

Secret-Key Encryption Lab Report

Mudit Vats
mpvats@syr.edu
2/23/2019

Table of Contents

Overview	3
Task 1: Frequency Analysis Monoalphabetic Substitution Cipher	3
Observations / Explanations	6
Redo: Further Explanation of Decryption	6
Task 2: Encryption using Different Ciphers and Modes.....	14
AES128CBC Encrypt/Decrypt.....	15
AES128CFB Encrypt/Decrypt.....	16
BFCBC Encrypt/Decrypt.....	17
Observations / Explanations	18
Task 3: Encryption Mode – ECB vs. CBC.....	19
Redo: Complete missing task.....	24
Observations / Explanations	29
Task 5: Error Propagation – Corrupted Cipher Text	30
Observations / Explanations	39

Overview

This lab report presents observations and explanations for the tasks described in the [Secret Key Encryption Lab.](#)

Please note, I updated the icons and some theming elements to make the UI a little more pleasing to the eye. It's still the Ubuntu 16.04 Seed VM.

Task 1: Frequency Analysis Monoalphabetic Substitution Cipher

Use Frequency Analysis to decrypt the cipher text.

The cipher text is below. This is the [ciphertext file](#) as downloaded from the SEED Lab web-site:

```
ytn xqavhq yzhu xu qzupvd ltmat qnncq vgxy hmrty vbynh ytmq ixur qyhvurn  
vlvhpq yhme ytn gvrrnh bnniq imsn v uxuvrnuvhmvu yxx  
  
ytn vlvhpq hvan lvq gxxsnupnp gd ytn pncmqn xb tvhfnd lnmucqymnu vy myq xzyqny  
vup ytn veehnuy mceixqmxu xb tmq bmic axcevud vy ytn nup vup my lvq qtvenp gd  
ytn ncncrnuan xb cnyxx ymcnq ze givasrxlu eximymaq vhacavupd vayfmqvc vup  
v uvymxuvi axufnhqvymxu vq ghmn vup cvp vq v bnfnh phnvc vxzy ltnytnh ytnhn  
xzrty yx gn v ehnqmpnuy lmubhnd ytn qnvqxu pmpuy ozqy qnnc nkyhv ixur my lvq  
nkyhv ixur gnazqzn ytn xqavhq lnhn cxfnp yx ytn bmhqv lnnsup mu cvhat yx  
vfxmp axubimaymur lmyt ytn aixqmur anhncxud xb ytn imuynh xidcemaq ytvusq  
ednxuratvur  
  
xun gmr jznqymxu qzhhxzupmur ytmq dnvhq vavpncd vlvhpq mq txi xh mb ytn  
anhncxud lmii vpphnqq cnyxx nqenamviid vbynh ytn rxipnu rixgnq ltmat gnacvn  
v ozgmivuy axcmurxzy evhyd bxh ymcnq ze ytn cxfnccnuy qenvhtvpnp gd  
exlnhbzi txiidlxp lxcnu ltx tnienc hvmqn cmiimxuq xb pxiivhq yx bmrt ynkzvi  
tvhvqqcnuy vhxzup ytn axzuyhd  
  
qmruvimir ytnmh qzeexhy rxipnu rixgnq vyyupnnq qlvytnp ytn cqnifnq mu givas  
qexhymp iveni emuq vup qxzupnp xbb vgxy qnkmqy exlnh mcgvivuanq bhxc ytn hnp  
avheny vup ytn qyvrn xu ytn vrmh n lvq aviinp xzy vxzy evd munjzmyd vbynh  
myq bxhcnh vuatxh avyy qvpinh jzmy xuan qtn invhunp ytvy qtn lvq cvsmur bv  
inqq ytvy v cvin axtxqy vup pzhmur ytn anhncxud uvyyimn exhycv uxxs v gizuy  
vup qvymqbdmur pmr vy ytn viicvin hxqy়nb xb uxcmuvynp pmhnayhq txi axzip  
ytvy gn yxeenp  
  
vq my yzhuq xzy vy invqy mu ynhcq xb ytn xqavhq my ehxvgid lxuy gn  
  
lxcnu mufxifnp mu ymcnq ze qvmp ytvy viytxzrt ytn rixgnq qmrumbmnp ytn  
mumymvymfnq ivzuaat ytd unfnh muynupnp my yx gn ozqy vu vlvhpq qnvqxu  
avcevmru xh xun ytvy gnacvn vqqxamvynp xuid lmyt hnpavheny vaymxuq muqynvp  
v qexsnqlxvnu qvmp ytn rhxze mq lhxsmur gntmup aixqnp pxxhq vup tvq qmu  
vcvqqnp cmiimxu bxh myq inrvi pnbnuqn bzup ltmat vbynh ytn rixgnq lvq  
bixxnpn lmyt ytxzqvupq xb pxuvymxuq xb xh inqq bhxc enxein mu qxcn  
axzuyhmnp  
  
ux avii yx lnvh givas rxiuq lnuy xzy mu vpfvuan xb ytn xqavhq ytxzrt ytn  
cxfnccnuy lmii vicxqy anhyvmuid gn hnbnhnuanp gnbxhn vup pzhmur ytn anhncxud  
nqenamviid qmuhan fxavi cnyxx qzeexhyhnp imsn vqtind ozpp ivzhv pnhu vup  
umaxin smpcvu vhn qatnpzinp ehnqnuynh  
  
vuxytnh bnvyzhh xb ytmq qnvqxu ux xun hnviid sulkq ltx mq rxmur yx lmu gnqy  
emayzhh vhrzvgid ytmq tveenuq v ixy xb ytn ymcn muvhrzvgid ytn uvmigmyh  
uvhhvymfn xuid qnhfnq ytn vlvhpq tden cvatmun gzy xbynu ytn enxein bxhnnavqymur
```

ytn hvan qxaviinp xqavhxixrmqyq avu cvsn xuid npzavynp rznqqnq

ytn lvd ytn vavpnecd yvgzivynq ytn gmr lmuunh pxnquy tnie mu nfnhd xytnh
avynrxdh ytn uxcmunn lmyt ytn cxqy fxynq lmuq gzy mu ytn gnqy emayzhn
avynrxdh fxynhq vhn vqsnp yx imqy ytnmh yxe cxfmnq mu ehnbnhnuymvi xhpnh mb v
cxfmn rnyq cxhn ytvt enhanuy xb ytn bmhqeivan fxynq my lmuq ltnu ux
cxfmn cvuvrnq ytvy ytn xun lmyt ytn bnlqy bmhqeivan fxynq mq nimcmuvynp vup
myq fxynq vhn hnppmqyhmgyzynp yx ytn cxfmnq ytvy rvhunhnp ytn nimcmuvynp gviixyq
qnaxupeivan fxynq vup ytmq axuymuznq zuymi v lmuunh ncchrnq

my mq vii ynhhmgid axubzqmur gzy veevhnuqid ytn axuqnuqzq bvxhmyn axcnq xzy
vtnvp mu ytn nup ytmq cnvuq ytvy nupxbqnvqxu vlvhpq atvyynh mufvhmvgid
mufxfifnq yxhyzhnp qenazivymxu vxzxy ltmat bmic lxzip cxqy imsnid gn fxynq
qnaxup xh ytmhp bvxhmyn vup ytn njzviid yxhyzhnp axuaizqmxuq vxzxy ltmat
bmic cmrty ehnfvmi

mu my lvq v yxqqze gnylnnu gxdtxxp vup ytn nfnuyzvi lmuunh gmhpcvu
mu lmyt ixyq xb nkenhyq gnyymur xu ytn hnfnuvuy xh ytn gmr qtxhy ytn
ehmwln lnyu yx qexyimrty ivqy dnvh unvhid vii ytn bxhnavqynh pnaivhnp iv
iv up ytn ehnqzceymfn lmuunh vup bxh ylx vup v tvib cmuzynq ytnd lnhn
axhhnay gnbxhn vu nufnixen quvzb lvq hnfnwvp vup ytn hmrtbyzbi lmuunh
cxxuiimrty lvq ahxlunp

ytmq dnvh vlvhpq lvyatnq vhn zunjzviid pmfmpnpn gnylnnu ythnn gmiigxvhpq
xzyqmpn nggmur cmqqxzdm ytn bvxhmyn vup ytn qtven xb lvynh ltmat mq
ytn gvrnnhq ehnpmaymxu lmyt v bnl bxhnavqymur v tvmi cvhd lmu bxh rny xzy

gzy vii xb ytxqn bmicq tvfn tmqyxhmai xqavhxymur evyynhuq vrvmuq ytn
qtven xb lvynh tvq uxcmuvymxuq cxhn ytvt vud xytnh bmic vup lvq viqx
uvcpn ytn dnvh gnyq gd ytn ehxpzanhq vup pmhnayxhq rzmpq dny my lvq uxy
uxcmuvynp bxh v qahnnu vayxhq rzmp vlvhp bxh gnyq nuqncgin vup ux bmic tvq
lxu gnyq emayzhn lmytxzy ehnfmxzqid ivupmur vy invqy ytn vayxhq uxcmuvymxu
qmuhan ghvntnvh mu ytmq dnvh ytn gnyq nuqncgin qvr nupnp ze rxmur yx
ythnn gmiigxvhpq ltmat mq qmrumbmavuy gnatzqn vayxhq cvsn ze ytn vavpncdq
ivhrnqy ghvuat ytvy bmic ltmin pmfmqmfn viqx lnx ytn gnyq phvcv rxipnu rixgn
vup ytn gvbyv gzy myq bmiccvsnh cvhymu capxuvrt lvq uxy uxcmuvynp bxh gnyq
pmhnayxh vup vevhy bhxc vrhx cxfmnq ytvy ivup gnyq emayzhn lmytxzy viqx
nvhumur gnyq pmhnayxh uxcmuvymxuq vhn bnl vup bvh gnylnnu

The decrypted plain text is below:

the oscars turn on sunday which seems about right after this long strange
awards trip the bagger feels like a nonagenarian too

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

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

signaling their support golden globes attendees swathed themselves in black
sported lapel pins and sounded off about sexist power imbalances from the red
carpet and the stage on the air e was called out about pay inequity after

its former anchor catt sadler quit once she learned that she was making far less than a male 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

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

another feature of this season no one really knows who is going to win best picture arguably this happens a lot of the time inarguably the nailbiter narrative only serves the awards hype machine but often the people forecasting the race socalled oscarologists can make only educated guesses

the way the academy tabulates the big winner doesnt help in every other category the nominee with the most votes wins but in the best picture category voters are asked to list their top movies in preferential order if a movie gets more than percent of the firstplace votes it wins when no movie manages that the one with the fewest firstplace votes is eliminated and its votes are redistributed to the movies that garnered the eliminated ballots secondplace votes and this continues until a winner emerges

it is all terribly confusing but apparently the consensus favorite comes out ahead in the end this means that endofseason awards chatter invariably involves tortured speculation about which film would most likely be voters second or third favorite and then equally tortured conclusions about which film might prevail

in it was a tossup between boyhood and the eventual winner birdman in with lots of experts betting on the revenant or the big short the prize went to spotlight last year nearly all the forecasters declared la la land the presumptive winner and for two and a half minutes they were correct before an envelope snafu was revealed and the rightful winner moonlight was crowned

this year awards watchers are unequally divided between three billboards outside ebbing missouri the favorite and the shape of water which is the baggers prediction with a few forecasting a hail mary win for get out

but all of those films have historical oscarvoting patterns against them the shape of water has nominations more than any other film and was also named the years best by the producers and directors guilds yet it was not nominated for a screen actors guild award for best ensemble and no film has won best picture without previously landing at least the actors nomination since braveheart in this year the best ensemble sag ended up going to three billboards which is significant because actors make up the academys largest branch that film while divisive also won the best drama golden globe

and the bafta but its filmmaker martin mcdonagh was not nominated for best director and apart from argo movies that land best picture without also earning best director nominations are few and far between

The key used is below. The yellow indicates the encrypted characters and the green indicates the plaintext characters. So, the yellow encrypted characters are replaced with the green plaintext characters:

Letter Frequency Order																									
N	Y	V	X	U	Q	M	H	T	I	P	A	C	Z	L	B	G	R	E	D	F	S	J	K	O	W
E	T	A	O	N	S	I	R	H	L	D	C	M	U	W	F	B	G	P	Y	V	K	Q	X	J	Z
Alphabetic Order																									
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	F	M	Y	P	V	B	R	L	Q	X	W	I	E	J	D	S	G	K	H	N	A	Z	O	T	U

Observations / Explanations

I started by using the trigrams for substitution by looking at highest frequency trigrams within the ciphertext and comparing that to the most used three letter words in the English language (provided in Frequency_Analysis_2_2.docx and links in the lab). I was able to substitute YTN with "THE" and VUP with "AND" (I used Microsoft Code to find/replace text). That translated six letters (four consonants and two vowels) out of twenty-six. I then looked at the single letter frequency order in the English language and started to make substitutions for the top frequency letters. From there, I was able to begin making out two and three letter words in the ciphertext which led to more discovery of the key. From there, it snow-balled in that the more I discovered, the easier it was to decode the rest of the key.

