

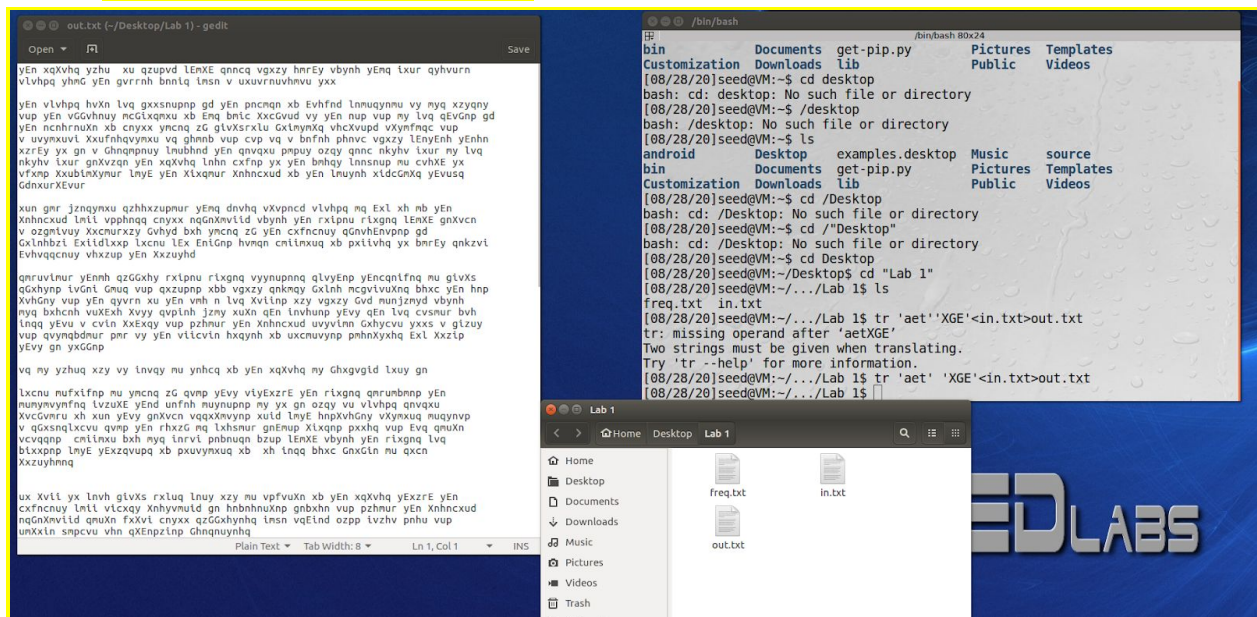
## Overview Secret Key Encryption

The purpose of this lab is to learn encryption and decryption techniques and how they can be broken. We will encrypt, decrypt and learn common mistakes and how some of the techniques can be exploited.

### TASK 1: FREQUENCY ANALYSIS

In task 1, we will be using frequency analysis to decrypt ciphertexts that are given to us by the lab. We are already given a ciphertext and are tasked with using frequency analysis to decipher. All of the text is lowercase, and our output will be in uppercase, which makes deciphering the text easier in the long run.

**\$ tr 'aet' 'XGE' < in.txt > out.txt**



After running the command all of the a,e,t were replaced with X,G,E and we assume this is a common word like the, or similar because of the high frequency of its appearance in the output file. We ran a frequency analysis on the ciphertext and then replaced the highest occurring scrambled letters with the highest occurring letters in order. We kept repeating this process by initially replacing vowels and started to identify keywords that were capable of being read with a few missing letters. We repeated this method until we started decrypting full words. Each decryption process we



ytn xqavhq yzhu xu qzupvd lmat qnnqc vxgzy hmrty vbynh ytmq ixur qyhvum  
vlvhpq yhme ytn gyrrnh bnniq imsn v uxuvmuvhmvu yxx

ytn vlvhpq hvan lvq gxsnupnp gd ytn pncmqn xb tvhfnid lmuqynmu vy myq xzyqny  
vup ytn veevhny mceixqmxu xb tmq bmic axcevud vy ytn nup vup my lvq qtenp gd  
ytn ncnhmuan xb cnyyx ymcnq ze givasrxlu eximymaq vhcavupd vaymfmqc vup  
v uvymxuvi axufnhqymxu vq ghmb vup cvp vq v bnfth phnvc vxgzy ltnytnh ytnhn  
xzrty yx gn v ehqmpnuy lmubhnd ytn qnvqxu pmpuy ozqy qnnc nkyhv ixur my lvq  
nkyhv ixur gnavzqn ytn xqavhq lnhn cxfnp yx ytn bmqh Innsup mu cvhat yx  
vfxmp axubimaymur lmyt ytn aixqmur anhnxcud xb ytn lmuynh xidcemaq ytvusq  
ednxuratvur

xun gmr jznqymxu qzhxhzupmur ytmq dnvqh vavpncd vlvhpq mq bdi xh mb ytn  
anhncxud lmiil vpphnqy cnyyx nqenamviid vbynh ytn rxipnu rixgnq lmat gnacn  
v ozgmivuy axcmurxzy evhyd bxh ymcnq ze ytn cxfncnuy qenvhtnvpnp gd  
exlnhbzi txiidbpx lxcnu ltx tnienp hvmqn cmilmxuq xb pxliivhq yx bmrty qnkzvi  
tvhvqqcnuy vhxzup ytn axzuyhd

qmruvimur ytnmh qzeexhy rxipnu rixgnq vyynupnq qlvytnp ytnqcniifnq mu givas  
qexhTEP iveEi emuq vup qxzupE xbb vxgzt qEkmqT exlEH mcgvivuaEq bhxc THE hEP  
avheET vup THE qTVrE xu THE vmh E lvq avilEP xzt vxgzt evd muEjzmTd vBTEh  
mTq bxhCEH vuaHxh avTT qpPiEH jzmT xuaE qHE iEvhuEP THVT qHE lvq cvsmur bvh  
iEqq THvu v cvIE axHxqT vup pzhmur THE aHEcXud uvTVimE exhTcvu Txxs v gizUT  
vup qvTmqbmdur pmr vT THE vliEvT hXqTEH xb uxcmuvTEP pmhEaTxhq Hxl axzip  
THVT gE TxeEgP

Letter Density	
N	488 (12%)
Y	373 (9%)
V	348 (9%)
X	291 (7%)
U	280 (7%)
Q	276 (7%)
M	264 (7%)
H	235 (6%)
T	183 (5%)
I	166 (4%)

