipher-aes-128-cbc.txt
-----BEGIN AES-128-CBC-----  
[REDACTED]  
-----END AES-128-CBC-----
[02/16/20]seed@[10.0.2.15]$ openssl enc -aes-128-cbc -d -in cipher-aes-128-cbc.txt -out plaintext-aes-128-cbc.txt -K 0011223344556677889aabcccddeff -iv 0102030405060708
[02/16/20]seed@[10.0.2.15]$ more plaintext-aes-128-cbc.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 blackown 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
spotted 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 cohort and during the ceremony natalie portman took a blunt
and satisfying dig at the allmale roster of nominated directors how could
```

Fig2: Encryption and Decryption using CBC

```
[02/16/20]seed@(10.0.2.15) $ ls -lrt
total 48
-rwxrwx--- 1 seed seed 4759 Feb 16 08:40 ciphertext.txt
-rw-rw-r-- 1 seed seed 4759 Feb 16 08:58 plaintext.txt
-rw-rw-r-- 1 seed seed 4768 Feb 16 09:17 cipher-aes-128-ecb.txt
-rw-rw-r-- 1 seed seed 4759 Feb 16 09:19 plaintext-aes-128-ecb.txt
-rw-rw-r-- 1 seed seed 4768 Feb 16 09:23 cipher-aes-128-cbc.txt
-rw-rw-r-- 1 seed seed 4759 Feb 16 09:24 plaintext-aes-128-cbc.txt
[02/16/20]seed@(10.0.2.15) $ openssl enc -aes-128-cfb -e -in plaintext.txt -out cipher-aes-128-cfb.txt -K 0011223344556677889aabccddeff -iv 0102030405060708
[02/16/20]seed@(10.0.2.15) $ ls -lrt
total 56
-rwxrwx--- 1 seed seed 4759 Feb 16 08:40 ciphertext.txt
-rw-rw-r-- 1 seed seed 4759 Feb 16 08:58 plaintext.txt
-rw-rw-r-- 1 seed seed 4768 Feb 16 09:17 cipher-aes-128-ecb.txt
-rw-rw-r-- 1 seed seed 4759 Feb 16 09:19 plaintext-aes-128-ecb.txt
-rw-rw-r-- 1 seed seed 4768 Feb 16 09:23 cipher-aes-128-cbc.txt
-rw-rw-r-- 1 seed seed 4759 Feb 16 09:24 plaintext-aes-128-cbc.txt
-rw-rw-r-- 1 seed seed 4759 Feb 16 09:27 cipher-aes-128-cfb.txt
[02/16/20]seed@(10.0.2.15) $ more cipher-aes-128-cfb.txt
[BEGIN_OF_TEXT]
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 blackown 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
[BEGIN_OF_TEXT]
signaling their support golden globes attendees swathed themselves in black
```

Fig3: Encryption and Decryption using CFB