One interesting item which made this task take a little longer was that spaces were removed in the analysis. This caused, for example, PYT to be a top five trigram. When we look at PYT translated, that's "DTH", which is not used in the plaintext. We do see "D TH" being used however. So, once I realized that the web tool took out spaces as part of the analysis, I was able to better understand how to substitute trigrams such as this.

Regardless, fun exercise!

Redo: Further Explanation of Decryption

I used Microsoft Visual Studio Code for the text replacement.

First I replaced "ytn" with "THE". This first figure is how the VS Code works for replacement. This is before the replacement.

SEEDUbuntu Encryption Lab (Before Apache Config) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Edit Selection View Go Debug Terminal Help ciphertext.txt - Visual Studio Code

THE

```

1 ytn xqavhq yzhu xu qzupvd ltmat qmcnq vgxz ymrty vbynh ytn ytn
2 vlvhpq yhme ytn gvrnh bnniq imsn v uxuvrnvhmvu yxx
3
4 ytn vlvhpq hvan lvq gxxsnupnp gd ytn pncmgn xb tvhfnd lnmuvgvmla vy myq xzuyqil
5 vup ytn veevhnuy mceixqmxu xb tmq bmcx acxevid vy ytn nup vup my lvq qtvenp gd
6 ytn ncnhruan xb cnyxx ymcnq ze givasrxi eximymaq vhacavupd vayfmq vup
7 v uvymxvi axufnqyvymxu vq ghmbn vup cvp vq v bnfn phvc vxgzy ltynth ytnh
8 xzrtt yx gn v ehngmpnuy lmbuhnd ytn qnvqxu pmupy ozqy qmcn nkyhv ixur my lvq
9 nkyhv ixur gnavaqn ytn xqavhq lnhn cxfnp yx ytn bmhgy lnnsnup mu cvhat yx
10 vfxmp axubimaymur lmyt ytn aixqmur anhncxud xb ytn lmuyh xidcemaq ytvusq
11 ednxuraturv
12
13 xun gmr jznqymxu qzhhxzupmum ytmq dnhq vavpncl vlvhpq mq txl xh mb ytn
14 anhncxud lmmi vpphnnq cnyxx nqenamviid vbynh ytn rxipnu rixgnq ltmat gnavcn
15 v ozgmivuy axcmurxzy evhyd bxh ymcnq ze ytn cxfncnq qenvhvtvnpn gd
16 exlnhbzi txiidlxp lxncu ltx tniemp hmgn cmimxu xb pxivh yx brmty qnkzv
17 tvhvqqcnuv vhxuzp ytn axzuyhd
18
19 qmrurimur ytnmbl qzeexhy rxipnu rixgnq vynupnpnq qlvyt ytn cqnifnq mu givas
20 exhyhyp ikeni emuq vup qzupnpn xbb vgxy qmkmy exlnh mcgvivuanq bhxc ytn hnp
21 avheny vup ytn qyrrn xu ytn vnmh n lvq avinpi xzy vxgzy evd munjzmyd vbynh
22 myg bxhcnu vuatxh avvy qvpinh jzmy xuan qtn invhnp ytvv qtn lvq cysmru bvh
23 inqq ytvu v cvin axtxqy vup pzhmr ytn anhncxud uvvymn exhycvu yxxs v gizuy
24 vup qvymqbdmru pmr v ytn viicvnx hqyhn xb uxcmuvnp pmhnyh qtl axzip
25 ytvu gn yxeenp
26
27 vq my yzhuq xzy vy invqy mu ynhcq xb ytn xqavhq my ehxgvgid lxuy gn
28
29 lxncu mufkifnp mu ymcnq ze qvmp ytvu viytxzrt ytn rixgnq qmrumbmp ytn
30 mumymvymfng ivzuat ytd unfnh muynupnp my yx gn ozqy vu vlvhpq qnvqxu
31 avcevmru xh xun ytvu gnacnv vqqxamvypn xuid lmyt hnpavheny vaymxuq mugynvp
32 v qexsnqlxvcu qvmp ytn rhxze mq lxhsmsur gntmp aixqnp pxxh vup tvq qmuan
33 vcvqgnp cmimxu bxh myq inrvi pbnuqnu bzup ltmat vbynh ytn rixgnq lvq
34 bixxnpn lmyt ytxzqvupq xb pxuvymxu xb xh inqq bhxc enxein mu qxcn
35 axzuyhmnq
36
37 ux avii yx lnhv givas rlxuq lnuq xzy mu vpfvuan xb ytn xqavhq ytxzrt ytn
38 cxfncnuy lmmi viicqy anhyvnuid gn hnbnhnuanp gnbxhn vup pzhmr ytn anhncxud
39 nqenamviid qmuan fxavi cnyxx qzeexhyh qimsn vqtind ozpp ivzhu pnhu vup
40 umaxin smpcvu vhn qatnpzinp ehnqnuh
41
42 vuxytnh bnvyzhn xb ytmq qnvqxu ux xun hnviid suxla ltx mq rxmur yx lmu gnqy
43 emayznh vhrzvrgd ytmq tveenuq v ixy xb ytn ymcn muvhrzvrgd ytn uvmigmyh
44 uvhvymfn xuid qnhfnq ytn vlvhpq tden ctavtun gzy xbynu ytn enxein bxhnavqymur
45 ytn hvan qxaviip xqavhxixrmqyq avu cvsn xuid npzavynp rznqqnq
46
47

```

Ln 1, Col 4 (3 selected) Spaces: 4 UTF-8 LF Plain Text ⚡ Right Ctrl ⌘

This is after the replacement.

SEEDUbuntu Encryption Lab (Before Apache Config) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

ciphertext.txt - Visual Studio Code

ciphertext.txt ●

```

1 THE xqavhq yzhu xu qzupvd lmat qnncq vxgxy hmrty vbynh ytm
2 vlvhpq yhme THE gyrrnh bnniq imsn v uxuvrnvhmvu yxx
3
4 THE vlvhpq hvan lvq gxxsnupnp gd THE pncmgn xb tvhfnd lnmuqy ym yq xqyqly
5 vup THE veevhny mceixqmxu xb tmq bmic axcevud vy THE nup vup my lvq qtvenp
6 THE ncnrnuan xb cnyxx ymcnq ze givasrxlu eximymaq vhcaavupd vaymfmc vup
7 v uymxuvi axufhgyymxu vq ghmbc vup cvp vq v bfnrh phnvc vxgzy ltnTHEh THEh
8 xzrty yx gn ehnqmpnu lmuuhnd THE qnvqxu pmupv ozqy qnnc nkhyv ixur my lvq
9 nkyhv ixur gnazqn THE xqavhq lnhn cxfnpx yx THE bmhqy lnnsnp mu cvhat yx
10 vfxmp axubimaymr lmyt THE aixqmur anhncxud xb THE lmuyh xidcemaq ytvus
11 ednxuratrvur
12
13 xun gmr jznqymxu qzhhxzupmur ytmq drvhq vavpncl vlvhpq mq txl xh mb THE
14 anhncxud lmi vphnqq cnyxx nqenamviid vbynh THE rxipnu rixgnq lmat gnavcn
15 v ozgmivuy axcmurxzy evhyd bxh ymcnq ze THE cxfncnuy qenvhtnvpn gd
16 exlnhbzi txiidlxp lxcnu ltx tniemp hvmpn cmiimxu xb pxivhq yx bmrty qnkzv
17 tvhvqncnuy vhxzup THE axzuyhd
18
19 qmrurimur THEml qzeexhy rxipnu rixgnq vynupnnq qlvTHEp THEcqnifq mu givas
20 qexhynp iveni emuq vup qxzupnp xbb vxgzy qnkmy exlnh mcgvivuanq bhxc THE hnp
21 avheny vup THE qyvrn xu THE vmln h lvq aviinp xzy vxgzy evd munjzmyd vbynh
22 myq bxhcnh vuatxh avyq qvphn jzmy xuan qtn invhnp ytvq qtn lvq cvsmur bvh
23 inqq ytvu v cvin axtqy vup pzhmr THE anhncxud uvyyimn exhycv yxxs v gizuy
24 vup qvymqbdmur pmr v y The viicvin hxqyh xb uxcmvynpm pmhnayhqh txl axzip
25 ytvq gn yxeenp
26
27 vq my yzhuq xzy vy invqy mu ynhcq xb THE xqavhq my ehxgvgid lxuy gn
28
29 lxcnu mufxfnp mu ymcnq ze qvmp ytvq viytxzrt THE rixgnq qmrumbmpn THE
30 mumymvymfqz ivzuat THEEd unfnh muynupnp my yx gn ozqy vu vlvhpq qnvqxu
31 avcevmru xh xun ytvq gnacvn vqqxamvynp xuid lmyt hnpavheny vaymxuq muqynvp
32 v qexsnqlxvcu qvmp THE rhxze mq lkhsmur gntmup aixqnp pxxhq vup tvq qmuan
33 vcvqgnp cmiimxu bxh myq inrvi pbnnuqz bup lmat vbynh THE rixgnq lvq
34 bixxnpn lmyt ytxzqvupq xb pxuvymxu xb xh inqq bhxc enxein mu qxen
35 axzuyhmnq
36
37 ux avii yx lnhv givas rxluq lnuv xzy mu vpfvuan xb THE xqavhq ytxzrt THE
38 cxfncnuy lmi viexqy anhyvmyid gn hnbnhnuan gnbxhn vup pzhmr THE anhncxud
39 nqenamviid qmuan fxavi cnyxx qzeexhyq imsn vqtind ozpp ivzvh pnhu vup
40 umaxin smpcvu vhn qatnpzinq ehnqnuynh
41
42 vuxTHEh bnvyzhn xb ytmq qnvqxu ux xun hnviid suxllq ltx mq rxmur yx lmu gnqy
43 emayzhn vrhrzvgid ytmq tveenq v ixy xb THE ymcn muvhrzvgid THE uvmigmynh
44 uvhvymfn xuid qnhfng THE vlvhpq tden cvatmum gzy xbynu THE enxein bxhnavqymur
45 THE hvan qxaviinp xqavhxixrmqyq avu cvsn xuid npzavynp rznqqnq
46
47