Word Count  
Writing Mistakes  
Plagiarism

```
08/28/20]seed@VM:~/.../Lab 1$ tr 'aet' 'XGE' < in.txt > out.txt
08/28/20]seed@VM:~/.../Lab 1$ tr 'ytn' 'THE' < in.txt > out.txt
08/28/20]seed@VM:~/.../Lab 1$ tr 'ytnv' 'THEA' < in.txt > out.txt
08/28/20]seed@VM:~/.../Lab 1$ tr 'ytnviq' 'THEALS' < in.txt > out.txt
08/28/20]seed@VM:~/.../Lab 1$ tr 'ytnviqc' 'THEALSD' < in.txt > out.txt
08/28/20]seed@VM:~/.../Lab 1$ tr 'ytn' 'THE' < in.txt > out.txt
08/28/20]seed@VM:~/.../Lab 1$ tr 'ytnh' 'THER' < in.txt > out.txt
08/28/20]seed@VM:~/.../Lab 1$ tr 'ytnhx' 'THERO' < in.txt > out2.txt
08/28/20]seed@VM:~/.../Lab 1$ tr 'ytnhxl' 'THEROW' < in.txt > out3.txt
08/28/20]seed@VM:~/.../Lab 1$ tr 'ytnhxl' 'THEROWA' < in.txt > out4.txt
08/28/20]seed@VM:~/.../Lab 1$ tr 'ytnhxl' 'THEROWAF' < in.txt > out5.txt
08/28/20]seed@VM:~/.../Lab 1$ tr 'ytnhxl' 'THEROWAFI' < in.txt > out6.txt
08/28/20]seed@VM:~/.../Lab 1$ tr 'ytnhxl' 'THEROWAFISN' < in.txt > out7.txt
08/28/20]seed@VM:~/.../Lab 1$ tr 'ytnhxl' 'THEROWAFISNUL' < in.txt > out
.txt
08/28/20]seed@VM:~/.../Lab 1$ tr 'ytnhxl' 'THEROWAFISNULPMD' < in.txt > out9.txt
08/28/20]seed@VM:~/.../Lab 1$ tr 'ytnhxl' 'THEROWAFISNULPMDCKG' < in.txt > out10.txt
08/28/20]seed@VM:~/.../Lab 1$ tr 'ytnhxl' 'THEROWAFISNULPMDCKGBV' < in.txt > out11.tx
08/28/20]seed@VM:~/.../Lab 1$ tr 'ytnhxl' 'THEROWAFISNULPMDCKGBVYXJ' < in.txt > ou
11.txt
08/28/20]seed@VM:~/.../Lab 1$ tr 'ytnhxl' 'THEROWAFISNULPMDCKGBVYXJQ' < in.txt >
ut12.txt
```

3 TURN ON SOUNP WHICH SEELS AGOUT RHTI AFTER THIS LONI STRAME  
Ie THE gARRER FEELS LISe A NONARENARIAN TOO

S RAaE WAS gOoSEnPEp gd THE pECISE OF HARFEd WEINSTEIN AT ITS OUTSET  
eeAREnt IceLOSION OF HIS FILC aOceAnd AT THE ENp ANp IT WAS SHAEp gd  
ENaE OF cETOO TICES Ue gLAAsROWN eOLITIAS ARCaAnPd AaTtIfISC ANp  
L aONFERASION aS gRIEF ANp cAp aS A fEFeR pREAc AGout WHETHER THERE  
gE a ERESIPENT WINFREd THE SEASON pINpt ouST SEEC EKTRA LONr IT WAS  
r gEAUSE THE OSaARS WERE cOfEP TO THE FIRST WEESEnP IN cARaH TO  
fLIaTInr WITH THE aLOSInr aERECOND OF THE WINTER OldceIaS THANsS  
Nr

UESTION SURROUnPinr THIS DEARS AaApEcd AWARps IS HOW OR IF THE  
WILL AppRESS cETOO ESeEaIALLd AFTER THE rOLPEN rLOGES WHIaH gEAACE  
T aOCInROUT eARTd FOR TICES Ue THE cOfECENT SeEARHEApEp gd  
HOLLdWOOp WOCen WHO HELEp RAISE cILLIONS OF pOLLARS TO FirHT SEKUAL  
T AROUnP THE aOUNTRd

THEIR SUEeORT rOLPEN rLOGES ATTENPEES SWATHEP THEcSELFES IN gLAAs  
AeEL eINS ANP SOUNPEp OFF AGout SEKIST eOWER IcgALANaES FroC THE Rep  
p THE STaRE ON THE AIR E WAS aALLEp OUT AGout eAd INEJUITd AFTER  
R ANaHOR aATT SAPler JUIT ONaE SHE LEARNep THAT SHE WAS cASInr FAR  
A CALE aOHST ANp PURInr THE aERECOND NATALIE eORTcAN TOOs A gLUNT  
FdInr pIr AT THE ALLcALE ROSTER OF NOCINATEP pIREaTORS HOW aOULP  
DeeEp

NS OUT AT LEAST IN TERCS OF THE OSaARS IT eROgAgLd WONT gE

OLfEp IN TICES Ue SAIP THAT ALTHOUrH THE rLOGES SIrNIFIEp THE  
ES LAUNaH THEd NEFER INTENPEp IT TO gE ouST AN AWARps SEASON  
OR ONE THAT gEAACE ASSOaIATEP ONLd WITH REpaAREET AaTIONS INSTEAP  
OCAN SAIP THE rROUE IS WORsInr gEHInP aLOSEP pOORS ANP HAS SINaE  
cILLION FOR ITS LErAL pEFENSE FUNP WHIaH AFTER THE rLOGES WAS  
ITH THOUSAnPs OF pONATIONS OF OR LESS FroC eEOeLE IN SOcE

lTHE xqavhq Tzhu xu qzupvd lHmaH qEEcq vxgzt hmrHT vBTEh THmq ixur qThvurE  
vlvhpq Thme THE gyrrEH bEEIq imSE v uxuvrEuVhmvu Txx

THE vlvhpq hvaE lvq gxssEupEp gd THE pECmqE xb HvHfEd lEmuqTEmu vT mTq xztqET  
vup THE veevhEuT mceixqmxu xb Hmq bmic axcevud vT THE Eup vup mT lvq qHveEp gd  
THE EcEhrEuaE xb cETxx TmcEq ze givasrxlu eximTmaq vhcavupd vaTmfmc vup  
v uvTmxuvi axufehqvTmxu vq ghmb vup cvp vq v BEfEH phEvc vxgzt LHETHEh THEhE  
xzrHT Tx gE v ehEqmpEuT lmubhEd THE qEvqxu pmpuT ozqT qEEc EkThv ixur mT lvq  
EkThv ixur gEavzqE THE xqavhq lEHc cxEP Tx THE bmqhT lEESEup mu cvhaH Tx  
vfxmp axubimaTmur lMTH THE aixqmur aHEcXud xb THE lmuTEh xidcemaq THvusq  
edExuraHvur

xuE gmr jzEqTmxu qzhxhzupmur THmq dEvqh vavpEcd vlvhpq mq Hxl xh mb THE  
aHEcXud lmiil vppHEqq cETxx EgeEanviid vBTEh THE rxipEu rixgEq lHmaH gEavCE  
v ozgmivUT axcmurxzt evhTd bxh TmcEq ze THE cxFEcEuT qEvHHEvPEp gd  
exlEHbzi Hxiidlxxp lxcEu lHx HEIEp hvmqE cmilmxuq xb pxliivhq Tx bmrHT qEKzvi  
HvhvqqcEuT vhxzup THE axzuThd

qmruvimur THEmh qzeexht rxipEu rixgEq vTEupEEq qlvTHEP THEcQEIfEq mu givas  
qexhTEP iveEi emuq vup qxzupE xbb vxgzt qEkmqT exlEH mcgvivuaEq bhxc THE hEP  
avheET vup THE qTVrE xu THE vmh E lvq avilEP xzt vxgzt evd muEjzmTd vBTEh  
mTq bxhCEH vuaHxh avTT qpPiEH jzmT xuaE qHE iEvhuEP THVT qHE lvq cvsmur bvh  
iEqq THvu v cvIE axHxqT vup pzhmur THE aHEcXud uvTVimE exhTcvu Txxs v gizUT  
vup qvTmqbmdur pmr vT THE vliEvT hXqTEH xb uxcmuvTEP pmhEaTxhq Hxl axzip  
THVT gE TxeEgP