```
[02/16/20]seed@(10.0.2.15) $ clear
[02/16/20]seed@(10.0.2.15) $ ls -lrt
total 64
-rwxrwx--- 1 seed seed 4759 Feb 16 08:40 ciphertext.txt
-rw-rw-r-- 1 seed seed 4759 Feb 16 08:58 plaintext.txt
-rw-rw-r-- 1 seed seed 4768 Feb 16 09:17 cipher-aes-128-ecb.txt
-rw-rw-r-- 1 seed seed 4759 Feb 16 09:19 plaintext-aes-128-ecb.txt
-rw-rw-r-- 1 seed seed 4768 Feb 16 09:23 cipher-aes-128-cbc.txt
-rw-rw-r-- 1 seed seed 4759 Feb 16 09:24 plaintext-aes-128-cbc.txt
-rw-rw-r-- 1 seed seed 4759 Feb 16 09:27 cipher-aes-128-cfb.txt
-rw-rw-r-- 1 seed seed 4759 Feb 16 09:28 plaintext-aes-128-cfb.txt
[02/16/20]seed@(10.0.2.15) $ openssl enc -aes-128-ofb -e -in plaintext.txt -out cipher-aes-128-ofb.txt -K 0011223344556677889aabccddeff -iv 0102030405060708
[02/16/20]seed@(10.0.2.15) $ ls -lrt
[BEGIN_OF_TEXT]
another feature of this season no one really knows who is going to win best
[BEGIN_OF_TEXT]
signaling their support golden globes attendees swathed themselves in black
```

Fig4: Encryption and Decryption using OFB

Fig5: Encryption and Decryption using Blowfish

Observation: Encrypted the plain text with modes like ECB, CBC, CFB, OFB and Blowfish using Openssl utility and also decrypted the cipher texts back to plain text. The CFB and OFB are stream ciphers, so the size of both plain text and cipher text are of same size.

Explanation: Using the Openssl and enc utility encrypted the plain text with various symmetric key encryption modes. In this, used Electronic Code Block (ECB), Cipher Block Chain (CBC), Cipher Feedback (CFB), Output Feedback (OFB) and Blowfish. All the modes produced different ciphers and also decrypted the ciphers back to plain text.

Task 3: Encryption Mode – ECB vs. CBC

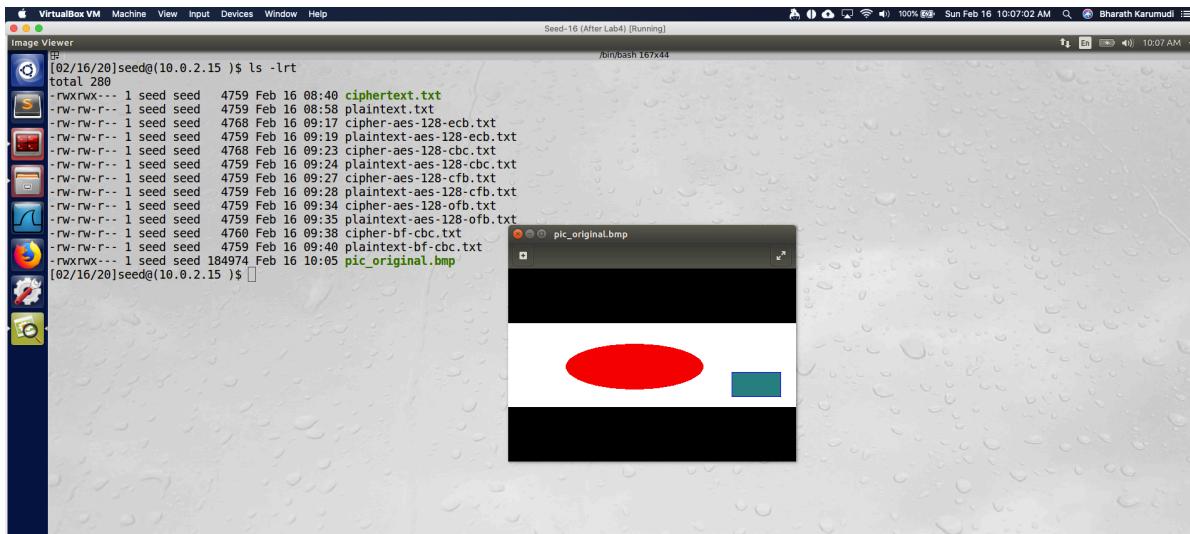


Fig1: Original bmp image – unencrypted

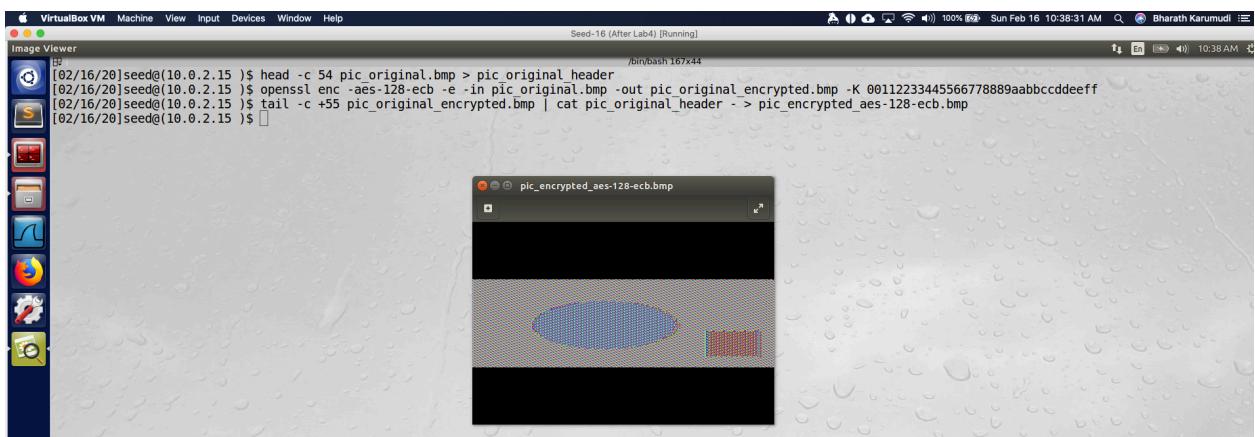


Fig2: Encrypted BMP image with ECB

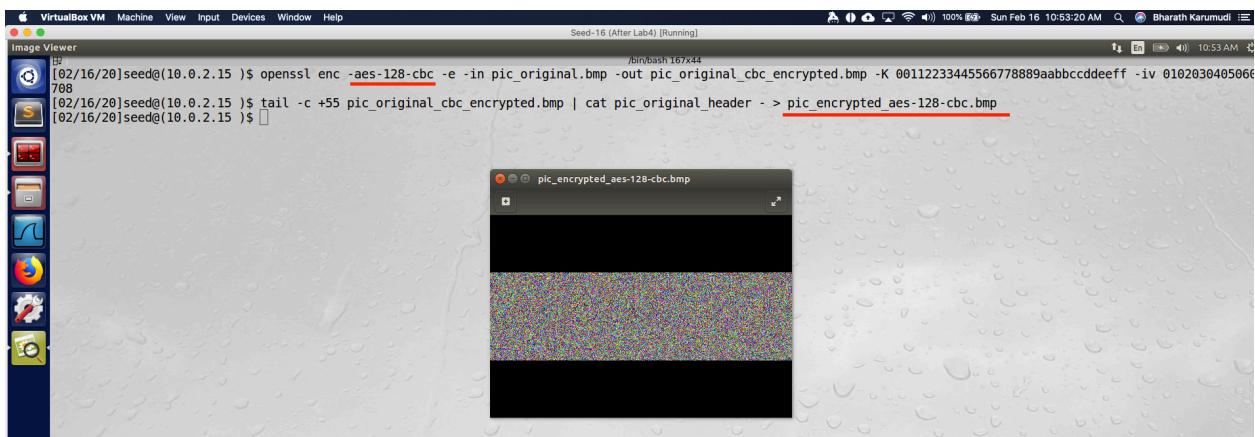


Fig3: Encrypted BMP image with CBC

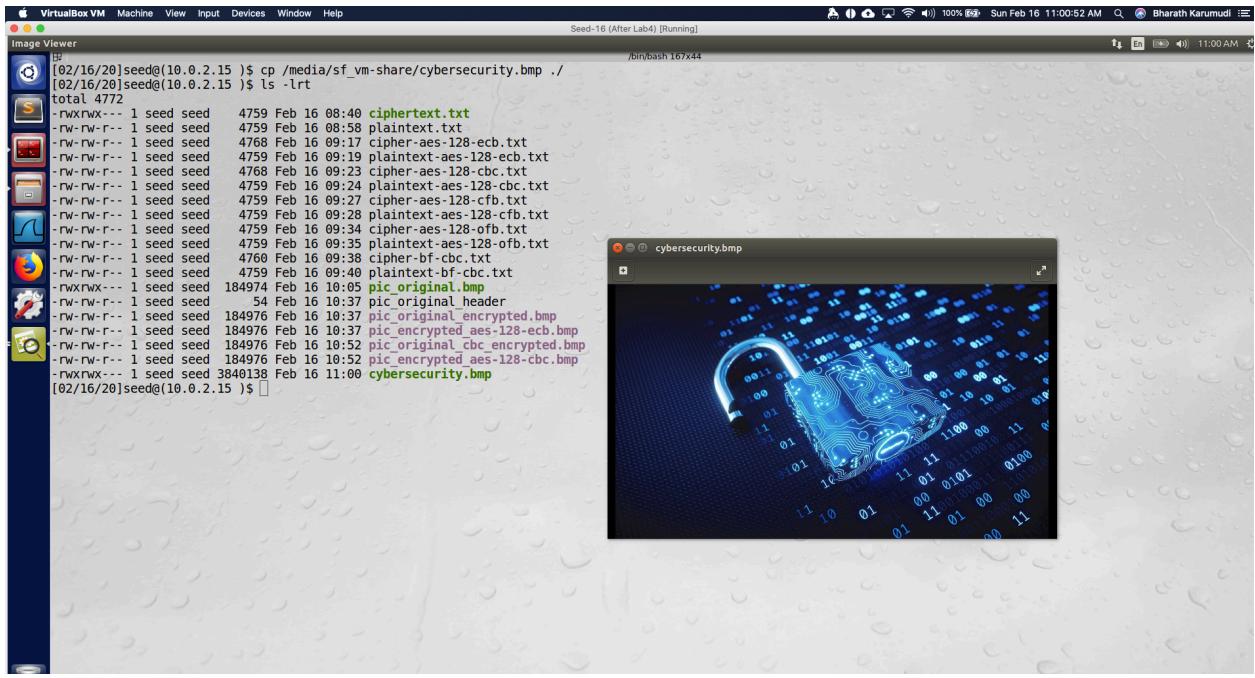


Fig4: Unencrypted bmp image

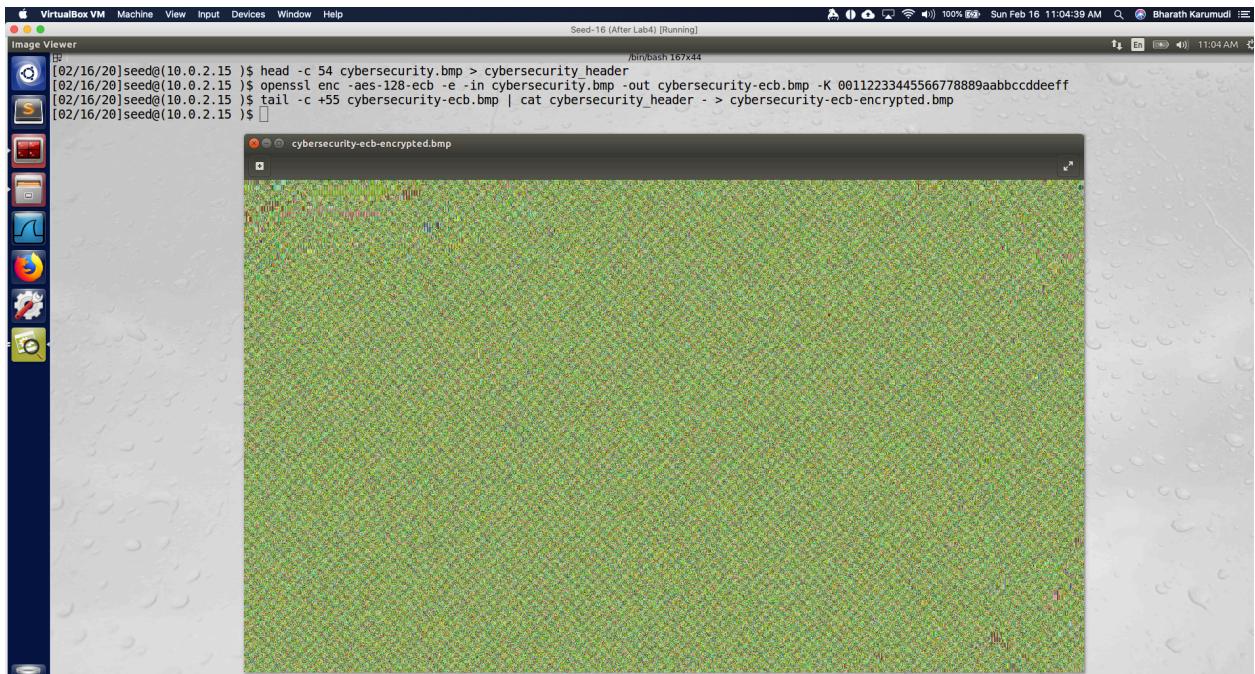


Fig5: Encrypted with ECB

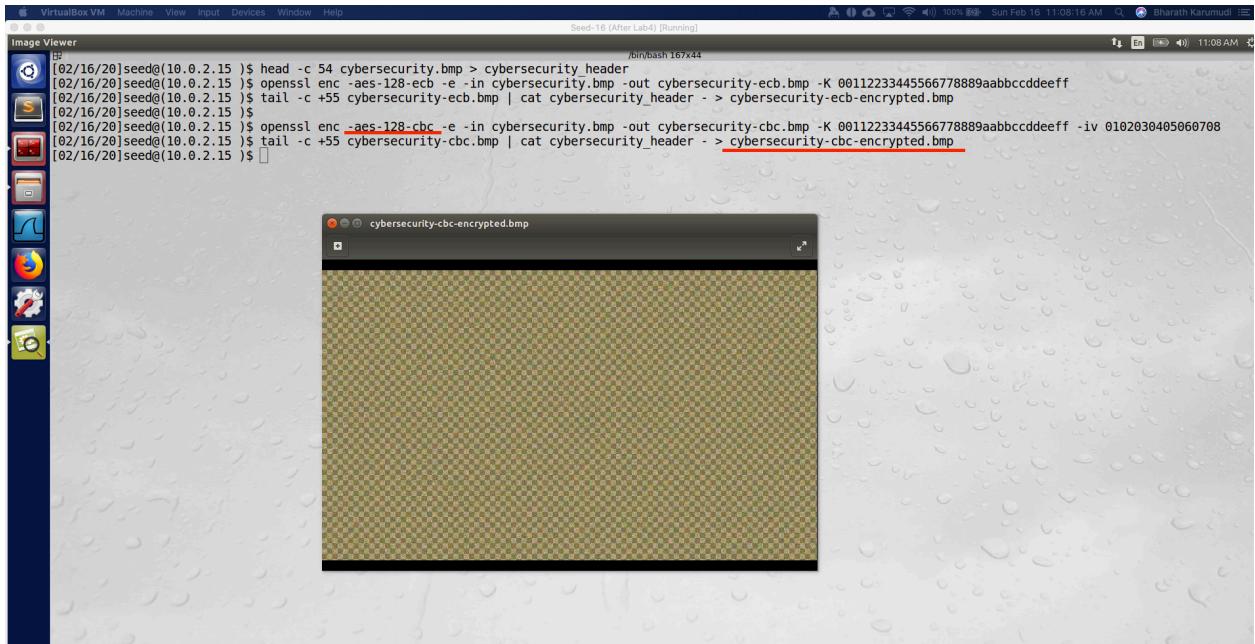