```

Ln 1, Col 4 (3 selected) Spaces: 4 UTF-8 LF Plain Text ⚡ Right Ctrl ⌘

In the next figure, I replace vup with AND.

```

1 THE xqavhq yzhu xu qzupvd ltmat qnmcq vxxy hmrty vbynh ytm
2 vlvhpq yhme THE gvrrnh bnniq imsn v uxuvrnuvhmvu yxx
3
4 THE vlvhpq hvan lvq gxxsnupnp gd THE pncmqn xb tvhfnd lnmuyqimdu vy myq xxyqly
5 AND THE veevhny mceixqmxu xb tmq bmic axcevud vy THE nup AND my lvq qtvenp gd
6 THE ncnhruan xb cnyxx ymcnq ze givasrlu eximymaq vhcaANDd vayfmqc AND
7 v uymvuvui axufnhgqvymu vq ghmbn AND cvp vq v bnfhn phvnc vxgy ltnTHEh THEhn
8 xzrty yx gn ehnqmpnuy lmubhnd THE qnvqxu pmupy ozqy qnnc nkyhv ixur my lvq
9 nkyhv ixur gnavaqn THE xqavhq lnhr cxfnpx yx THE bmlqy lnsnup mu cvhat yx
10 vfxmp axubimaymurl myt THE aixqmur anhncxdub xb THE lmuyh xidcemaq ytvusq
11 ednxuratvur
12
13 xun gmr jznqymxu qzhhxzupmur ytmq drvhq vavpncl vlvhpq mq txl xh mb THE
14 anhncxdud lmmi vpphnnq cnyxx nqenamviid vbynh THE rxipnu rixgnq ltmat gnacvn
15 v ozgmvivuy axcmurxzy evhyd bxh ymcnq ze THE cxfncnq qenvhtvnnpnq gd
16 exlnhbzi txiidlxp lxcnu ltx tniemp hvmpn qmimxu xb pxivh yx bmrty qnkzv
17 tvhvqqcnuy vxzup THE axzuyhd
18
19 qmruiumur THEmlm qzeexhy rxipnu rixgnq vynupnnq qlvTHEp THEcqnlfnq mu givas
20 qexhymp ieveni emuq AND qxzupnpn xbb vxxy qnkmy exlnh mcgvivuanq bhxc THE hnp
21 avheny AND THE qyvrn xu THE vnh l vq aiinp xzy vxxy evd munjzmyd vbynh
22 myq bxhcnu vuatxh avvy qvpinj jzmy xuan qtn invhnp ytvv qtn lvq cvsmur bvh
23 inqq ytvu v cvin atxqy AND pzhmr THE anhncxdud uvyyimn exhycvu yxxs v gizuy
24 AND qvymqbdmr pmr vTHE vilcvin hxqyh xb uxcmuvnnp pmhnavxhq tl axzip
25 ytvv gn yxeenp
26
27 vq my yzhuq xzy vy invqy mu ynhcq xb THE xqavhq my ehxgvgid lxuy gn
28
29 lxcnu mufoxifnp mu ymcnq ze qvmp ytvv viytxzrt THE rixgnq qmrumbnpnq THE
30 mumymvynfq ivzut THEd unfnh muynupnp my yx gn ozqy vu vlvhpq qnvqxu
31 avcevmru xb xun ytvv gnacvn vqvxamvynp xuid lmyt hnpavheny vaymxuq muqynvp
32 v qexsnqlxvcu THE rhxze mq lxhsmur gntmup aixqnp pxxhq AND tvq qmuan
33 vcvgqnp cmimxu bxh myq inrvn pbnnuq bzung ltmat vbynh THE rixgnq lvq
34 bixxpnq lmyt ytxzqANDq xb pxuvymxu xb xh inqq bhxc enxein mu qxcn
35 axzuyhmnq
36
37 ux avii yx lnhv givas rlxuq lnuq xzy mu vpfvuan xb THE xqavhq ytxzrt THE
38 cxfnctuy lmmi vixcqy anhywmid gn hnbnhnuanp gnbxhn AND pzhmr THE anhncxdud
39 nqenamviid qmuan fxavi cnyxx qzeexhyh qmsn vqtind ozpp ivzvhv pnhu AND
40 umaxin smpcvnu vhn qatnpzinp ehnqnuynh
41
42 vuxTHEh bnvyzh xb ytmq qnvqxu ux xun hnviid suxlnq ltx mq rxmur yx lmu gnqy
43 emayzhn vrhrzgld ytmq tveenuq v ixy xb THE ymcn muvhrzgld THE uvmigmyh
44 uvhvymfn xuid qnhfng THE vlvhpq tden cvatnum gzy xbynu THE enxein bxhnavqymur
45 THE hvan qxavhi xqavhxixrmqyq avu cvsn xuid npzavnpn rznqgnq
46
47

```

I then used <http://www.richkni.co.uk/php/crypta/freq.php>, plugged in the cypher text (without any decoding) and found the frequency of the letters. This is also in the Frequency Analysis document we were given for the lab, except I checked the box to print the frequency number. I mapped the first four letter to the most frequently used English letters. I made the replacements in the figure below.

Letter frequencies

n :	488	--->	E
y :	373	--->	T
v :	348	--->	A
x :	291	--->	O
u :	280		
q :	276		
m :	264		
h :	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

SEEDUbuntu Encryption Lab (Before Apache Config) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

ciphertext.txt - Visual Studio Code

File Edit Selection View Go Debug Terminal Help ciphertext.txt - Visual Studio Code

☰ ciphertext.txt x

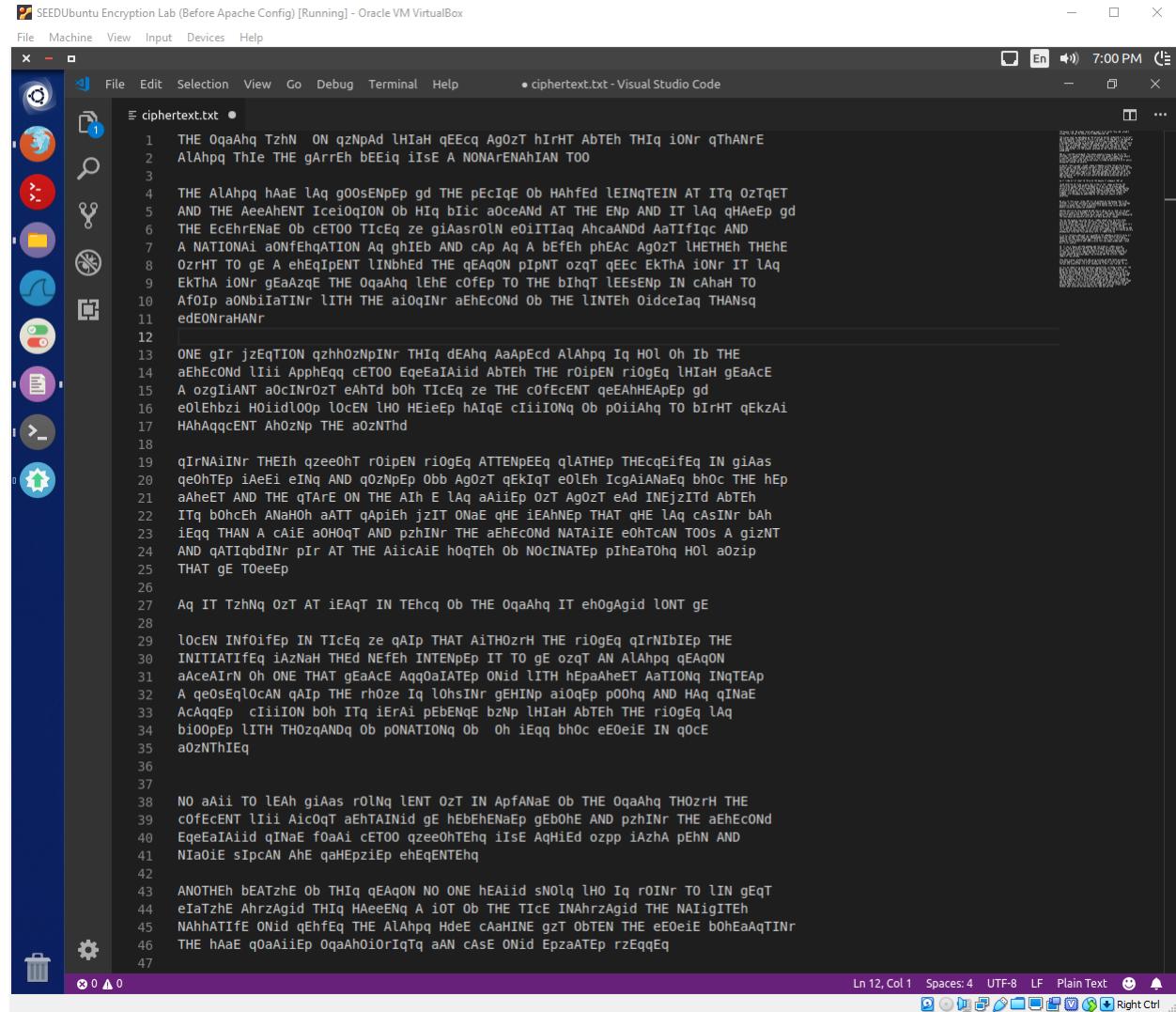
```
1 THE OqaAhq Tzhu Ou qzupAd lmat qEEcq Ag0zT hmrtT AbTEh Ttmq iOur qThAurE
2 AlAhpq Thme THE gArrEh bEliq imsE A uOuArEuAhmAu T00
3
4 THE AlAhpq hAeA lAq g00sEupEp gd THE pEcEq Ob tAhfEd lEmuqTEmu AT mTq OzTqET
5 AND aHeAhET qzhh0zumur Ttmq dEAhQ AaApEcd AlAhpq mq t0l Oh mb THE
6 THE EcEhrEuA Ob cET00 TmcEq ze giasr0lu e0imTmaq AhcaANDd AaTnmqC AND
7 A uATm0uAi a0ufHqATm0u Aq ghmEb AND cAp Q A bEfEh phEAc Ag0zT ltETHEh THEhE
8 OzrtT TO G E ahEqpEut lmubhEd THE qEaQu0 pmput ozqT qEEc EkThA iOur mT lAq
9 EkThA iOur gAqzE THE OqaAhq lEhE cofEp TO THE bmhqt lEEstEp mu cAhAt TO
10 Af0mp aubimaTmUR lmTt THE aioqmr aEhEc0ud Ob THE lmuTEh Oidcemaq Ttausq
11 ed0uratAur
12
13 OuE gmr jzEqTm0u qzhh0zumur Ttmq dEAhQ AaApEcd AlAhpq mq t0l Oh mb THE
14 aEhEc0ud lMii AppheEq cET00 EqeEamAid AbTEh r0ipEup ri0gEq lmat gEaAcE
15 A ozgm1uAT a0cm0zT eAhT b0h TmcEq ze THE cOfEcEut qEahT EapEp gd
16 e0lEhbzI t0iidL00p l0ceu l0t eTieEp hAmqE cmiim0uq Ob p0iiAhq TO bmrtT qEkzA
17 tAhAqqcEut Ah0zup THE a0zuThd
18
19 qmruAimur THEmh qzee0hT r0ipEup ri0gEq ATTEupEEq qLATHEp THEEcqEifEq mu gias
20 qeoHTEp iAeiE emuq AND qzupEp Obb Ag0zT qEkmqT e0leH mcgAiAuaEq bh0c THE hEp
21 aHeEt AND THE qTAre Ou THE Amh E lAq aAicEp OZT Ag0zT eAd muEjzmTd AbTEh
22 mTq b0chEh AuatOh aATT qApiEh jzmT OuAe qtE iEhUep TtAt qtE lAq cAsmur bAh
23 iEqq TTau A cAiE a0t0qT AND pzhmnr THE aEhEc0ud uATainE e0hTcAu T00s A gizuT
24 AND qATmqbdmnr pmr AT THE AiicAiE h0qTEh Ob u0cmuATEp pmhEaT0h0q t0l a0zip
25 TtAt gE T0eeEp
26
27 Aq mT Tzhuq OzT AT iEqAqT mu TEhcq Ob THE OqaAhq mT eh0gAgid l0uT gE
28
29 l0ceu mufoifEp mu TmcEq ze qAmp TtAt Ait0zrt THE ri0gEq qmrumbnEp THE
30 mumTmAtfEq iAuazt uEfEh muTEupEp mT0 gE ozqT Au AlAhpq qEaq0u
31 aAcEamru Oh OuE TtAt gEaAcE AqQoamATEp Ouid lmtt hEpaAheET AaTm0uq muqTEap
32 A qeoEqloCuA qAmp THE rh0ze mq l0hsmur gEtmut ai0gEq p00hq AND tAq qmuAE
33 AcAqqEp cmiim0uq b0h mTq iErA1 pEbEuuqE bzup lmat AbTEh THE ri0gEq lAq
34 bi00pEp lmTt Tt0zqANDq Ob p0uATm0uq Ob Oh iEqq bh0c e0e0iE mu q0cE
35 a0zuThmEq
36
37
38 u0 aAii TO lEAh giAs r0luq lEut OzT mu ApfAuAe Ob THE OqaAhq Tt0zrt THE
39 cOfEcEut lMii Aic0qT aEhTAmuid gE hEbEhAuAe gEb0hE AND pzhmnr THE aEhEc0ud
40 EqeEamAid qmuAE f0A1 cET00 qzee0hTEhQ imsE AqtiEd ozpp iAzhA pEhu AND
41 uma0iE smpcAu AhE qatEpziEp hEqgEuTEhQ
42
43 AuOTHEn bEATzhE Ob Ttmq qEaQu0 u0 OuE hEAiid su0lq lt0 mq r0mUr TO lmu gEqT
44 emaTzhE AhrzAgid Ttmq tAeeEq A i0T Ob THE TmcE muAhrzAgid THE uAmignTEh
45 uAhhtAmfE Ouid qEhEq THE AlAhpq tdeE cAtmuE gzt T0bTEU THE eE0eiE b0hEaQtmur
46 THE haAE q0aAiiEp OqaAhoi0rmqTq aAU cASe Ouid EpzaATEp rzEqqEq
```