vq mT Tzhuq xzt vT iEvqT mu TEhcq xb THE xqavhq mT ehxgvgid lxuT gE

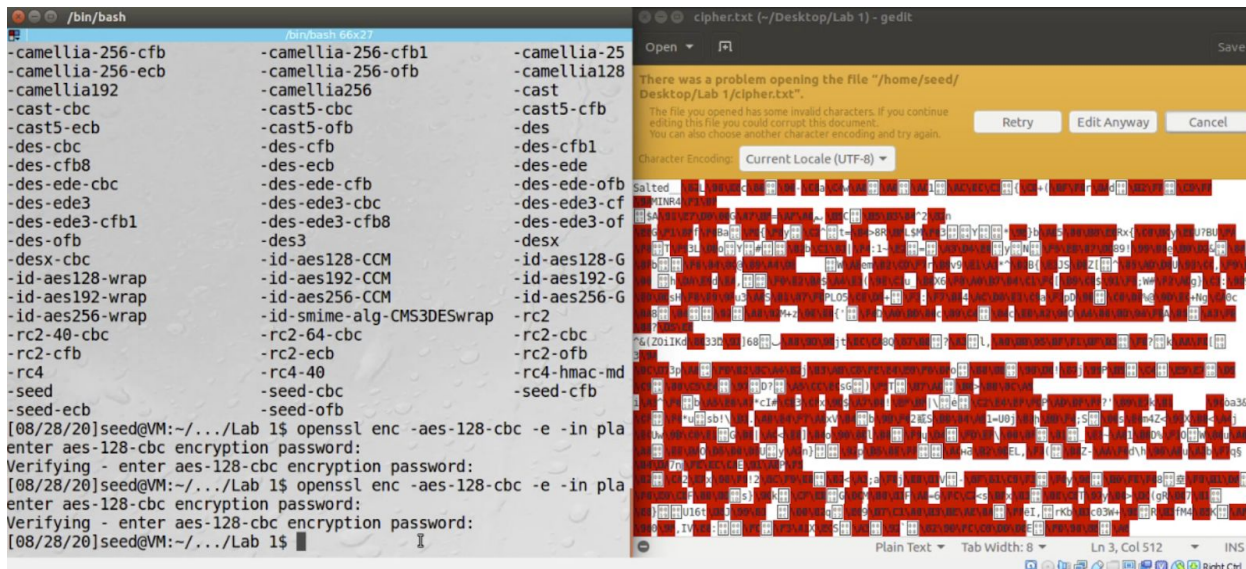
lxcEu mufxifEp mu TmcEq ze qvmp THVT viTHxzrH THE rixgEq qmrumbEp THE  
munTmvTmfEq izvuaH THEd uFEh muTEupEp mT Tx gE ozqT vu vlvhpq qEvqxu  
avcevmru xh xuE THVT gEavCE vqxmavTEP xuid lMTH hEPavheET vaTmxuq muqTEvp  
v qexsEqLxcvu qvmp THE rhxze mq lxhsmur gEHmup aixqEP pxxhq vup Hvq qmuAE  
vcvqqEP cmilmxu bxh mTq iErvi pEBEuqE bzup lHmaH vBTEh THE rixgEq lvq  
bixxpEP lMTH THxzvupq xb pxuvTmxuq xb xh iEqq bhxc eEXeIE mu qxCE



outputted a new text file every time so we could backtrack if any mistakes were made in the decryption process. After successfully decrypting the text file it took us about 12 steps of this method. The resulting decrypted text file was an article about hollywood.

## TASK 2: Encryption using different ciphers and modes

Basically we encrypted a plaintext with an aes 128 and opened the ciphertext and saw how it all is a ciphertext and unreadable.



## TASK 3: Encryption mode -ECB vs CBC

The picture given to us we had to encrypt. We used aes 128 ecb and cbc to encrypt the file and then we modified the binary files headers and the new encrypted file we got was encrypted and the original picture was changed. ECB seemed to only change the color, while CBC basically encrypted the entire image and it can't be seen at all. We also used the *bless* hex editor to manually change the first 54 header bits of both encrypted files.

```
[08/28/20]seed@VM:~/.../Lab 1$ openssl enc -aes-256-ecb -e -in pic_original.bmp -out aes_256_ecb.bmp -k 012345
[08/28/20]seed@VM:~/.../Lab 1$ openssl enc -aes-256-cbc -e -in pic_original.bmp -out aes_256_cbc.bmp -k 012345 -iv 0102030405060708
```

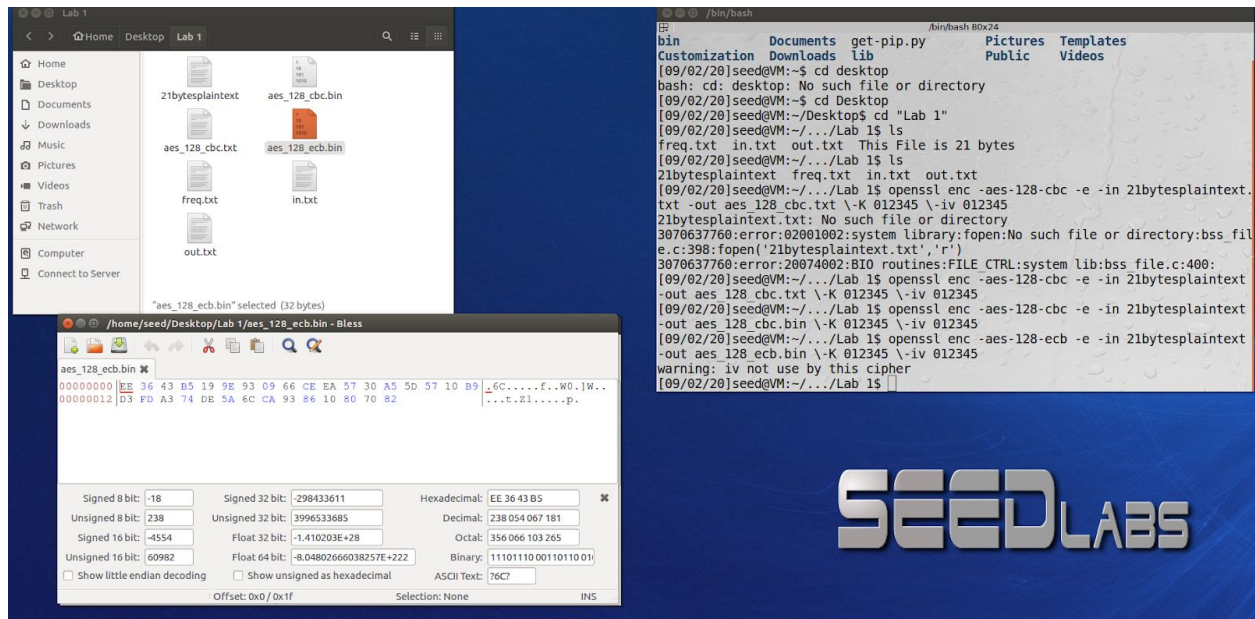
```
$ head -c 54 p1.bmp > header
$ tail -c +55 p2.bmp > body
$ cat header body > new.bmp
```