Fig6: Encrypted the image with CBC

Observation: When encrypted the given bmp image using Electronic Code Block the encrypted image still shows the evidences of the images like boarders and shapes, whereas with Cipher Block Chain there were no evidences. Also performed the same with a random image.

Explanation:

Figure 1 shows the original bmp image which is unencrypted. The image is then encrypted using ECB and appended the header of original image to the encrypted image which is bmp header, this was done using head and tail commands as shown in Fig2. The final encrypted image can be seen in Fig2 though the colors are changed it still reflects the boarders and gives the details of the image. This was because ECB is a block-based encryption.

The same image is then encrypted with Cipher Block Chain (CBC) and the result encrypted image is as shown in Fig3. We can notice there were no details of the image and it is because the CBC is a stream-based cipher so every bit will be encrypted.

The same exercise was done with a random image but as the colors in image are similar both ECB and CBC didn't reveal any details.

Task 5: Error Propagation – Corrupted Cipher Text

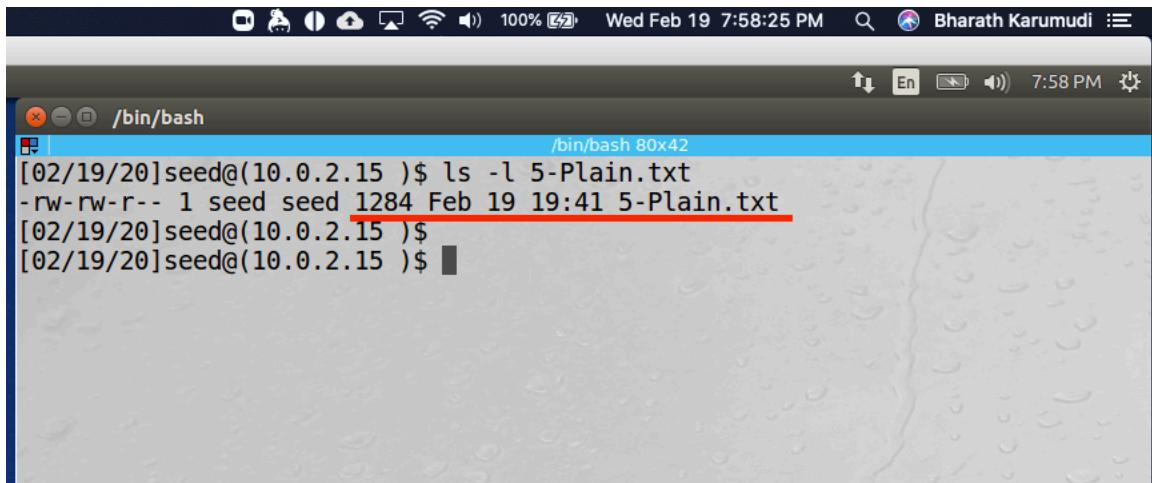
Before starting the task, I assume by corrupting the 55th byte of an encrypted file will result as follows while decrypting for specific modes:

Electronic Code Block – The corrupted bit block will be corrupted during decryption and no impact to others.

Cipher Block Chaining - The corrupted bit block will be corrupted during decryption and no impact to others.

Cipher Feedback – The corrupted bit and the following block will be impacted during decryption.

Output Feedback – Only the corrupted bit will be impacted during decryption.



The screenshot shows a terminal window titled '/bin/bash' running on a desktop environment. The terminal displays the command 'ls -l 5-Plain.txt' and its output. The output shows a file named '5-Plain.txt' with a size of 1284 bytes, which is highlighted with a red underline. The terminal window has a dark theme with light-colored text. The desktop background is visible behind the window.