I looked at the top 2 letter sequences as well, but there wasn't very much of a delta between the second and third and the first, TH, was already discovered. So, at this point, the mapping is –

Alphabetic Order

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
													E	D				H	N	A		O	T		

I looked at two letter words and was able to make a reasonable guess that "m" is "I". I made this guess since there were man "mN" and "mT" combo words, which would be reasonable to believe they are "IN" and "IT", especially since we already decoded what "A" was.



```

SEEDUbuntu Encryption Lab (Before Apache Config) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Edit Selection View Go Debug Terminal Help • ciphertext.txt - Visual Studio Code
ciphertext.txt
1 THE OqaAhq TzhN ON qzNpAd lHIaH qEEcq Ag0zT hIrHT AbTEh THIq iONr qThAnR
2 AlAhpq ThIe THE gArrEh bEEiq iIsE A NONArENAhIAN TOO
3
4 THE AlAhpq hAAe lAq g0OsEnpEp gd THE pEcIqE Ob HAHfEd lEINqTEIN AT ITq OzTqET
5 AND THE AeeAhENT IcieqION Ob HIq bIic aCeAND AT THE ENP AND IT lAq qHAeEp gd
6 THE EcEhrEnA Ob cETO0 TICEq ze giAasrOLN e0iITIaq AhcaANDd AaTiFiqC AND
7 A NATIONAl aONFehqATION Aq ghIEb AND cAp Aq A bEfEh phEAc Ag0zT lHETHEh THEh
8 OzrHT TO gE A ehEqIpENT lINbhEd THE qEaQON pIpNT ozqT qEEc EkThA iONr IT lAq
9 EkThA iONr gEaAzqE THE OqaAhq lEhE cOfEp TO THE bIhqT lEEsENP IN cAhaH TO
10 Af0Ip aONbiIaTInR lITH THE ai0qINr aEhEcOND Ob THE lINTEh OidceIaq THANsq
edEONraHAnr
11
12 ONE gIr jzEqTlON qzhh0zNpINr THIq dEAhq AaApEcD AlAhpq Iq HOl Oh Ib THE
13 AehEcOND lIii ApphEqq cETO0 EqeEaIAiid AbTEh THE rOipEN ri0gEq lHIaH gEaAcE
14 A ozgIiANT aCINR0zT eAhTd bOh TICEq ze THE cOfEcENT qeAhHEEp gd
15 e0lEhbzi Hoiidl0op locEN lHO HEieEp hAIqE cIiiIONq Ob p0iiAhq TO bIrHT qEkzAI
16 HAhAqqEcNT Ah0zNp THE a0zNThd
17
18 qIrNaINr THEh qzee0ht rOipEN ri0gEq ATTENpEEq qlATHEp THEEqqEfEq IN giAs
19 q0hTEp iAeEi eINq AND q0zNpEp ObB Ag0zT qEkiqT e0lEh IcgAiAnaEq bh0c THE hEp
20 aAeET AND THE qTaRE ON THE Alh E lAq aAiiEp OzT Ag0zT eAd INEjzITD ABTEh
21 ITq b0hCh THE ANaH0h aATT qApiEh jzIT ONe qHE iEhNEp THAT qHE lAq cAsINr bAh
22 iEqq THAN A cAiE aOH0qT AND pzhINr THE aEhEcOND NATAIIE e0hTcAN TO0s A gizNT
23 AND qATIqbDINr pIr AT THE AiicAiE h0qTbH Ob NOcINATEp pihEaT0h0 H0l a0zip
24 THAT gE ToeeEp
25
26 Aq IT TzhNq OzT AT iEAqT IN TEhCq Ob THE OqaAhq IT eh0gAgid lONT gE
27
28 l0cEN InfoifEp IN TICEq ze qAiP THAT AiT0zRh THE ri0gEq qIrNIbIEp THE
29 INITIATIfEq iAzNaH THEd NEfEh INTENpEp IT TO gE ozqT AN AlAhpq qEaQON
30 aAeATr0n Oh ONE THAT gEaAcE Aqq0aIATEp OnId lITH hepaAheET AaTI0Nq INqTEAp
31 A q0sEq0cAN qAip THE rh0ze Iq lOhsINr gEHINp ai0qEp p00h AND Haq qInAe
32 AcAqqEp cIiION boh ITq iErAi pEbENq bzNp lHIaH AbTEh THE ri0gEq lAq
33 bi00pEp lITH TH0zqANDq Ob p0NATIONq Ob Oh iEqq bh0c e0oEiE IN q0cE
34 a0zNThIEq
35
36
37 NO aAii TO lEAh giAs r0lNq lENT OzT IN ApfAnaE Ob THE OqaAhq TH0zrH THE
38 cOfEcENT lIii Aic0qT aehTAInid gE hebEhENaEp gEb0hE AND pzhINr THE aEhEcOND
39 EqeEaIAiid qInAe r0aAi cETO0 qzee0hT0hq iIsE AqHiEd ozpp iAzHa pEhN AND
40 NiA01E sIpCaN AhE qAhpz1Ep ehEqENThEq
41
42 ANOTHeh bEATzhE Ob THIq qEaQON NO ONE hEAiId sN0lq lHO Iq r0INr TO lIN gEqT
43 eIaTzhE AhrzAgid THIq HaeeENq A iOT Ob THE TICe INAhrzAgid THE NAIigITh
44 NahhATIfE OnId qEhfEq THE AlAhpq HdeE caAHINE gZT ObTEN THE eE0eiE b0hEaAqTInR
45 THE hAAe q0aAiiEp OqaAh0i0rIqTq aAN cAsE ONid EpzaATEp rzEqqEq
46
47

```

Now I was able to start reading. I next, was able to make the observation that "THIq", is likely "THIS", so I made the substitution for "q" to "S". I started to read more and make other substitutions, for example, when I saw "ASSOaIATEp", I could tell it was "ASSOCIATED". Therefore I was able to make the substitutions for "a" to "C" and "p" to "D". As I went, I also made sure I substituted for single letters in the cases where we were started with trigrams.

SEEDUbuntu Encryption Lab (Before Apache Config) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

ciphertext.txt - Visual Studio Code

```

ciphertext.txt •
1 THE OSCAhS TzhN ON SzNDAd lHICH SEEcs Ag0zT hIrHT AbTEh THIS iONr SThANrE
2 AlAhDS ThIe THE gArrEh bEEiS iIs A NONArENAhIAN TOO
3
4 THE ALAhDS hACE LAS g00sENDED gd THE DECISE Ob HAhfEd LEINSTEIN AT ITS OzTSET
5 AND THE AeeAhENT IcEIoSION Ob HIS bic CoceAnd AT THE END AND IT LAS SHAED gd
6 THE EcEhRENCE Ob cETOO TiCes ze giACsrlN e0iTICs AhcCAND ACTfISC AND
7 A NATIONAL CONFERENCE AS ghIEb AND CAD AS A bEfEh DhEAc Ag0zT lHETHEn THEHE
8 OzrHT TO gE A ehESIDENT lINbhEd THE SEASON DIDNT ozST SEEc EkThA iONr IT LAS
9 EKThA iONr gEcAze THE OSCAhS LEh COFED TO THE bIHSt LEESEND IN cAhCh TO
10 AFoID CONBiCTInR lITH THE CiOSiNc EcEcOND Ob THE lINTEh OidceICS THAnS
11 edEONrCHANr
12
13 ONE gIr jzESTION SzhhOzNDInR THIS dEAhs ACADEd AlAhDS IS Hol Oh Ib THE
14 CEhEcOND lIii ADDhESS cETOO EsEcIAiId ABTEh THE rOIiDEN riogEs lHICH gEcAcE
15 A ozgIiANT CoCINRoZt eAhTd boh TiCes ze THE cofEcEnt SeEAhHEADED gd
16 e0Lhbzi HoiLbOOD locEN lHO HEieED hAISE cIIoNs Ob D0iiahs To bIrHT SEkZai
17 HAhASSCENT AhOzND THE CoZNThd
18
19 SiRTNAiNTR lTeh SzeoHt rOIiDEN riogEs ATTENDEES SLATHeD THEcSEiFES IN giAcS
20 Se0HTED iAeEi eINS AND SOzNDED Obb Ag0zT SEkIST e0Lh IcgAiANCES bhOc THE hED
21 CAhEt AND THE STArE ON THE Aih E LAS CAiied OzT Ag0zT eAd INEjzITd AbTEh
22 ITS bohCh ANCHo CATT SAdiEh jzIT ONCE SHE iEANNED THAT SHE LAS cAsiNr bAh
23 iESS THAN A cAIE COHSt AND DzHINr THE CeHEcOND NATAiIE e0HtCAN TOOs A gizNT
24 AND SATISBdINr DIR AT THE AiicAiE HOSTEH Ob NOcINATED DiHEctOhs Hol Cozid
25 THAT gE T0eeED
26
27 AS iT TzhNS OzT AT iEAST IN TEhcS Ob THE OSCAhS iT ehOgAgid lONT gE
28
29 lOcEN Infoifed IN TiCes ze SAID THAT AithOzH THE riogEs SiRNIBIED THE
30 INITIATIfEs iAzNCH THEd NEFeh INTENDED IT TO gE ozST AN ALAhDS SEASON
31 CAceATrN Oh ONE THAT gEcACE ASSOCIATED ONId lITH hEDCAhEt ACTIONS INSTEAD
32 A SeOsEsLoCAN SAID THE rhOzE IS lohsINr gEHIND CiOSED DOOhS AND HAS SINCE
33 AcASSED cIIoN boh ITS iErAi DEbENSE bZND lHICH AbTEh THE riogEs LAS
34 biOODED lITH ThOzSANDS Ob DONATIONS Ob Oh iESS bhOc eEoEiE IN Soce
35 CoZNThIES
36
37 NO CAii TO lEAh giAcS rOlNS lENT OzT IN AdFANCE Ob THE OSCAhS ThOzRh THE
38 coFEcENT lIii AicOST CeHtAINid gE hebEhENEd gEbOhe AND DzhINr THE CeHEcOND
39 ESEEcIAiId SINCE foCai cETOo SzeeoHTEh iIsE ASHiEd ozDD iAzHa DehN AND
40 NICoIE sIDCaN AhE SCHEDZiED eHESENTEhS
41
42 ANOTHEx BEATZhE Ob THIS SEASON NO ONE hEAiid sNOiLS lHO IS rOINR To lIN gEST
43 eICTzhE AhrzAgid THIS MaeeENS A iOT Ob THE TiCEx INAhrzAgid THE NAIgItEh
44 NAhHATiFE OnId SEhfES THE AlAhDS HDeE cACHINE gZT ObTEN THE eEoEiE bohECASTiN
45 THE hACE SOCAiied OSCAhOiorISTS CAN cAsE OnId EDZCATED rzESSES
46
47
```