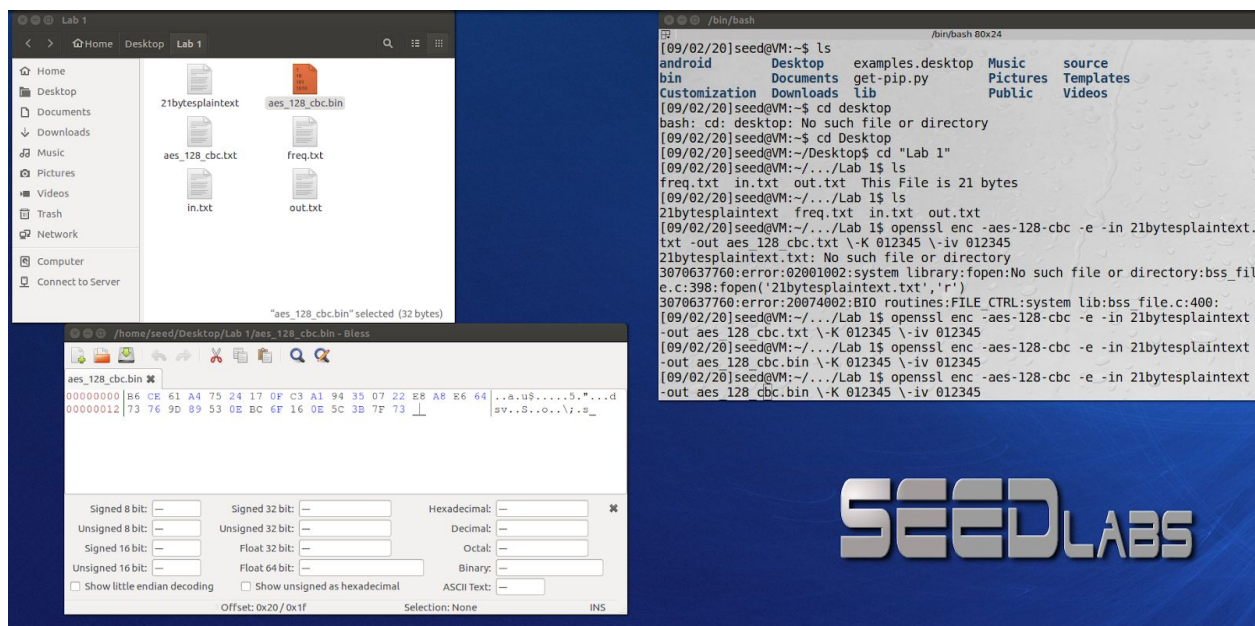


## TASK 4:

**ECB:** Aes-ECB encryption uses 16 byte blocks for encryption. The original text file we used was 21 bytes long, and after encrypting and checking the byte size using Bless Hex Editor, we found the byte size of the file to now be 32. ECB uses padding, as it changed the original file's size to a multiple of 32.

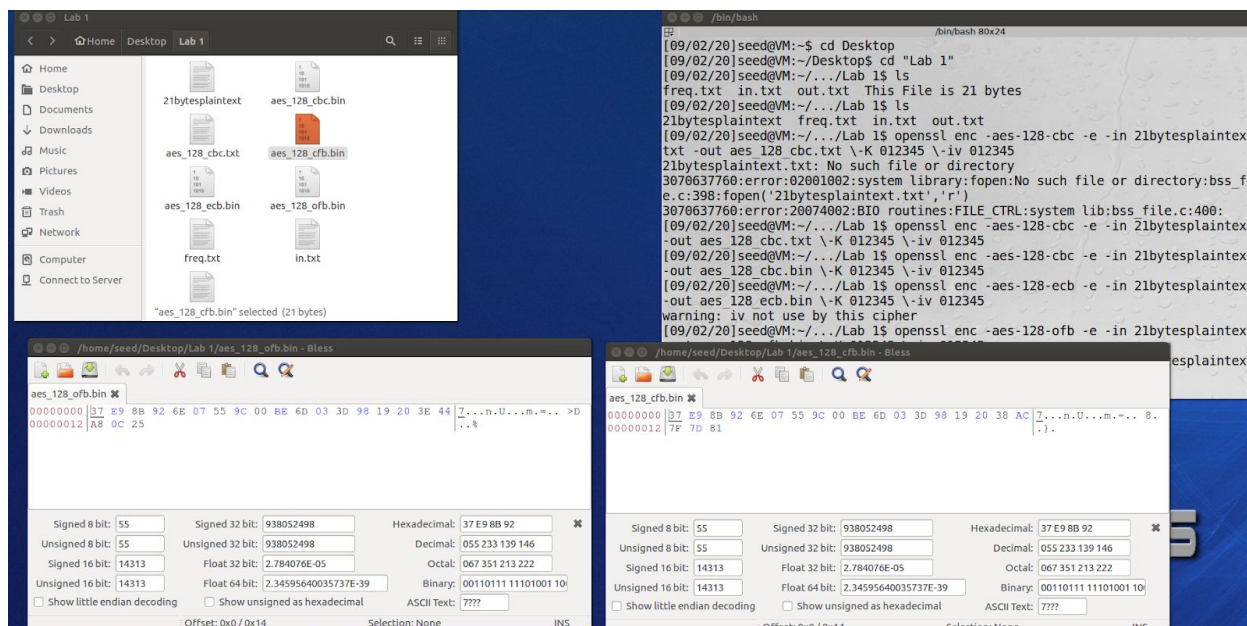


**CBC:** Aes-CBC encryption uses 16 byte blocks for encrypting. The plaintext file we used was 21 bytes long, and when we encrypted it and checked the byte size after using the Bless Hex Editor, we found out the file was now 32 bytes. This would mean that CBC uses padding, as it changed the byte size of the original file to a multiple of 32 to compensate for the missing 11 bytes.