```
[02/19/20]seed@(10.0.2.15 )$ ls -l 5-Plain.txt
-rw-rw-r-- 1 seed seed 1284 Feb 19 19:41 5-Plain.txt
[02/19/20]seed@(10.0.2.15 )$
```

Fig1: A plain text file created with 1284 bytes

[After Lab4] [Running]

```
/bin/bash
[02/19/20]seed@(10.0.2.15 )$ ls -l 5-Plain.txt
-rw-rw-r-- 1 seed seed 1284 Feb 19 19:41 5-Plain.txt
[02/19/20]seed@(10.0.2.15 )$
[02/19/20]seed@(10.0.2.15 )$ hexdump -C 5-Plain.txt
00000000  4f 6e 65 20 6d 6f 72 6e 69 6e 67 2c 20 77 68 65 | One morning, whe
00000010  6e 20 47 72 65 67 6f 72 20 53 61 6d 73 61 20 77 | n Gregor Samsa w
00000020  6f 6b 65 20 66 72 6f 6d 20 74 72 6f 75 62 6c 65 | oke from trouble
00000030  64 20 64 72 65 61 6d 73 2c 20 68 65 20 66 6f 75 | d dreams, he fou
00000040  6e 64 20 68 69 6d 73 65 6c 66 20 74 72 61 6e 73 | nd himself trans
00000050  66 6f 72 6d 65 64 20 69 6e 20 68 69 73 20 62 65 | formed in his be
00000060  64 20 69 6e 74 6f 20 61 20 68 6f 72 72 69 62 6c | d into a horribl
00000070  65 20 76 65 72 6d 69 6e 2e 20 48 65 20 6c 61 79 | e vermin. He lay
00000080  20 6f 6e 20 68 69 73 20 61 72 6d 6f 75 72 2d 6c | on his armour-l
00000090  69 6b 65 20 62 61 63 6b 2c 20 61 6e 64 20 69 66 | ike back, and if
000000a0  20 68 65 20 6c 69 66 74 65 64 20 68 69 73 20 68 | he lifted his h
000000b0  65 61 64 20 61 20 6c 69 74 74 6c 65 20 68 65 20 | ead a little he
000000c0  63 6f 75 6c 64 20 73 65 65 20 68 69 73 20 62 72 | could see his br
000000d0  6f 77 6e 20 62 65 6c 6c 79 2c 20 73 6c 69 67 68 | own belly, slight
000000e0  74 6c 79 20 64 6f 6d 65 64 20 61 6e 64 20 64 69 | ly domed and di
000000f0  76 69 64 65 64 20 62 79 20 61 72 63 68 65 73 20 | vided by arches
00000100  69 6e 74 6f 20 73 74 69 66 66 20 73 65 63 74 69 | into stiff secti
00000110  6f 6e 73 2e 20 54 68 65 20 62 65 64 64 69 6e 67 | ons. The bedding
00000120  20 77 61 73 20 68 61 72 64 6c 79 20 61 62 6c 65 | was hardly able
00000130  20 74 6f 20 63 6f 76 65 72 20 69 74 20 61 6e 64 | to cover it and
00000140  20 73 65 65 6d 65 64 20 72 65 61 64 79 20 74 6f | seemed ready to
00000150  20 73 6c 69 64 65 20 6f 66 66 20 61 6e 79 20 6d | slide off any m
00000160  6f 6d 65 6e 74 2e 20 48 69 73 20 6d 61 6e 79 20 | oment. His many
00000170  6c 65 67 73 2c 20 70 69 74 69 66 75 6c 6c 79 20 | legs, pitifully
00000180  74 68 69 6e 20 63 6f 6d 70 61 72 65 64 20 77 69 | thin compared wi
00000190  74 68 20 74 68 65 20 73 69 7a 65 20 6f 66 20 74 | th the size of t
000001a0  68 65 20 72 65 73 74 20 6f 66 20 68 69 6d 2c 20 | he rest of him,
000001b0  77 61 76 65 64 20 61 62 6f 75 74 20 68 65 6c 70 | waved about help
000001c0  6c 65 73 73 6c 79 20 61 73 20 68 65 20 6c 6f 6f | lessly as he loo
000001d0  6b 65 64 2e 20 57 68 61 74 20 68 61 70 70 65 6e | ked. What happen
000001e0  65 64 20 74 6f 20 6d 65 20 68 65 20 74 68 6f 75 | ed to me he thou
000001f0  67 68 74 2e 20 49 74 20 77 61 73 6e 27 74 20 61 | ght. It wasn't a
00000200  20 64 72 65 61 6d 2e 20 48 69 73 20 72 6f 6d 6d | dream. His room
00000210  2c 20 61 20 70 72 6f 70 65 72 20 68 75 6d 61 6e | , a proper human
00000220  20 72 6f 6f 6d 20 61 6c 74 68 6f 75 67 68 20 61 | room although a
00000230  20 6c 69 74 74 6c 65 20 74 6f 6f 20 73 6d 61 6c | little too smal
00000240  6c 2c 20 6c 61 79 20 70 65 61 63 65 66 75 6c 6c | l, lay peacefully
00000250  79 20 62 65 74 77 65 65 6e 20 69 74 73 20 66 6f | y between its fo
```

Fig2: View of Plain text file with hexdump



The image shows a screenshot of a Linux terminal window titled "/bin/bash". The terminal is running on a blue-themed desktop environment. The terminal's title bar also displays "(After Lab4) [Running]". The terminal window contains the following command-line session:

```
[02/19/20]seed@(10.0.2.15 )$ ls -l 5-Plain.txt  
-rw-rw-r-- 1 seed seed 1284 Feb 19 19:41 5-Plain.txt  
[02/19/20]seed@(10.0.2.15 )$  
[02/19/20]seed@(10.0.2.15 )$ openssl enc -aes-128-ecb -e -out 5-cipher-aes-128-e  
cb-orig.bin -in 5-Plain.txt -K 00112233445566778889aabbccddeeff  
[02/19/20]seed@(10.0.2.15 )$
```

Fig3: Encrypted the plain text with ECB

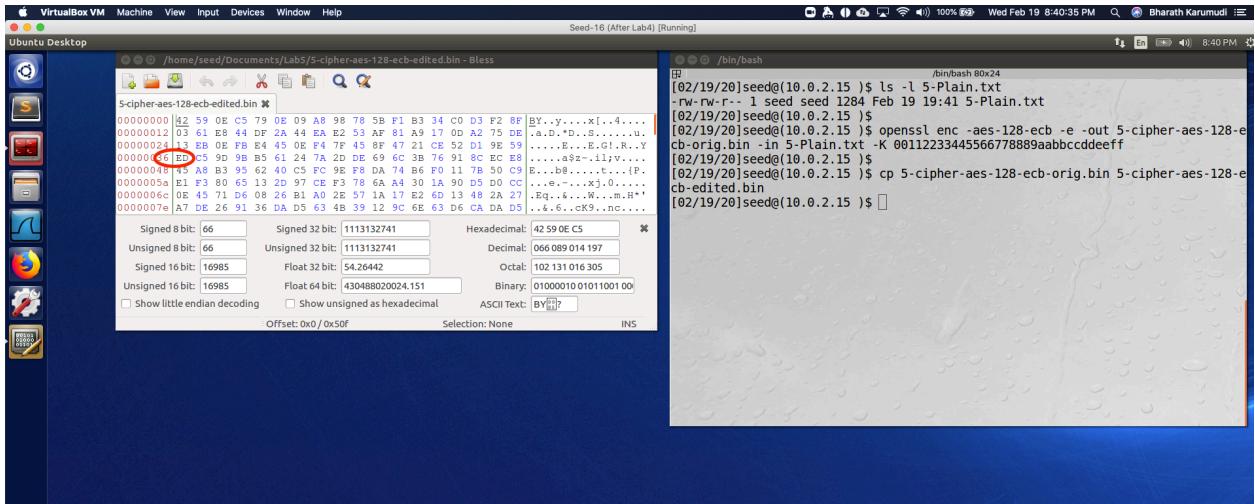


Fig4: ECB encrypted binary file in bless and highlighted the 55th byte which has ED

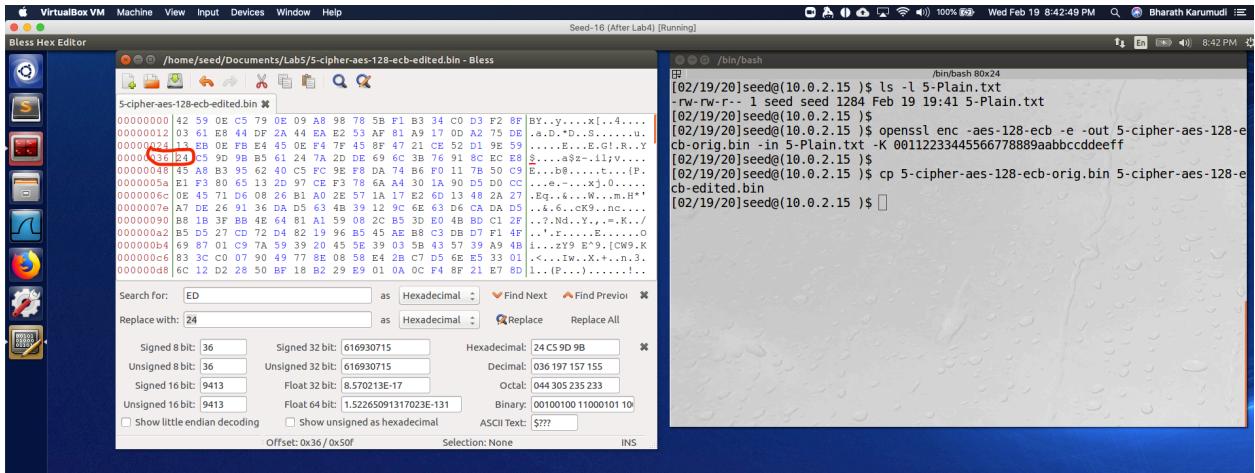


Fig5: Modified the 55th byte to 0x24