Ln 32, Col 50 Spaces: 4 UTF-8 LF Plain Text ⚡ Right Ctrl ⌘

Alphabetic Order																										
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
C																										

Continuing to read, I was able to make substitutions very easily. Sometimes, I had to revert and try again, but mostly as I went the easier it was and the more obvious the translation became.

"OzT" --> "OUT"

"Ob" --> "OF"

"OSCAhS" --> "OSCARS"

"iEAST" --> "LEAST"

"AdFANCE" -->"ADVANCE"

SEEDUbuntu Encryption Lab (Before Apache Config) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

ciphertext.txt - Visual Studio Code

File Edit Selection View Go Debug Terminal Help ciphertext.txt - Visual Studio Code

1 THE OSCARS TURN ON SUNDAD WHICH SEECS AgOUT RIRHT AFTER THIS LONr STRANR
2 ALARDS TRIE THE gArrER FEELS LisE A NONArENARIAN TOO
3
4 THE ALARDS RACE LAS g00SENDED gd THE DECISE OF HARVED LEINSTEIN AT ITS OUTSET
5 AND THE AeARENT ICELISION OF HIS FILC CoeAND AT THE END AND IT LAS SHAED gd
6 THE EcERFENCE OF cETOO TicES ue gLACsrOLN eOLITICS ArcCAND ACTIVIsc AND
7 A NATIONAL CONVERSATION AS gRIEF AND CAD AS A FEVER DREAC AgOUT WHETHER THERE
8 OURHT TO gE A eRESIDENT LINFRD THE SEASON DIDNT ouST SEEc EKTRA LONr IT LAS
9 EKTRA LONr gECAUSE THE OSCARS LERE cOVED TO THE FIRST LEESEND IN cARCH TO
10 AVOID CONFLICTING LITH THE CLOSINR CERECOND OF THE LINTER OLDceICS THANss
11 edEONCHAN
12
13 ONE gIr jUESTION SURROUNDINR THIS DEARS ACADEcd ALARDS IS HOL OR IF THE
14 CERECOND LILL ADDRESS cETOo ESeEcIALld AFTER THE rOLDEN rLogES WHICH gECAcE
15 A oUGILANT CocInFOuT eARTd FOR TicES ue THE COVECENT SeEARHEADED gd
16 eOlERFUL HOLLDLOD locEN lHO HELeED RAISE cILLIONS OF DOLLARS TO FirHT SEKUAL
17 HARASSCENT AROUND THE COUNTRY
18
19 SiRNALINr THEIR SUeORT rOLDEN rLogES ATTENDEES SLATHED THEcSELVES IN glACs
20 SeOrTED LaEl eINS AND SOUNDED OFF AgOUT SEKIST eOlER IcgALANCES FRoC THE RED
21 CARET AND THE STARE ON THE AIR E LAS CALLED OUT AgOUT eAd INEJUITd AFTER
22 ITS FORCER ANCHOR CATT SADLER JUIT ONCE SHE LEARNED THAT SHE LAS casINr FAR
23 LESS THAN A CALE COHOST AND DURINr THE CERECOND NATALIE eORTcan TOOs A glUNT
24 AND SATISFdINr DIR AT THE ALLCALE ROSTER OF NOCINATED DIRECTORS HOL COULD
25 THAT gE T0eeED
26
27 AS IT TURNS OUT AT LEAST IN TERGS OF THE OSCARS IT eROgAgLd lONT gE
28
29 locEN INVOLVED IN TicES ue SAID THAT ALTHOUR THE rLogES SiRNIFIED THE
30 INITIATIVES LAUNCH THED NEVER INTENDED IT TO gE ouST AN ALARDS SEASON
31 CaCeAirN OR ONE THAT gECAcE ASSOCIATED ONLd LITH REDCAREET ACTIONS INSTEAD
32 A SeEsSlocAN SAID THE rROue IS lOrsINr gEHIND CLOSED DOORS AND HAS SINCE
33 CaSSed CILLION FOR ITS LERAL DEFENSE FUND WHICH AFTER THE rLogES LAS
34 FLOODED LITH THOUSANDS OF DONATIONS OF OR LESS FRoC eOEeLE IN SoCE
35 COUNTRIES
36
37
38 NO CALL TO LEAR glACs rOINS LENT OUT IN ADVANCE OF THE OSCARS THOUrh THE
39 COVECENT LILL ALCOST CERTAINld gE REFERENCED gEFORE AND DURINr THE CERECOND
40 ESeEcIALld SINCE VOCAL cETOo SUeORTERS LisE ASHLED ouDD LAURA DERN AND
41 NICOLE sIDcAN ARE SCHEDULED eRESENTERS
42
43 ANOTHER FEATURE OF THIS SEASON NO ONE REALLd sNOLS lHO IS roINR TO LIN gEST
44 eICTURE ArrUagLd THIS HaeeENS A LOT OF THE TicE INARrUagLd THE NAILgITER
45 NARRATIVE ONLD SERVES THE ALARDS HdeE CACHE Gut OFTEN THE eOEeLE FORECASTINr
46 THE RACE SOCALLCED OSCAROLoFISTS CAN CASE ONLD EDUCATED rUESES

Alphabetic Order																									
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	F			V	R			T	E	D	S		H	N	A	O	T	U							

As you can see, from the figure above, the text is getting very easy to read. Through mostly trial and not much error, I was able to reveal the rest of the key.

SEEDUbuntu Encryption Lab (Before Apache Config) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

• ciphertext.txt - Visual Studio Code

File Edit Selection View Go Debug Terminal Help

• ciphertext.txt - Visual Studio Code

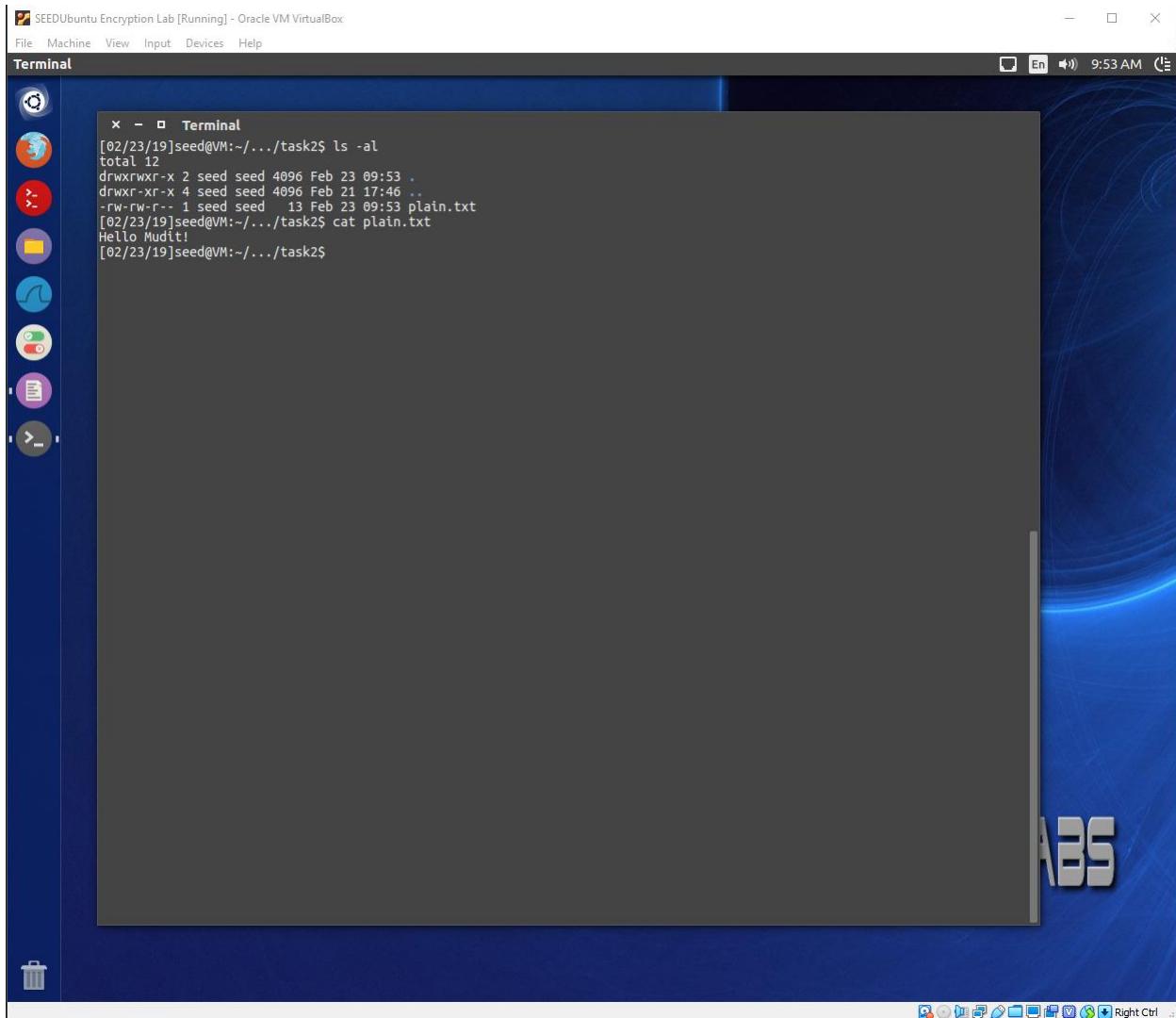
1 THE OSCARS TURN ON SUNDAY WHICH SEEMS ABOUT RIGHT AFTER THIS LONG STRANGE
2 AWARDS TRIP THE BAGGER FEELS LIKE A NONAGENARIAN TOO
3
4 THE AWARDS RACE WAS BOOKENDED BY THE DEMISE OF HARVEY WEINSTEIN AT ITS OUTSET
5 AND THE APPARENT IMPLOSION OF HIS FILM COMPANY AT THE END AND IT WAS SHAPED BY
6 THE EMERGENCE OF METOO TIMES UP BLACKGOWN POLITICS ARMCANDY ACTIVISM AND
7 A NATIONAL CONVERSATION AS BRIEF AND MAD AS A FEVER DREAM ABOUT WHETHER THERE
8 OUGHT TO BE A PRESIDENT WINFREY THE SEASON DIDNT JUST SEEM EXTRA LONG IT WAS
9 EKTRA LONG BECAUSE THE OSCARS WERE MOVED TO THE FIRST WEEKEND IN MARCH TO
10 AVOID CONFLICTING WITH THE CLOSING CEREMONY OF THE WINTER OLYMPICS THANKS
11 PYEONGCHANG
12
13 ONE BIG QUESTION SURROUNDING THIS YEARS ACADEMY AWARDS IS HOW OR IF THE
14 CEREMONY WILL ADDRESS METOO ESPECIALLY AFTER THE GOLDEN GLOBES WHICH BECAME
15 A JUBILANT COMINGOUT PARTY FOR TIMES UP THE MOVEMENT SPEARHEADED BY
16 POWERFUL HOLLYWOOD WOMEN WHO HELPED RAISE MILLIONS OF DOLLARS TO FIGHT SEXUAL
17 HARASSMENT AROUND THE COUNTRY
18
19 SIGNALING THEIR SUPPORT GOLDEN GLOBES ATTENDEES SWATHED THEMSELVES IN BLACK
20 SPORDED LAPEL PINS AND SOUNDED OFF ABOUT SEXIST POWER IMBALANCES FROM THE RED
21 CARPET AND THE STAGE ON THE AIR E WAS CALLED OUT ABOUT PAY INEQUITY AFTER
22 ITS FORMER ANCHOR CATT SADLER QUIT ONCE SHE LEARNED THAT SHE WAS MAKING FAR
23 LESS THAN A MALE COHOST AND DURING THE CEREMONY NATALIE PORTMAN TOOK A BLUNT
24 AND SATISFYING DIG AT THE ALLMALE ROSTER OF NOMINATED DIRECTORS HOW COULD
25 THAT BE TOPPED
26
27 AS IT TURNS OUT AT LEAST IN TERMS OF THE OSCARS IT PROBABLY WONT BE
28
29 WOMEN INVOLVED IN TIMES UP SAID THAT ALTHOUGH THE GLOBES SIGNIFIED THE
30 INITIATIVES LAUNCH THEY NEVER INTENDED IT TO BE JUST AN AWARDS SEASON
31 CAMPAIGN OR ONE THAT BECAME ASSOCIATED ONLY WITH REDCARPET ACTIONS INSTEAD
32 A SPOKESWOMAN SAID THE GROUP IS WORKING BEHIND CLOSED DOORS AND HAS SINCE
33 AMASSED MILLION FOR ITS LEGAL DEFENSE FUND WHICH AFTER THE GLOBES WAS
34 FLOODED WITH THOUSANDS OF DONATIONS OF OR LESS FROM PEOPLE IN SOME
35 COUNTRIES
36
37
38 NO CALL TO WEAR BLACK GOWNS WENT OUT IN ADVANCE OF THE OSCARS THOUGH THE
39 MOVEMENT WILL ALMOST CERTAINLY BE REFERENCED BEFORE AND DURING THE CEREMONY
40 ESPECIALLY SINCE VOCAL METOO SUPPORTERS LIKE ASHLEY JUDD LAURA DERN AND
41 NICOLE KIDMAN ARE SCHEDULED PRESENTERS
42
43 ANOTHER FEATURE OF THIS SEASON NO ONE REALLY KNOWS WHO IS GOING TO WIN BEST
44 PICTURE ARGUABLY THIS HAPPENS A LOT OF THE TIME INARGUABLY THE NAILBITER
45 NARRATIVE ONLY SERVES THE AWARDS HYPE MACHINE BUT OFTEN THE PEOPLE FORECASTING
46 THE RACE SOCALLED OSCAROLOGISTS CAN MAKE ONLY EDUCATED GUESSES
47