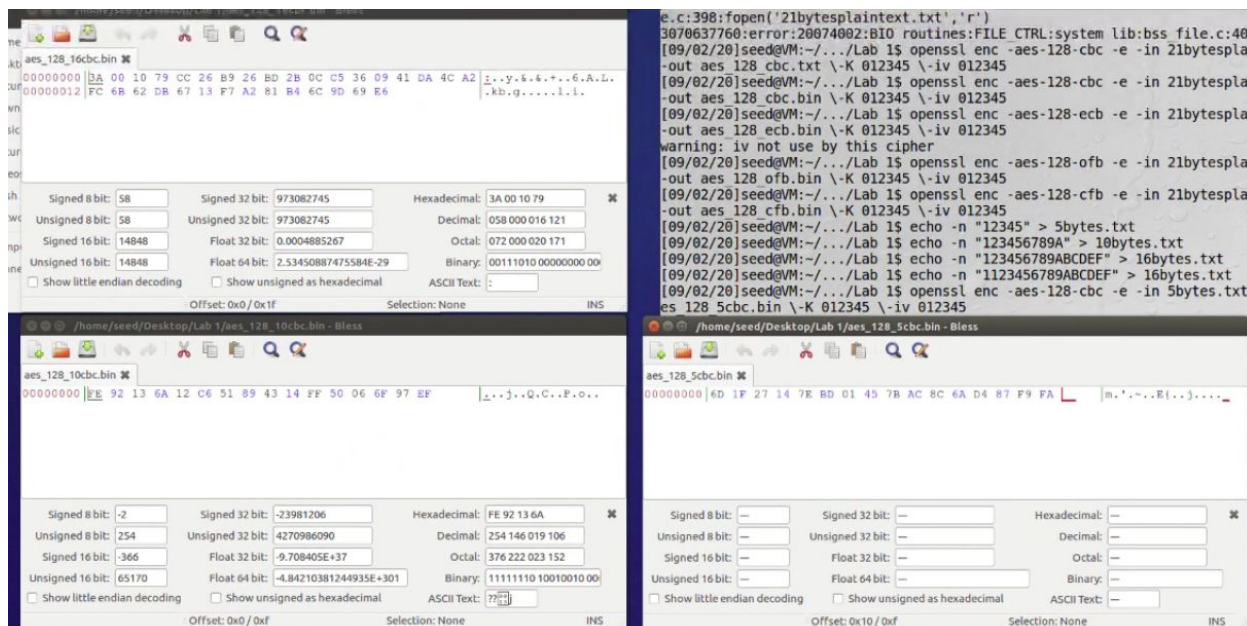


**CFB:** Aes-CFB encryption did not use padding.

**OFB:** Aes-OFB encryption was found to not use padding either.



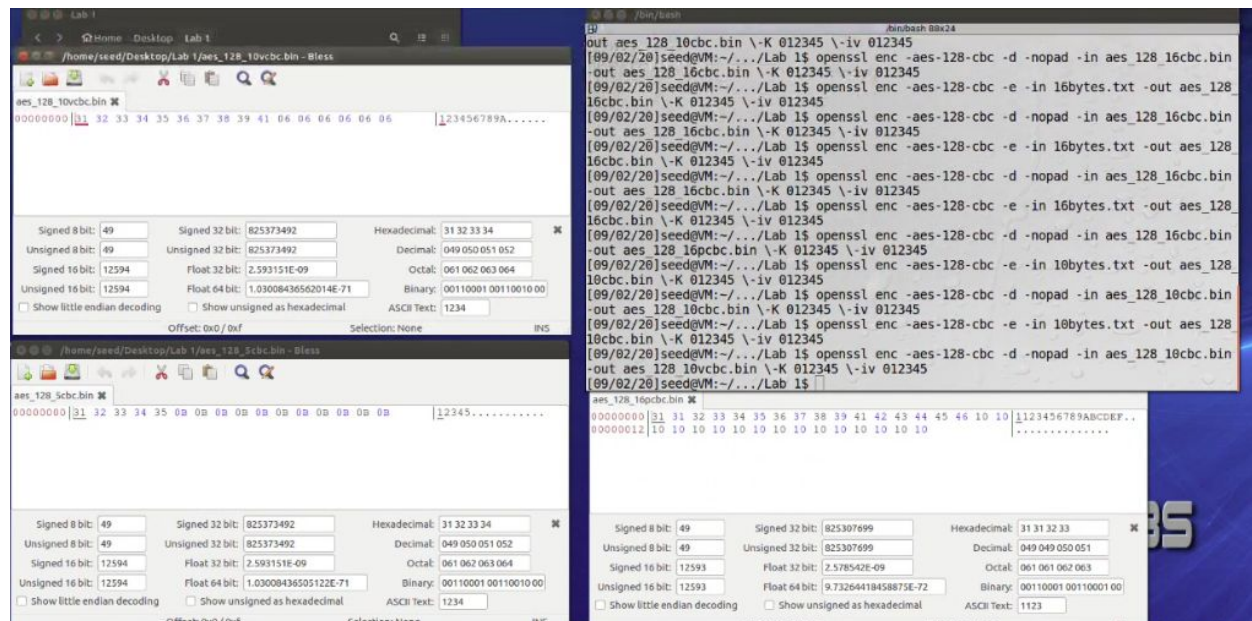
In step 2, we used aes-cbc encryption on 3 different sized files, a 5 byte, 10 byte, and 16 byte plaintext file. Then we studied their hex formats to see what kind of padding was used on the files. The



After decrypting, we could see the padding that was added and decrypted. When decrypting, we found out that we could not overwrite the file, as it caused an empty file everytime we tried. This was most likely due to the fact that the file was being decrypted



and overwritten, causing an error in the process.

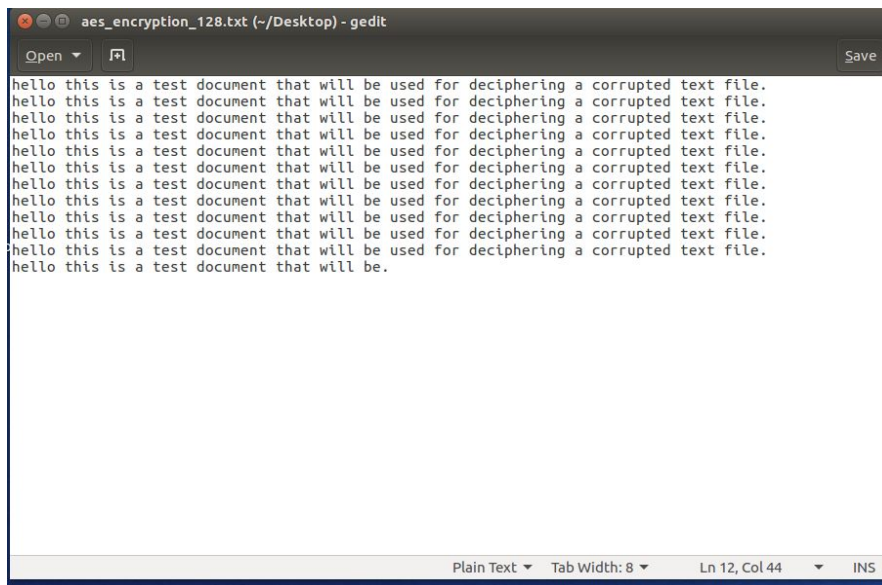


## TASK 5 Error Propagation - Corrupted Cipher Text:

Exactly how much information can we recover on decrypting corrupted files if the following encryption methods are used, ECB, CBC, CFB, and OFB? We will answer this before performing the task to verify if our predictions are correct.

1. **ECB:** A single cipher text block corruption will only affect one single block of plain text and each individual block of a cipher text is decrypted separately in ECB encryption. But it is possible for the 30th byte in a ciphertext block of 8 bytes to be corrupted and affect  $n$  bits of plaintext block 8 bytes since each block of decryption is done individually.
2. **CBC:** Same occurrence for ECB encryption but instead of one block of ciphertext corruption affecting one block of plaintext, it affects 2 blocks.
3. **CFB:** Error propagation is poorer in CFB because error in a cipher-text block affects the decipherment of the next  $(n/r)$  plain-text block.
4. **OFB:** Corrupted ciphertext files using OFB mode for recovery, error propagation is minimal. The feedback is in the key-generation system, and when there are errors in  $n$ th bit of ciphertext, it will affect the corresponding  $n$ th bit of plaintext.