```
000000510
[02/19/20]seed@(10.0.2.15 )$ clear
[02/19/20]seed@(10.0.2.15 )$ openssl enc -aes-128-ecb -d -out 5-plain-corrupted.txt -in 5-cipher-aes-128-ecb-edited.bin -K 00112233445566778889aabcccddeeff
[02/19/20]seed@(10.0.2.15 )$
[02/19/20]seed@(10.0.2.15 )$ hexdump -C 5-plain-corrupted.txt
00000000  4f 6e 65 20 6d 6f 72 6e  69 6e 67 2c 20 77 68 65 |One morning, whe|
00000010  6e 20 47 72 65 67 6f 72  20 53 61 6d 73 61 20 77 |n Gregor Samsa w|
00000020  6f 6b 65 20 66 72 6f 6d  20 74 72 6f 75 62 6c 65 |oke from trouble|
00000030  b1 a7 f7 01 bc ee ef 5c  b8 e4 fd 86 7b 6a ed fc |.....\....{j..|
00000040  6e 64 20 68 69 6d 73 65  6c 66 20 74 72 61 6e 73 |nd himself trans|
00000050  66 6f 72 6d 65 64 20 69  6e 20 68 69 73 20 62 65 |formed in his be|
00000060  64 20 69 6e 74 6f 20 61  20 68 6f 72 72 69 62 6c |d into a horribl|
00000070  65 20 76 65 72 6d 69 6e  2e 20 48 65 20 6c 61 79 |e vermin. He lay|
00000080  20 6f 6e 20 68 69 73 20  61 72 6d 6f 75 72 2d 6c |on his armour-l|
00000090  69 6b 65 20 62 61 63 6b  2c 20 61 6e 64 20 69 66 |ike back, and if|
000000a0  20 68 65 20 6c 69 66 74  65 64 20 68 69 73 20 68 |he lifted his h|
000000b0  65 61 64 20 61 20 6c 69  74 74 6c 65 20 68 65 20 |ead a little he|
000000c0  63 6f 75 6c 64 20 73 65  65 20 68 69 73 20 62 72 |could see his br|
000000d0  6f 77 6e 20 62 65 6c 6c  79 2c 20 73 6c 69 67 68 |own belly, sligh|
000000e0  74 6c 79 20 64 6f 6d 65  64 20 61 6e 64 20 64 69 |tly domed and di|
000000f0  76 69 64 65 64 20 62 79  20 61 72 63 68 65 73 20 |vided by arches|
00000100  69 6e 74 6f 20 73 74 69  66 66 20 73 65 63 74 69 |into stiff secti|
```

Fig6: Decrypted the file with ECB and can notice the corrupted block

The screenshot shows a terminal window titled '/bin/bash' running on a Linux desktop environment. The terminal displays the following command and its output:

```
[02/19/20]seed@(10.0.2.15 )$ openssl enc -aes-128-cbc -e -out 5-cipher-aes-128-cbc-orig.bin -in 5-Plain.txt -K 00112233445566778889aabbccddeeff -iv 0102030405060708
[02/19/20]seed@(10.0.2.15 )$ bless 5-cipher-aes-128-cbc-orig.bin
Unexpected end of file has occurred. The following elements are not closed: pref , preferences. Line 22, position 36.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/plugins' not found.
Could not find file "/home/seed/.config/bless/export_patterns".
Could not find file "/home/seed/.config/bless/history.xml".
Document does not have a root element.
Sharing violation on path /home/seed/.config/bless/preferences.xml
Sharing violation on path /home/seed/.config/bless/preferences.xml
Sharing violation on path /home/seed/.config/bless/preferences.xml
Document does not have a root element.