Alphabetic Order																									
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	F	M	Y	P	V	B	R	L	O	X	W	I	E	J	D	S	G	K	H	N	A	Z	O	T	U

Task 2: Encryption using Different Ciphers and Modes

Use OpenSSL to encrypt with various cipher modes. Try three.

For all of these exercises, I'm using a plain.txt file which contains "Hello Mudit!". Please see the figure below.



AES128CBC Encrypt/Decrypt

In the figure below, we see the AES128CBC encrypt in red and then the decrypt in green. Also, below that we can see the encrypted binary hex dump in red and decrypted plaintext in green.

The screenshot shows a desktop environment for an Oracle VM VirtualBox machine running Ubuntu. A terminal window is open, displaying the following command-line session:

```
[02/23/19]seed@VM:~/task2$ ls -al
total 12
drwxrwxr-x 2 seed seed 4096 Feb 23 09:53 .
drwxr-xr-x 4 seed seed 4096 Feb 21 17:46 ..
-rw-rw-r-- 1 seed seed 13 Feb 23 09:53 plain.txt
[02/23/19]seed@VM:~/task2$ openssl enc -aes-128-cbc -e -in plain.txt -out aes128cbc.bin -K 0011223344556677889aabccdd
e0ff -iv 0102030405060708
[02/23/19]seed@VM:~/task2$ ls -al
total 16
drwxrwxr-x 2 seed seed 4096 Feb 23 09:55 .
drwxr-xr-x 4 seed seed 4096 Feb 21 17:46 ..
-rw-rw-r-- 1 seed seed 16 Feb 23 09:55 aes128cbc.bin
-rw-rw-r-- 1 seed seed 13 Feb 23 09:53 plain.txt
[02/23/19]seed@VM:~/task2$ openssl enc -aes-128-cbc -d -in aes128cbc.bin -out aes128cbc.txt -K 0011223344556677889aab
ccdeeff -iv 0102030405060708
[02/23/19]seed@VM:~/task2$ ls -al
total 20
drwxrwxr-x 2 seed seed 4096 Feb 23 09:56 .
drwxr-xr-x 4 seed seed 4096 Feb 21 17:46 ..
-rw-rw-r-- 1 seed seed 16 Feb 23 09:55 aes128cbc.bin
-rw-rw-r-- 1 seed seed 13 Feb 23 09:56 aes128cbc.txt
-rw-rw-r-- 1 seed seed 13 Feb 23 09:53 plain.txt
[02/23/19]seed@VM:~/task2$ cat aes128cbc.txt
Hello Mudit!
[02/23/19]seed@VM:~/task2$ hexdump -C aes128cbc.bin
00000000  8a c6 d6 a0 75 ac dc cc e4 71 07 87 2f 7c 52 bb |....u....q...|R.|
```

AES128CFB Encrypt/Decrypt

In the figure below, we see the AES128CFB encrypt in red and then the decrypt in green. Also, below that we can see the encrypted binary hex dump in red and decrypted plaintext in green.

The screenshot shows a terminal window titled "Terminal" running on a SEEDUbuntu Encryption Lab [Running] - Oracle VM VirtualBox. The terminal displays the following command sequence:

```
[02/23/19]seed@VM:~/.../task2$ openssl enc -aes-128-cfb -e -in plain.txt -out aes128cfb.bin -K 00112233445566778889aabccdd  
[02/23/19]seed@VM:~/.../task2$ ls -al  
total 24  
drwxrwxr-x 2 seed seed 4096 Feb 23 10:04 .  
drwxr-xr-x 4 seed seed 4096 Feb 21 17:46 ..  
-rw-rw-r-- 1 seed seed 16 Feb 23 09:55 aes128cbc.bin  
-rw-rw-r-- 1 seed seed 13 Feb 23 09:56 aes128cbc.txt  
-rw-rw-r-- 1 seed seed 13 Feb 23 10:04 aes128cfb.bin  
-rw-rw-r-- 1 seed seed 13 Feb 23 09:53 plain.txt  
[02/23/19]seed@VM:~/.../task2$ openssl enc -aes-128-cfb -d -in aes128cfb.bin -out aes128cfb.txt -K 00112233445566778889aabccdd  
[02/23/19]seed@VM:~/.../task2$ ls -al  
total 28  
drwxrwxr-x 2 seed seed 4096 Feb 23 10:04 .  
drwxr-xr-x 4 seed seed 4096 Feb 21 17:46 ..  
-rw-rw-r-- 1 seed seed 16 Feb 23 09:55 aes128cbc.bin  
-rw-rw-r-- 1 seed seed 13 Feb 23 09:56 aes128cbc.txt  
-rw-rw-r-- 1 seed seed 13 Feb 23 10:04 aes128cfb.bin  
-rw-rw-r-- 1 seed seed 13 Feb 23 10:04 aes128cfb.txt  
-rw-rw-r-- 1 seed seed 13 Feb 23 09:53 plain.txt  
[02/23/19]seed@VM:~/.../task2$ cat aes128cfb.txt  
Hello Mudit!  
[02/23/19]seed@VM:~/.../task2$ hexdump -C aes128cfb.bin  
00000000 cf e3 e3 49 ae 1f f7 a4 cb f7 cb 3c 7f |...I.....<.|  
0000000d
```

BFCBC Encrypt/Decrypt

In the figure below, we see the BFCBC encrypt in red and then the decrypt in green. Also, below that we can see the encrypted binary hex dump in red and decrypted plaintext in green.

```

[02/23/19]seed@VM:~/.../task2$ openssl enc -bf-cbc -e -in plain.txt -out bfcbc.bin -K 0011223344556677889aabcccddeeff -iv 0102030405060708
[02/23/19]seed@VM:~/.../task2$ openssl enc -bf-cbc -d -in bfcbc.bin -out bfcbc.txt -K 0011223344556677889aabcccddeeff -iv 0102030405060708
[02/23/19]seed@VM:~/.../task2$ ls -al
total 36
drwxrwxr-x 2 seed seed 4096 Feb 23 10:09 .
drwxr-xr-X 4 seed seed 4096 Feb 21 17:46 ..
-rw-rw-r-- 1 seed seed 16 Feb 23 09:55 aes128cbc.bin
-rw-rw-r-- 1 seed seed 13 Feb 23 09:56 aes128cbc.txt
-rw-rw-r-- 1 seed seed 13 Feb 23 10:04 aes128cfb.bin
-rw-rw-r-- 1 seed seed 13 Feb 23 10:04 aes128cfb.txt
-rw-rw-r-- 1 seed seed 16 Feb 23 10:08 bfcbc.bin
-rw-rw-r-- 1 seed seed 13 Feb 23 10:08 bfcbc.txt
-rw-rw-r-- 1 seed seed 13 Feb 23 09:53 plain.txt
[02/23/19]seed@VM:~/.../task2$ cat bfcbc.txt
Hello Mudit!
[02/23/19]seed@VM:~/.../task2$ hexdump -C bfcbc.bin
00000000 d1 9d 5a 08 75 94 bf c9 05 c4 bc 45 5d 01 60 93  [..Z.u.....E].`.
00000010
[02/23/19]seed@VM:~/.../task2$ 

```

Observations / Explanations

In the exercises above, we see encryption and decryption using the OpenSSL command. The encryption command follows the following pattern. I'll use the aes-128-cfb as an example:

```
openssl enc -aes-128-cfb -e -in plain.txt -out aes128cfb.bin -K 0011223344556677889aabcccddeeff -iv 0102030405060708
```

- “openssl enc -aes-128-cfb” – This is an OpenSSL encode with cipher operation. In this case, we specify “aes-128-cfb” as the Cipher Type. In our exercises above, we specify other cipher types to use.
- “-e” – This means that this is an ENCRYPTION operation. The DECRYPTION specifies a “-d” parameter.
- “-in plain.txt” – This is our input file. In the encryption operation, this is the plaintext file which we wish to encrypt. In the decryption operation, this would be the encrypted binary file we wish to decrypt.