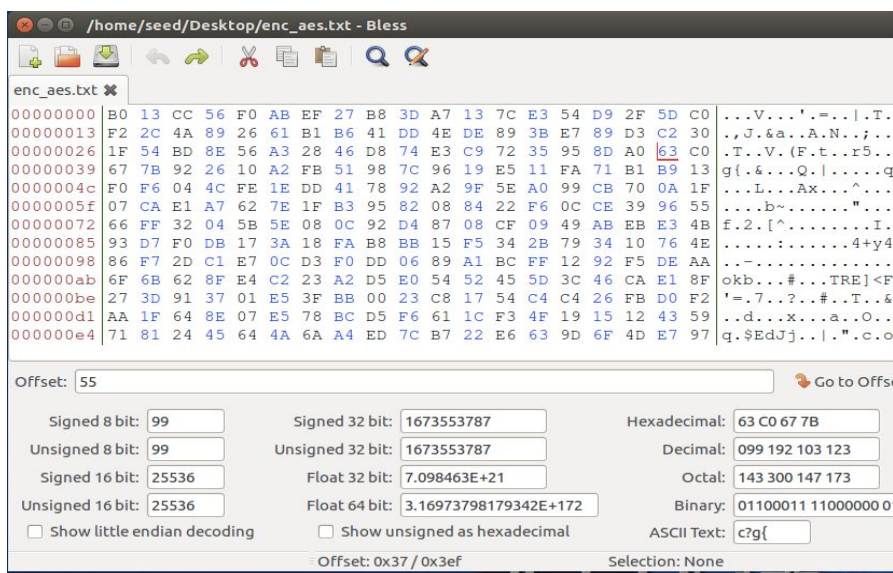
## Original text-file plaintext file



The screenshot shows a gedit window titled 'aes\_encryption\_128.txt (~/Desktop) - gedit'. The file contains 12 lines of text, each starting with 'hello this is a test document that will be used for deciphering a corrupted text file.' The status bar at the bottom indicates 'Plain Text', 'Tab Width: 8', 'Ln 12, Col 44', and 'INS'.

```
hello this is a test document that will be used for deciphering a corrupted text file.
hello this is a test document that will be used for deciphering a corrupted text file.
hello this is a test document that will be used for deciphering a corrupted text file.
hello this is a test document that will be used for deciphering a corrupted text file.
hello this is a test document that will be used for deciphering a corrupted text file.
hello this is a test document that will be used for deciphering a corrupted text file.
hello this is a test document that will be used for deciphering a corrupted text file.
hello this is a test document that will be used for deciphering a corrupted text file.
hello this is a test document that will be used for deciphering a corrupted text file.
hello this is a test document that will be used for deciphering a corrupted text file.
hello this is a test document that will be used for deciphering a corrupted text file.
hello this is a test document that will be.
```

## Locating 55th byte in the encrypted text file using bless



The screenshot shows the Bless application window titled '/home/seed/Desktop/enc\_aes.txt - Bless'. The main display shows the hex dump of the file 'enc\_aes.txt'. The 55th byte is highlighted in red. Below the hex dump, the 'Offset: 55' is entered, and the 'Go to Offset' button is visible. The application also displays various conversion options for the selected byte.

Offset:	55
Signed 8 bit:	99
Unsigned 8 bit:	99
Signed 16 bit:	25536
Unsigned 16 bit:	25536
Signed 32 bit:	1673553787
Unsigned 32 bit:	1673553787
Float 32 bit:	7.098463E+21
Float 64 bit:	3.16973798179342E+172
Hexadecimal:	63 C0 67 7B
Decimal:	099 192 103 123
Octal:	143 300 147 173
Binary:	01100011 11000000 01100011 11000000
ASCII Text:	c?g{

Offset: 0x37 / 0x3ef Selection: None



```
hello this is a test document that will be used
^F2iF0iB8B[REDACTED]t[REDACTED]uA[REDACTED]"^F7qQnU^D2iD8U^AC^D[REDACTED]^Gj[REDACTED]^D5^C9^-F4[REDACTED]^E[REDACTED]28*,-d8[REDACTED]9C^E5r^CD^D8^E1^E2^]Pk[REDACTED]^E5NZ[REDACTED]^C5d;4a^D2s^F2[^E6^B0h[REDACTED]uq8
96V[REDACTED]^A1^A51hm^98e*W^94635^F0[REDACTED]FV^E8^9EHQ^A0H^F1^C7k[REDACTED]^9F[REDACTED]
-^FE^91^E2^FAU^F^CC^C5^D[REDACTED]^FE^9^88^A3^98[REDACTED]^E9^90[REDACTED]^B0#:[REDACTED]^E[REDACTED]^F^A[REDACTED]^D7A^DF^F7^D2^C0^C0t^FD^C0^:Qz^D7
^FD15m^A0[REDACTED]^8v[REDACTED]^A0[REDACTED]^84^BE^E9K^88u^A3G!^D0[REDACTED]^~^F9^EF[REDACTED]^8D^D5[REDACTED]^F9c^89^B5z^B48[REDACTED]^84^DE[REDACTED]^E2D^80^FFL^F45H^C2i[REDACTED]^E2^E8[REDACTED]^C7[REDACTED]^E4
^E79^E5^DAE^A0[REDACTED]^B^E2
^9C^B4^E[REDACTED]^8E^97m^E[REDACTED]^C4^FC^D9p[REDACTED]^H^F[REDACTED]^B^F^B^I^A9^9B^C1^80^E3W[REDACTED]^CF[REDACTED]^A2.kC^8E^FD^C2M^p[REDACTED]^AE^FC^A4^A5^F8^~^A0c[REDACTED]^97,"^id0^D4^F7^A0
^DE4q^98t^C^D0^DE^Hr4^AF^C9<|^C^A^s)^A8^D0^C5^CE^F2t^BDU^B7C^BC^B9^B3[REDACTED]^H^-^C[REDACTED]^1^FCB^C2.^)E6s^F2^A[REDACTED]^F6S^FE^B7^80^AA^D7
^E2[REDACTED]^n[REDACTED]^*I^88^A7K^J0v^85^QD^E8[REDACTED]^t^B^AC0^E3Y^D03M^AF>^F7^C2I^-=^/B^C[REDACTED]^3m6[REDACTED]^E3^FCB^98^f<p^B2^裁^E4^A0^C2^CA^ECc(^D0>z^0Mf0^CB
^C0^B9^D0n^E3ZYC^F7^D6vmh^86^BA^AD^C56S^Iw.^[REDACTED]^FA^A8^e^9D^CFp60[REDACTED]^94^B83^8E^B2^F3[REDACTED]^C80^@N^A8brs[REDACTED]^8[REDACTED]^FV/u^FC[REDACTED]
>7|^F0^hp^B6p[REDACTED]^0^B^G^I^Q^C^I^C^W^80^F5^AD^95k^J^B^F^B0^D33^B8[REDACTED]
^EBM^D3UI^888^E7
^A4^F0U^DEH^87^80^A7^CF^C3^C^98^B3i^C0^8A^RqQ^F0[REDACTED]^E^F1[REDACTED]^99^C7Z^1a^E7[REDACTED]^9E<^94^C^CP"^FED^F9^F3^B2^A0[REDACTED]^E2^D8[REDACTED]^A1^F8^E2^Hg/;^A0^I^Q
^86s^Bc^F3
^9F[REDACTED]^CC^F8^C4^C0[REDACTED]^kt[REDACTED]^w*^E8^[REDACTED]^88^82^Fc.^CD*^9CI^0^FE^E8^9F[REDACTED]^D8^!OU^D88[REDACTED]^FQ^98V^91^B2g^A9^97^B5[REDACTED]^E8^D0[REDACTED]^AD
^EB^B0[REDACTED]^98t^E8^F48^-^FD^F2^BC^AF6^A3^8CD^C9^EBL^Rm[REDACTED]^E6^DabD^A1^cpVRf^E0^FE[REDACTED]^E6^D0[REDACTED]^F1^8E:^AC^F7^DF^DB^D87^A7^8BV^89Y7^86
^9F^A4[REDACTED]^CBH^91^80Wm^u^94^B4^C2^g0g[REDACTED]^DF^C^A^E^C^A8^9g^E1^Bf^-^F[REDACTED]^EA^C9^D1^C^ED^EC^E6Z&U^B0[REDACTED]^7^D9Z^D4^oB3^F8DB^86^B3C[REDACTED]^9A[REDACTED]
^FC^F0^D0j^90^E9H^88^E4^C1K[REDACTED]^C80^B0^F2^C8D3^+F^C6^C0D^D5^UN^84^E1^V[S^F1M[REDACTED]^B8K0^F3^F3^B8^R^AD^D4^E1^W8A[REDACTED]^86^88^A27^-o
^E05^F6iU"^A8X^8C^9Ez!^[REDACTED]^F13^FF^98s^E562^Iq^B2fdwj'^x9[REDACTED]^88[REDACTED]^CB[REDACTED]^C1^9D^-^B2[REDACTED]^D7^C34^FBZ4^-@U^CDnb
I[REDACTED]^93^83T^C2[REDACTED]^80^81^80;[REDACTED]^83^E6^E7^9AKcS[REDACTED]^8AN^8C^91^P0^80XRD^-m^o0
```