(bless:2659): GLib-CRITICAL **: Source ID 1958 was not found when attempting to remove it

(bless:2659): GLib-CRITICAL **: Source ID 1959 was not found when attempting to remove it
```

At the bottom of the terminal, another command is shown:

```
[02/19/20]seed@(10.0.2.15 )$ openssl enc -aes-128-cbc -d -in 5-cipher-aes-128-cbc-orig.bin -out 5-Plain-corrupted-cbc.txt -K 00112233445566778889aabbccddeeff -iv 0102030405060708
```

Fig7: Encryption with CBC and corrupting with Bless and decrypting the file

```

[02/19/20]seed@(10.0.2.15)$ hexdump -C 5-Plain-corrupted-cbc.txt
00000000  4f 6e 65 20 6d 6f 72 6e  69 6e 67 2c 20 77 68 65 |One morning, whe|
00000010  6e 20 47 72 65 67 6f 72  20 53 61 6d 73 61 20 77 |n Gregor Samsa w|
00000020  6f 6b 65 20 66 72 6f 6d  20 74 72 6f 75 62 6c 65 |oke from trouble|
00000030  11 41 8f 50 6b 14 fd b5  d9 06 12 c3 d6 e9 6c e0 |.A.Pk.....|
00000040  6e 64 20 68 69 6d e4 65  6c 66 20 74 72 61 6e 73 |nd him.etc trans|
00000050  66 6f 72 6d 65 64 20 69  6e 20 68 69 73 20 62 65 |formed in his be|
00000060  64 20 69 6e 74 6f 20 61  20 68 6f 72 72 69 62 6c |d into a horribl|
00000070  65 20 76 65 72 6d 69 6e  2e 20 48 65 20 6c 61 79 |e vermin. He lay|
00000080  20 6f 6e 20 68 69 73 20  61 72 6d 6f 75 72 2d 6c |on his armour-l|
00000090  69 6b 65 20 62 61 63 6b  2c 20 61 6e 64 20 69 66 |ike back, and if|
000000a0  20 68 65 20 6c 69 66 74  65 64 20 68 69 73 20 68 |he lifted his h|
000000b0  65 61 64 20 61 20 6c 69  74 74 6c 65 20 68 65 20 |ead a little he|
000000c0  63 6f 75 6c 64 20 73 65  65 20 68 69 73 20 62 72 |could see his br|
000000d0  6f 77 6e 20 62 65 6c 6c  79 2c 20 73 6c 69 67 68 |own belly, slight|
000000e0  74 6c 79 20 64 6f 6d 65  64 20 61 6e 64 20 64 69 |ly domed and di|
000000f0  76 69 64 65 64 20 62 79  20 61 72 63 68 65 73 20 |vided by arches|
00000100  69 6e 74 6f 20 73 74 69  66 66 20 73 65 63 74 69 |into stiff secti|
00000110  6f 6e 73 2e 20 54 68 65  20 62 65 64 64 69 6e 67 |ons. The bedding|
00000120  20 77 61 73 20 68 61 72  64 6c 79 20 61 62 6c 65 |was hardly able|
00000130  20 74 6f 20 63 6f 76 65  72 20 69 74 20 61 6e 64 |to cover it and|
00000140  20 73 65 65 6d 65 64 20  72 65 61 64 79 20 74 6f |seemed ready to|
00000150  20 73 6c 69 64 65 20 6f  66 66 20 61 6e 79 20 6d |slide off any m|
00000160  6f 6d 65 6e 74 2e 20 48  69 73 20 6d 61 6e 79 20 |oment. His many|

```

Fig8: Decrypted the file with CBC and can notice the corrupted block

```

[02/19/20]seed@(10.0.2.15)$ openssl enc -aes-128-cfb -e -out 5-cipher-aes-128-cfb.bin -in 5-Plain.txt -K 00112233445566778899aabccdddeeff -iv 0102030405060708
[02/19/20]seed@(10.0.2.15)$ 
[02/19/20]seed@(10.0.2.15)$ 
[02/19/20]seed@(10.0.2.15)$ 
[02/19/20]seed@(10.0.2.15)$ openssl enc -aes-128-cfb -d -out 5-plain-corrupted-cfb.txt -in 5-cipher-aes-128-cfb.bin -K 00112233445566778899aabccdddeeff -iv 0102030405060708
[02/19/20]seed@(10.0.2.15)$ 

```

Fig9: Encryption with CFB and corrupting with Bless and decrypting the file