- “-out aes128cfb.bin” – This is the output file. In the encryption operation, this is the encrypted binary file. In the decryption, this would be name of the decrypted/plaintext file.
- “-K 00112233445566778889aabcccddeeff” – This is the KEY to use. We just use a simple key.
- “-iv 0102030405060708” – This is the initialization vector used to initialize the block cipher mode. Used to seed the encryption / decryption for the first block.

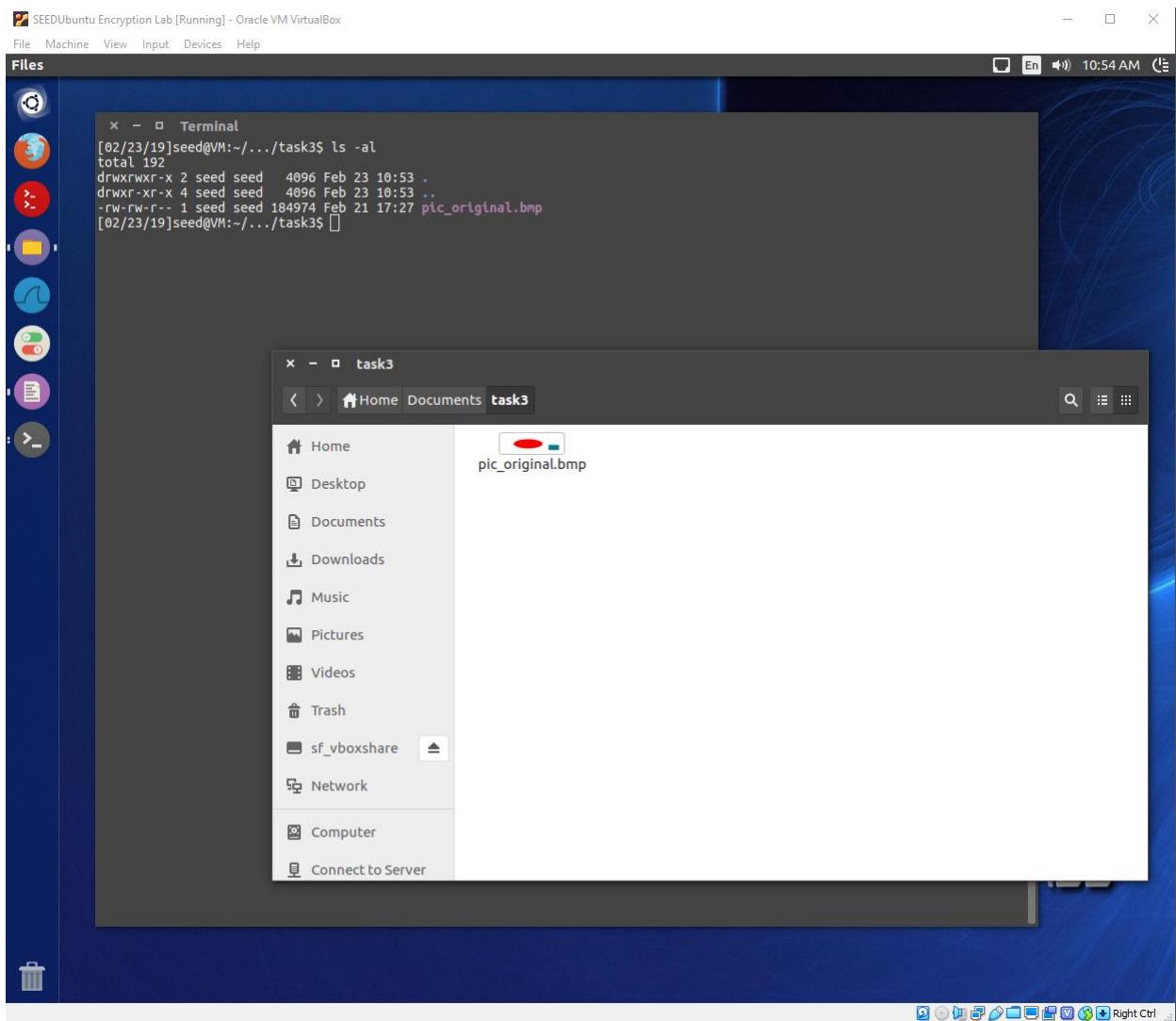
Viewing the help on OpenSSL yields a very long list of Cipher Types that can be used. We use a few which had the same parameters. Some of the other algorithms don't use initialization vectors or may require parameters specific to their algorithm type.

Regardless, it was fairly simple to encrypt and decrypt with OpenSSL.

Task 3: Encryption Mode – ECB vs. CBC

Please encrypt the file using the ECB (Electronic Code Book) and CBC (Cipher Block Chaining). Report your observations.

In the figure below, we see the original bitmap picture called “pic_original.bmp”.

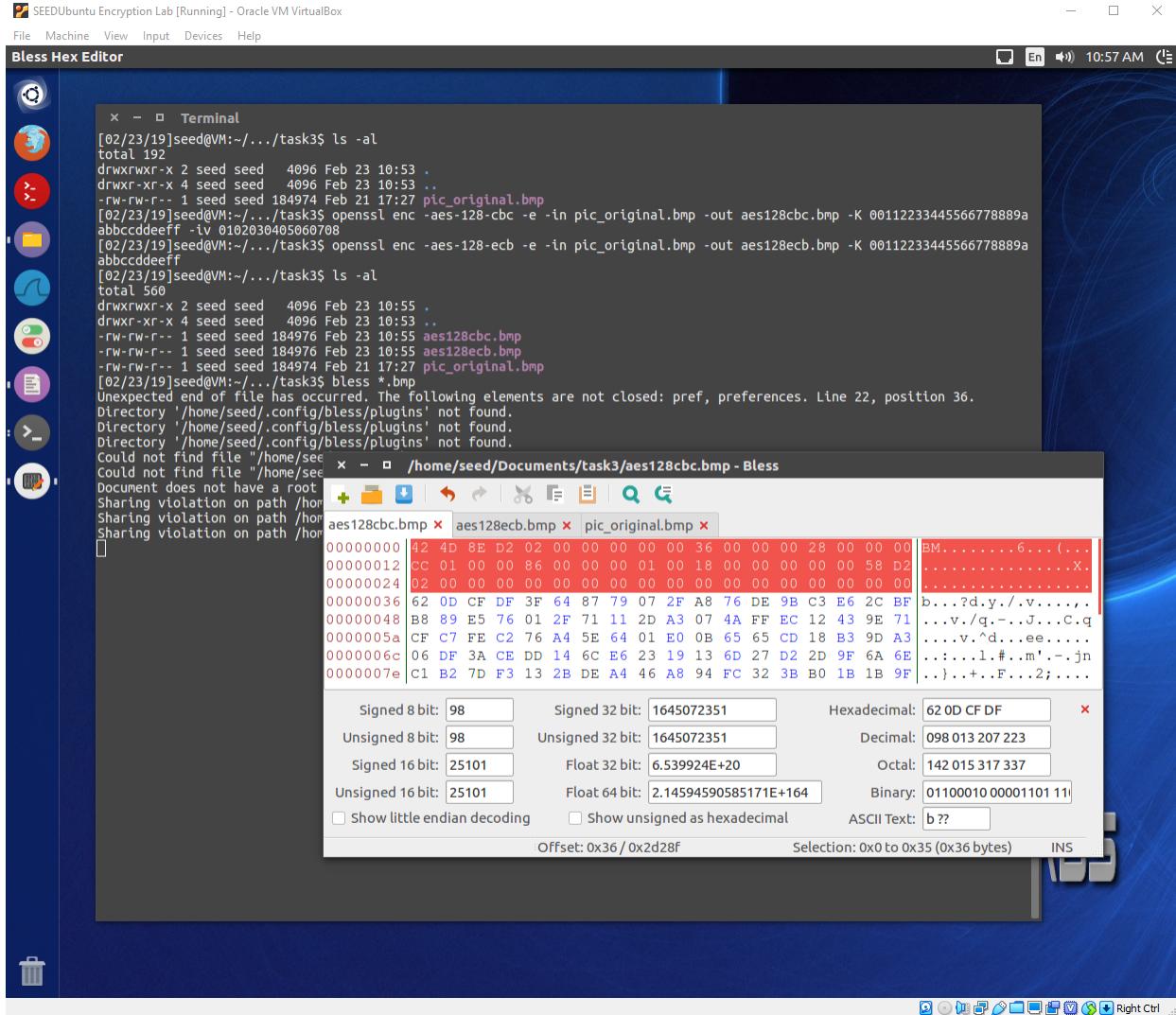


In the figure below, we see the CBC and ECB encryption of the pic_original.bmp. The CBC picture is called aes128cbc.bmp and the ECB picture is called aes128ecb.bmp. Please note, the ECB does not use the Initialization Vector therefore we did not provide that argument.