Decrypted plaintext on corrupting the 55th byte on the ciphertext using CBC method. As You can see the plaintext retained only half a line of one sentence from the original plaintext.

```
hello this is a test document that will be used sek"9180A9A3M8895&9C96F39EE%90F6F7D8D
(F5g)BBD4zsBEBSU96A43P90D0D6FAABVCLD500F194F83C8FA\ECDDN8F1g8[700TFj\A2&BA\C6
E99o\FB\AEس\AA\D7\F0i\A6\B4\94\E3\D6\F099A3\D9\F99B1M\EAu\A2h9\8D\E5\D899ko99k\90WC5E99C7v\F4\A4\D9
\F2\91\BD\B2q)\95\C2\D699ECDL\BF\8A\B8
E2C\F4\8A\DF99F19v\04\FE9\FBd!aq\F59994M\F8b99DB\EE\F9999^AB99C3\FD\D6\DF\E8\CDp\A82\BC\B7[BA\87\E9E\83
93\ES\EC99FC\8E\AEy\AB
B2E6!ED\FA\AE\F0\C1\B4\B4*998799C99b3
ADs99BS\C6o"v\BE\E4ft99ED\AB\BA\F899O\E5h\B9T\CS$DAB6NY99FCu\FA99D5\89t99,A9\B9a`B7\F0g99D3\B5\A2\k
84:99799,%99
FCq~taW"99FM909
,F1j399EY99F6C7}
\AE\B5\A399BAm\A1\D5\94\8F4\97\98!A4v\FAI您c99`G\D199#D73S99A3zR\BAotm\EF\A7\C12\9A;]999AD6\B3\DA^A2\B1
E9\C2%\C1z\D899C2X\9B\AEUJ\DAexB\EA>99EC\9A\EE\89Rzd-\C1nZq99G<-94\ABD\984>9996\98\AD\E3\F399C\F1\C97
\06
AFx\BB\B599H00\ED\00n\J\A7\D1Q\BE>\D8AX\9E\EF99F1999D6=#\A4R99~99\8C\F7.\E1\88\FC\ED9999C\DE\EF\Q\FA\A3P\
EB\A2,XoS9\87XI\C9,94\A6\CE9999D999C4\DE\FE\9C5*84\C9\F599DZ\95\80E\C1K\BD?99D3U\C9:99x^T9994SB96\FA
F7\9BVX:9995\F4\CA\CA{\A4W\8D\9F99FCO99J\8F&+99799A0\A6F\E0\D82t199t\00\A8<X\ED\9E998\DFYm\BA!\8Fy\D6;
93\96\ABuV\DFd3)\F9R\BD\B8Q\F9MB599d99a99FV\F2J_92H\86\90\F6C\E699v81\00\j\A7\8E_A7\E0\E8\AE9992D99\AF\F2
F7>\D8999.zw\87\9E\E0\84SgO\9E99m\A6r\AD\99\EB\H\D8\CDz99'
E4:3\CO\CC\E1%06998AH<C3\D4\C7\F7\041?C4Q\86\90,DD99CB99\F8\C599D499Z-\D6\99999999\BB\D7L\EF):DE\C199
F6J\CSN\04\EA\04\F2\85\FD\F8C99S\A8\95DBI\AFT\AD\CEV\C599:F3Z\F5zB4\C8\D78\912\AC99B19989F\F899
TW\A9\ED\E2\84R\99E99C)\E4[F4\97\C8M\F8_r\9E\AE999AmdF%BD992+R99B99C29992\00Y\99V\89T\FA\F4\{A49999\87
DF&\B299}Q\01"S\8C\BD\DEB~\F6]]\BD=-0699Ej\B8\88k
99\AC\009999\BC99\A0E99P\84\84\B89999\9B\9C\AC\EG\8399&;B9\F0
B4\D699C3\E7\90/E999FD\99\EBH{\E4\FD
```

## CFB mode

```
hello this is a test document that will be used for dec\F1^J\AB\ES\9B\C8\F1\F8G\EBR\F2t^BB\D29999\F1\F1e99E3
AE2\BE999FE\FF\F5;A>A3Q;A7\99993Mq\D3\FB\C0\9E?F999A6\89\04
EE S\EB\BB\D3\00z%97RZD\069984\B091\J\AD99FA\FC\BD99B\E1\BC\95\AEx9999wq%998\89p\88\A50\FA\00L\D\A499
B5x\F2\A6z\96\F1\F7M\8D\82\FB?FC\|C7\C9998\F2j(\95\EE2\BFerO\C9H\9D099EhE/\93#\D7C~\9F-PUy\A330\F6\B5)0
F2c99ت\B5&t\0699EC4C7t\E7\A1i99=99S\B5v\C9\ABc;9993\B8\799A4\C0\88\C20\8F\A5\9D\8F99BFMC\909999\F9\8C\88
u\94\BAF\DE^8C99994\BA*2o\B1\8U\AD\86\8Bv
EE\E3\AD\C8\00CE9999\B8\A9-y9999B0\8199A7_zX\F7\ACB0\BAT\AC\A2\9Ck\87\91\CEm\EDRE\08\F10EmG\F8\FB\B4\FDX\04]
F8\91\8F\A5E>99Hr=+\DFP\CAf(\99v99995?900
\08\E3\F3m99BA\F0y`0\F3\00y\A2\B0C\BD\2\DE.O999FE3n\98997\9999\F2t99:8F\CE\FE9999\F3\80\ED9999D8p
\0299\A2\83\DE9\,9999\BC>99p$nb\cQ(\EE\88\FFK0
B8\9E\9A"B4\F8GY\B5*p\B4FE\DA9999CB>\83u\EC9999FF9999\BE\CFL\ACq\A1\A7=8F\88k\8B\FE\9C\9B\92(\BD99\F9)4\B9
S('μ\FA\DF\00k\9599A3\ED[e\DFK\B5[\D3\l\88ckB\8D\CF\F6999A84-X\E9~J\BA\AA\859999Fw\019999\F9\00\9C
A6k99g\9Fz\A89999Des\ED+3j?9999$BF\09-f09999P]Act"\F5\Ed\AB\80\B0Q999A6+9999t\EAk}\BCSHy%;A\A0v\FA\B2
BE~sHz9988-BA9999G1\C9\F89999'-9999E59999J9A\98\9CX\9FRn\9999S9999VS\92UB\9E\E40\029999bu\FB\96ff\F6\B6\EBA9999CCS<\AA
\C6\DA7)&\F92Cc8\02AS\FB\9A\E9\8A9999FE@97\96P\F69999S999994\FA\E3\9CPQ\B3y9999t\ES[\E8\8F\lgF\A86y\B0\A899999A\CF=
\FB3999
w$W\037\F1\99\9F\C1t\EDr.S\A8`8799Q)9999C7C\AB\E1%BBE9999C0\DB\C7B\BC\F5\C5{9999:8F\A0\CD:\BDG=87DM\F0\80{8F,{J
\88P\06!\07*83_E39999\F8\C8\D5\CFw9999A\CD\08b\F5J\85\EF\AB\F69999B6'\EF\91\05k\F90"9999^B6b\90\E3}I\FC\F1\84V\A
A0\EF\84;\F5\E0\ABF\8D\A3B\82`Z\FE\88\82;\B1\B9\DD9999B9\92w\EFi\A9\EC\E5\F4ok\9E\8A\BFT$E7%(CE)\8Fi\F
CFho\BD\0D4\050d\FfI5\81\B09999+7!\93H\CB9999EAY6\A4j\9C/\9999^s9999\8C\82\989C9\FAX\81\9E5X\F45\C1\0B\05\F09999AF\A
```