```
[02/19/20]seed@(10.0.2.15)$ openssl enc -aes-128-cfb -e -out 5-cipher-aes-128-cfb.bin -in 5-Plain.txt -K 00112233445566778889aabbccddeeff -iv 0102030405060708
[02/19/20]seed@(10.0.2.15)$
[02/19/20]seed@(10.0.2.15)$
[02/19/20]seed@(10.0.2.15)$ openssl enc -aes-128-cfb -d -out 5-plain-corrupted-cfb.txt -in 5-cipher-aes-128-cfb.bin -K 00112233445566778889aabbccddeeff -iv 0102030405060708
[02/19/20]seed@(10.0.2.15)$ hexdump -C 5-plain-corrupted-cfb.txt
00000000  4f 6e 65 20 6d 6f 72 6e  69 6e 67 2c 20 77 68 65 |One morning, whe|
00000010  6e 20 47 72 65 67 6f 72  20 53 61 6d 73 61 20 77 |n Gregor Samsa w|
00000020  6f 6b 65 20 66 72 6f 6d  20 74 72 6f 75 62 6c 65 |oke from trouble|
00000030  64 20 64 72 65 61 43 73  2c 20 68 65 20 66 6f 75 |d dreamt, he fou|
00000040  cd 59 5e 14 31 47 dd 2b  d3 6c e1 f8 ad 5a 90 b9 |l.Y^..1G.+.l...Z..|
00000050  66 6f 72 6d 65 64 20 69  6e 20 68 69 73 20 62 65 |formed in his be|
00000060  64 20 69 6e 74 6f 20 61  20 68 6f 72 72 69 62 6c |d into a horribl|
00000070  65 20 76 65 72 6d 69 6e  2e 20 48 65 20 6c 61 79 |e vermin. He lay|
00000080  20 6f 6e 20 68 69 73 20  61 72 6d 6f 75 72 2d 6c |on his armour-l|
00000090  69 6b 65 20 62 61 63 6b  2c 20 61 6e 64 20 69 66 |ike back, and if|
000000a0  20 68 65 20 6c 69 66 74  65 64 20 68 69 73 20 68 |he lifted his h|
000000b0  65 61 64 20 61 20 6c 69  74 74 6c 65 20 68 65 20 |ead a little he|
000000c0  63 6f 75 6c 64 20 73 65  65 20 68 69 73 20 62 72 |could see his br|
000000d0  6f 77 6e 20 62 65 6c 6c  79 2c 20 73 6c 69 67 68 |own belly, sligh|

```

Fig10: Decrypted the file with CFB and can notice the corrupted bit and block

```
[02/19/20]seed@(10.0.2.15)$ openssl enc -aes-128-ofb -e -out 5-cipher-aes-128-ofb.bin -in 5-Plain.txt -K 00112233445566778889aabbccddeeff -iv 0102030405060708
[02/19/20]seed@(10.0.2.15)$
[02/19/20]seed@(10.0.2.15)$ openssl enc -aes-128-ofb -d -out 5-plain-corrupted-ofb.txt -in 5-cipher-aes-128-ofb.bin -K 00112233445566778889aabbccddeeff -iv 0102030405060708
[02/19/20]seed@(10.0.2.15)$
[02/19/20]seed@(10.0.2.15)$
[02/19/20]seed@(10.0.2.15)$

```

Fig11: Encryption with OFB and corrupting with Bless and decrypting the file

```
fb.bin -in 5-Plain.txt -K 00112233445566778889aabccddeeff -iv 0102030405060708
[02/19/20]seed@(10.0.2.15 )$ openssl enc -aes-128-ofb -d -out 5-plain-corrupted-ofb.txt -in 5-cipher-aes-128-ofb.bin -K 00112233445566778889aabccddeeff -iv 0102030405060708
[02/19/20]seed@(10.0.2.15 )$ hexdump -C 5-plain-corrupted-ofb.txt
00000000  4f 6e 65 20 6d 6f 72 6e  69 6e 67 2c 20 77 68 65 |One morning, whe|
00000010  6e 20 47 72 65 67 6f 72  20 53 61 6d 73 61 20 77 |n Gregor Samsa w|
00000020  6f 6b 65 20 66 72 6f 6d  20 74 72 6f 75 62 6c 65 |oke from trouble|
00000030  64 20 64 72 65 61 c1 73  2c 20 68 65 20 66 6f 75 |d drea.s, he fou|
00000040  6e 64 20 68 69 6d 73 65  6c 66 20 74 72 61 6e 73 |nd himself trans|
00000050  66 6f 72 6d 65 64 20 69  6e 20 68 69 73 20 62 65 |formed in his be|
00000060  64 20 69 6e 74 6f 20 61  20 68 6f 72 72 69 62 6c |d into a horribl|
00000070  65 20 76 65 72 6d 69 6e  2e 20 48 65 20 6c 61 79 |e vermin. He lay|
00000080  20 6f 6e 20 68 69 73 20  61 72 6d 6f 75 72 2d 6c |on his armour-l|
00000090  69 6b 65 20 62 61 63 6b  2c 20 61 6e 64 20 69 66 |ike back, and if|
000000a0  20 68 65 20 6c 69 66 74  65 64 20 68 69 73 20 68 |he lifted his h|
000000b0  65 61 64 20 61 20 6c 69  74 74 6c 65 20 68 65 20 |ead a little he|
000000c0  63 6f 75 6c 64 20 73 65  65 20 68 69 73 20 62 72 |could see his br|
000000d0  6f 77 6e 20 62 65 6c 6c  79 2c 20 73 6c 69 67 68 |own belly, sligh|
000000e0  74 6c 79 20 64 6f 6d 65  64 20 61 6e 64 20 64 69 |tly domed and di|
000000f0  76 69 64 65 64 20 62 79  20 61 72 63 68 65 73 20 |vided by arches|
00000100  69 6e 74 6f 20 73 74 69  66 66 20 73 65 63 74 69 |into stiff secti|
```

Fig12: Decrypted the file with OFB and can notice the corrupted bit

Observation: Encrypted the plaintext (5-Plain.txt) using four different AES block cipher modes – ECB, CBC, CFB and OFB. Once encrypted, modified the 55th byte to 0x24 and then decrypted the files back. The decrypted files in the four experiments shows different results. In ECB mode the entire block that contained the corrupted byte was lost. In CBC mode, the entire block plus one byte in the following block was lost. Using CFB, only the byte that we changed was lost in the block, but the entire following block was lost. And finally using OFB, only the byte that we changed was lost.

Explanation: Data corruption errors propagate in various modes of AES encryption differently. In OFB mode only the corrupted byte that is lost, in other modes the entire block is lost, or the proceeding for following blocks are affected as well. The differences are due to how XOR and Initialization Vectors are implemented in the different modes of AES cipher.