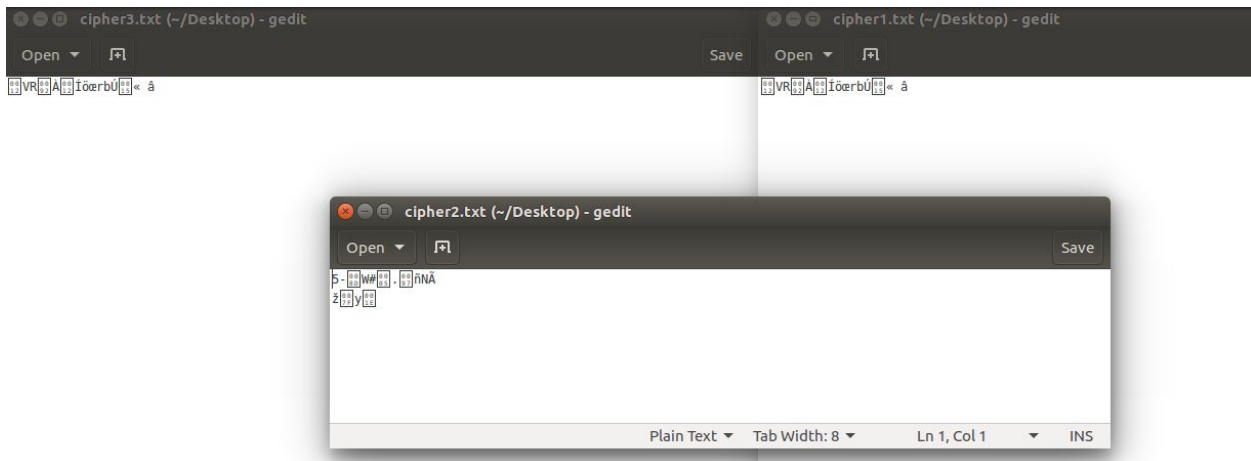


## OFB mode

```
hello this is a test document that will be used for decX[00]2i1\AF\CC0!k5-\C9S`A\95zx\04U\82\89\82zx\CB\R\C30
\BB\07\07\FE+[00]\96\E8\F6\C4\CC\8FuU[00]\AD\85\F7\B95\F3L\A!3[00]\C0[00]\9F\F7\98G @UH4c[00]\AE89\3\F7\AE
\85H\95<\F9\C4
\82cr\FAH\87\C7\DF\00\9A,<[00]\CD\F3m[00]\C7[00]\C89\08r\83\F6[00]\AF\06\CF\CB^P[00]\DCU\B3\AB\86\EA\89hk[00]\8FT\81\00Y
\DF^00W[00]X\06\F6\9F\80(PXf[00]\AE\BF\EF\01w[00]I
[00]\D8DQ_jVf[00]\KI2$F6s\AD\96eEA\06\FE\90Y\ES\050\Fes\FA\CFb[00]\FCj\S\88V\EC[00]\F4W\F8m[00]\9C\95B^Y\83\AC*U^m[00]A$
\90\00\AF@_ \90\E9\80J\EE\00\A8[00]*ie\FF7\DF\F7r\C6[00]\E62\83\03[00]\ED\DE1[00]bi_\F6w\94Z\84\E9\E4\8Ac
\99[00]\C2\EE[y\90[00]i]\860\B3i[00]h\A4j6C\E5[00]\Z0\B0R0x[00]\D8[00]\87\02^00\C3\C6fr\FD\050`\F3\FD\EB\FE!<\F1e\A7[00]\90[00]
\F0\E6R+\C0L\B6[00]M\0[00]m\q\09\DE[00]\EF[00]\80;\8F\C4@082\06'#\A9\FE\8F\8A\F4\A5Z[00]k[00]\C8DE];jP8\EE[00]~f[00]\BF=[00]U\B7K
\90\00\F0\A8\90\EGa[00]N\A6~9[00]\>\A4\F1\BEoSAV[00]\0\8B`G\C4T\C45Lw\07\02\00\BCC[00]\0[00]\EA\02\F6\F0\FC\92\B0\FC\B5
\808\94\F81\B1\A5"\A0\AE\F5K>n\93R\CED[00]DFE\A3\BAZ[00]\DA\t\AA\90\C383\[\00]\B2n\EF\#t[00]\C3'\ED\E88"\BB\03\DAv\BF\04
\C2\C1\F4\B7\F5W~d\E3K!\95[00]\01[00]&:\879\C6[00]j\A1\EO\CO@4[00]\9DUJ\1\C2\EA[00]\F2[00]\AF\8E\8ct\98\9B\88[00]\L\04\DAg^ZZ
\FD`q)p\EA[00];-\B1\A0\A3\02\00\C8\C1\9F\A8\90\B8\AEL\EDt[00]
J\88\0DTB\92w5/\BA\8An\A1\A5'\9B\08'\BA\FC\89\B7\A6\85\04b\8ABB\C4 u[00]m\F9\8E1\91
ä\FEhy\82\A1\B0/[00]\09V\B0\99\EC\8C%\CDZ;\B8\85[00]\96[00]\83\9A4.k\AE\07"\860\E2\F7\A2\CF\01P[00]\ED\CB\03E[00]
$[00]t[00]\00[00]\00[00]\E9[00]\B4\CSi\8C[00]b\EFa\E3\C4[00]\99I\A5[00]\00\A3[00]\B9x\87\EGP\00\A5a[00]\A9x[00]
[00]\CD>\EC\8C,\E3\04
\F9\86\B8\CO[00]#\ECU\BAK\AF[00]\B3[00]Z\9\994[00]\A7\DC[00]\F5[00]{\AF\F1Y\DEY\AES:}\84\04S!\B9\9F[00]\CB=dZ-\A1
\AC\8E\A7\05\CF[00]\E5e\92[00]\F7VP\A3k\A4I\92\E5\C8\ED\05[00]\A3A[00]\E0\B8k5\02b\B9\83\DE/\8E[00]\DC[00]_2[\8B\03q\92
\E2Q-\CFSv[00]zT\B1\96-\EB\8A[00]AaQ'\AE[00]\C02\FA)\AE[00]\F6[00]\77k#S\8E\03\F6g|\F1E\03[00]p;1$ \85\0B\CB\DE0
[00]\FD5b\F8[00]\FF\ED\B4\F5{o\817Z\9C1:dk\F2\DEH\FF[00]\81[00]\EB[00]\BE{\BF
```

As it turns out, our original prediction turned out to be wrong. We believed theoretically that OFB mode would have the least error propagation, but it seems that only ECB mode was the only plaintext that retain the most information, which was one entire line of the original plaintext. Maybe there is an error in overwriting the 55th byte in bless, but this our results above.

## Task 6: Initial Vectors (IV) and Common Mistakes



In this task we use IVs to encrypt plaintext files. By changing the IV, cipher1.txt and cipher2.txt end up having different characters in their encryption text. Meanwhile, we

used the same IV for cipher1.txt and cipher3.txt and got the same output encryption text.



For the second part of the task, we were told to decrypt a message that had already been encrypted with OFB. After decrypting, we found the message to be “Here is a top secret.” By using an XOR file from the book, and getting the hex values for the encrypted files, we were able to decrypt the file without a key. If we used CFB, we would only be able to find partial parts of the message, due to it being a different type of encryption.

For the third part of task 6, we were not able to decrypt the message as we did not know how to use the XOR file. In the second task, we were able to easily see the message, however here, we do not understand how to use the XOR file in practice.