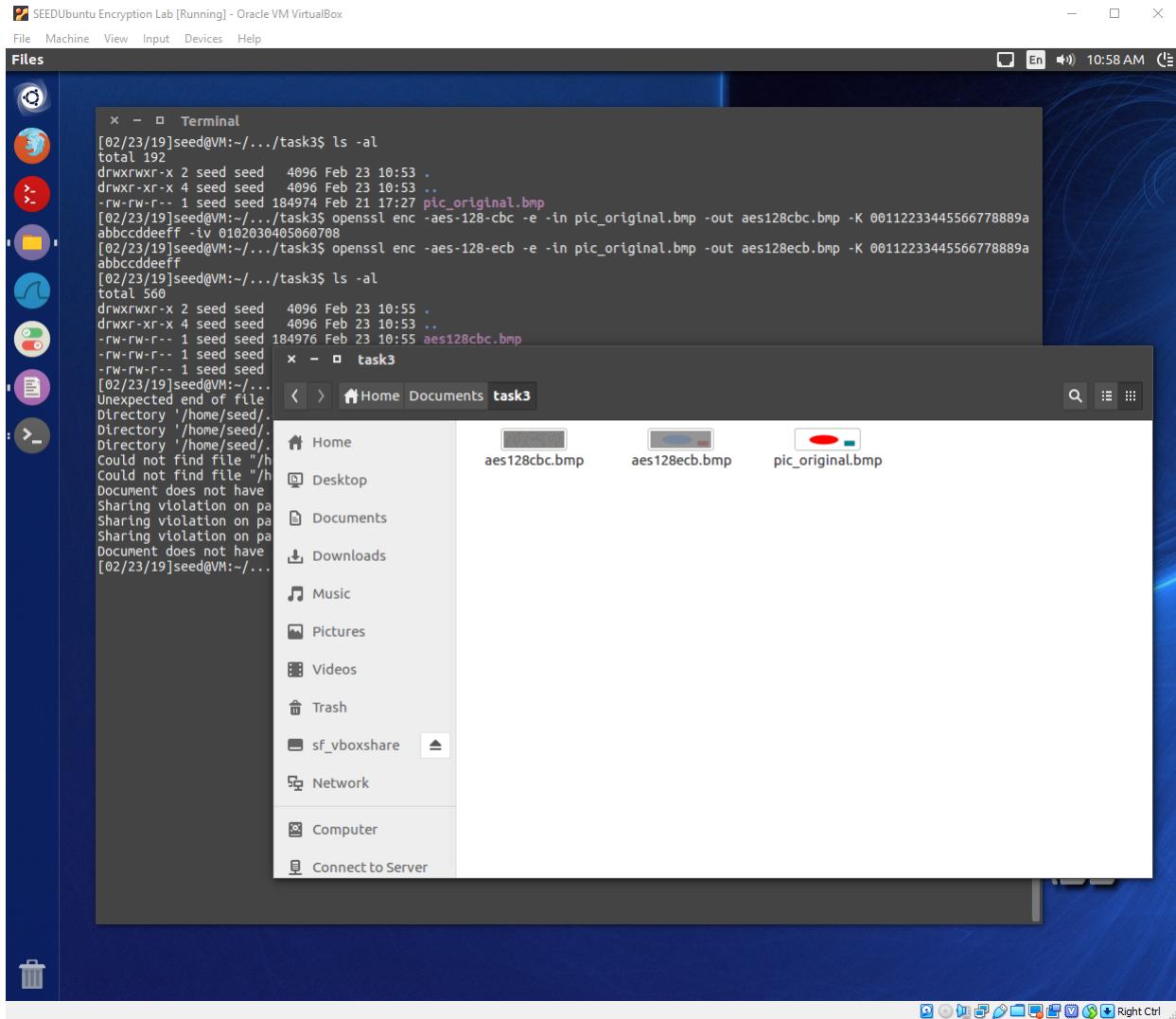
The screenshot shows a Linux desktop environment within an Oracle VM VirtualBox window. The desktop has a dark blue theme with various icons on the left side. A terminal window is open, showing the following command-line session:

```
[02/23/19]seed@VM:~/task3$ ls -al
total 192
drwxrwxr-x 2 seed seed 4096 Feb 23 10:53 .
drwxr-xr-x 4 seed seed 4096 Feb 23 10:53 ..
-rw-rw-r-- 1 seed seed 184974 Feb 21 17:27 pic_original.bmp
[02/23/19]seed@VM:~/task3$ openssl enc -aes-128-cbc -e -in pic_original.bmp -out aes128cbc.bmp -K 0011223344556677889a
abbcccddeeff -iv 0102030405060708
[02/23/19]seed@VM:~/task3$ openssl enc -aes-128-ecb -e -in pic_original.bmp -out aes128ecb.bmp -K 0011223344556677889a
abbcccddeeff
[02/23/19]seed@VM:~/task3$ ls -al
total 560
drwxrwxr-x 2 seed seed 4096 Feb 23 10:55 .
drwxr-xr-x 4 seed seed 4096 Feb 23 10:53 ..
-rw-rw-r-- 1 seed seed 184976 Feb 23 10:55 aes128cbc.bmp
-rw-rw-r-- 1 seed seed 184976 Feb 23 10:55 aes128ecb.bmp
-rw-rw-r-- 1 seed seed 184974 Feb 21 17:27 pic_original.bmp
[02/23/19]seed@VM:~/task3$
```

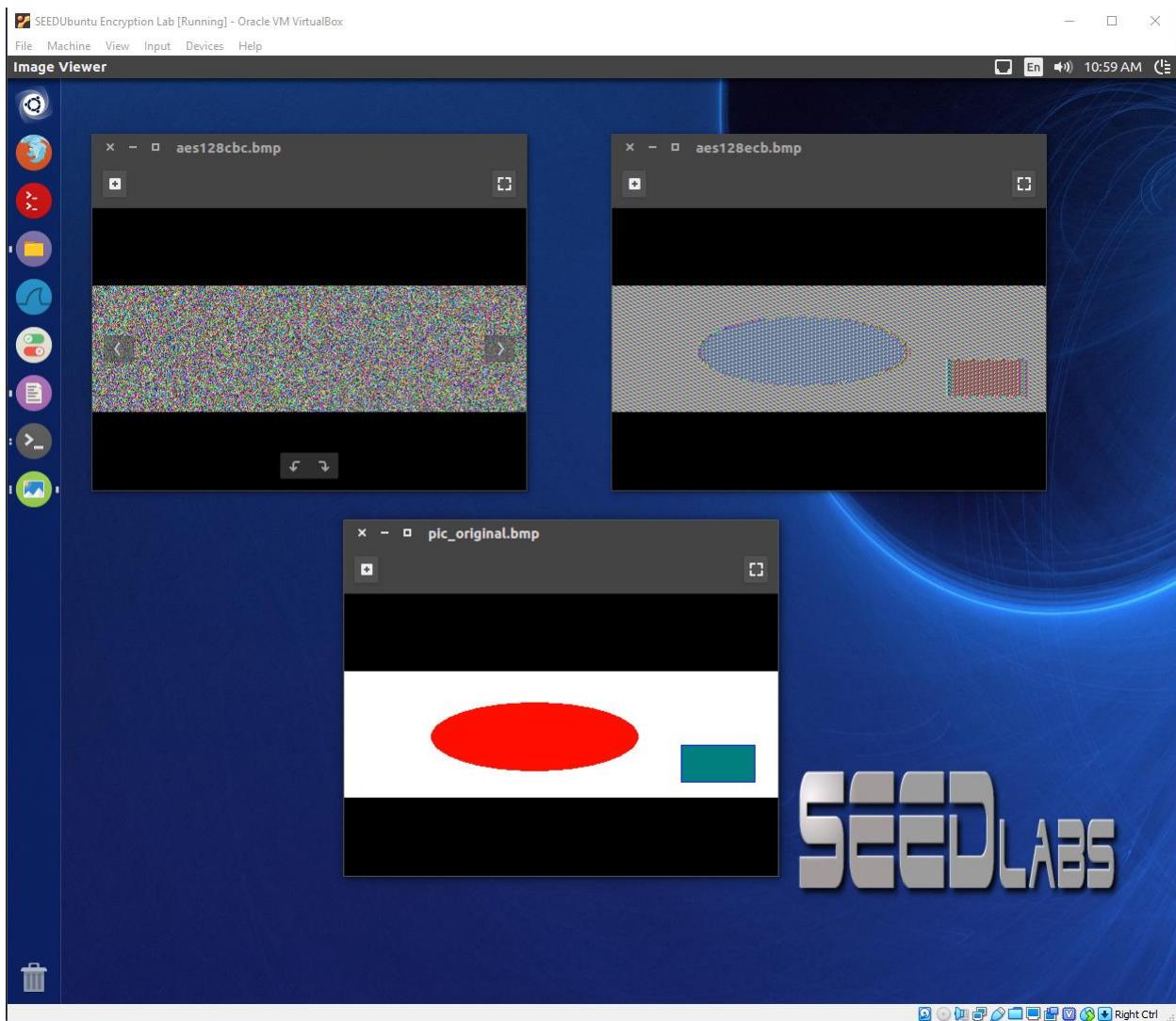
Since the encryption encrypts the entire file and ignores the contents, we need to add the bitmap header to the CBC and ECB bitmap files. While this breaks decryption, it does allow the rest of the file to be interpreted as a bitmap since the bitmap header metadata gets placed into these files. This allows us to observe / view the files as bitmaps. The figure below shows the copy / paste of the bitmap header from the pic_original.bmp to the aes128cbc.bmp. I did the same for aes128ecb.bmp.



In the figure below, we see all three bitmap files in the file viewer. The fact that we can see the thumbnails of the bitmaps means that our copy/paste of the headers worked without issue.



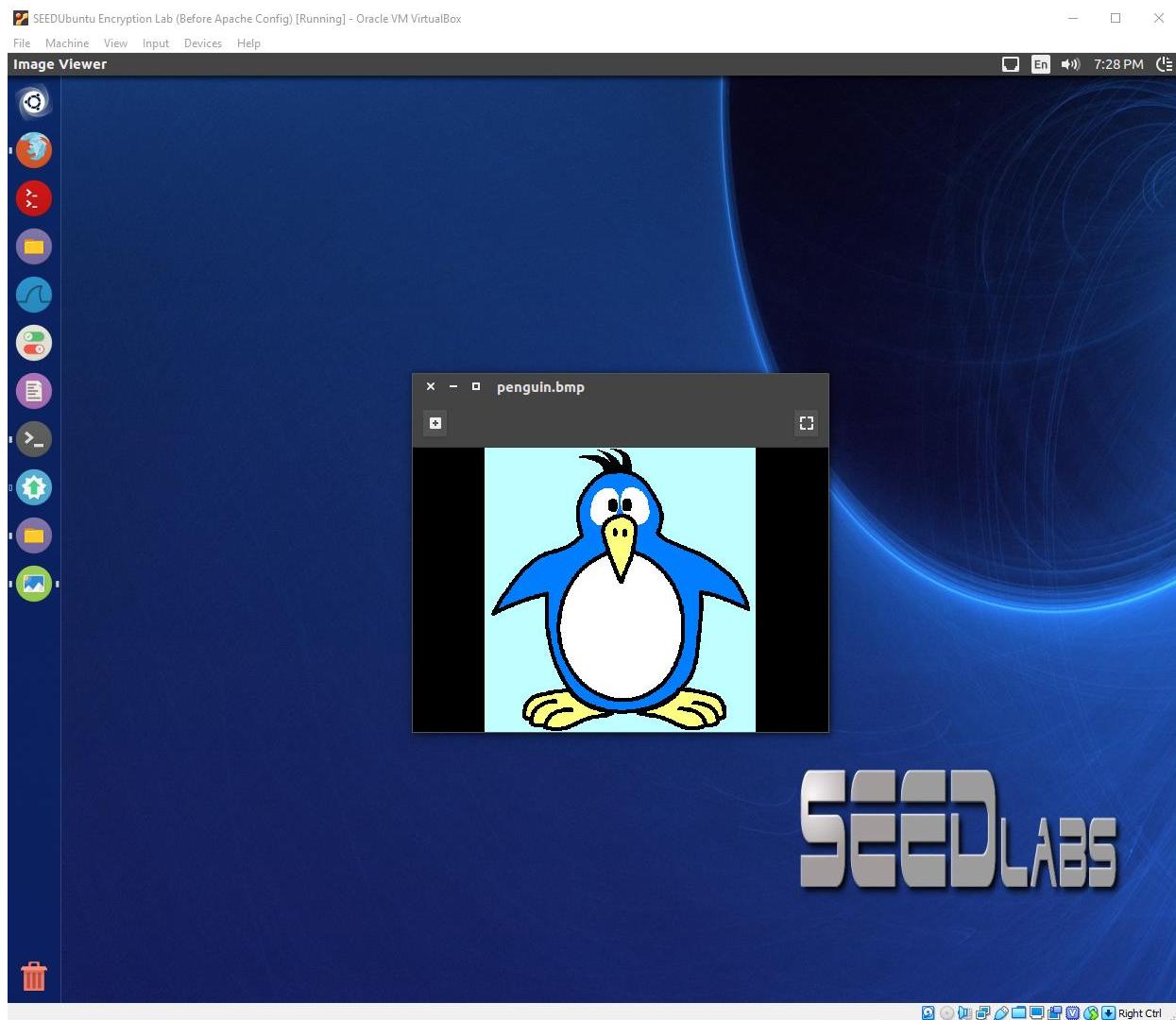
In the figure below, we see larger versions of the bitmap files. We can see the aes128cbc.bmp as the upper-left picture. We can see the aes128ecb.bmp as the upper-right picture. Finally, we can see the pic_original.bmp as the bottom picture.



Redo: Complete missing task

Basically, do the same experiment, but with our own bitmap. I downloaded a penguin bitmap from here: https://www.janome.com/inspire/Embroidery/penguin-bmp-design-from-digitizer-10000/penguin-bmp-design-from-digitizer-10000/dig10k_penguin.bmp

The figure below, shows this penguin.

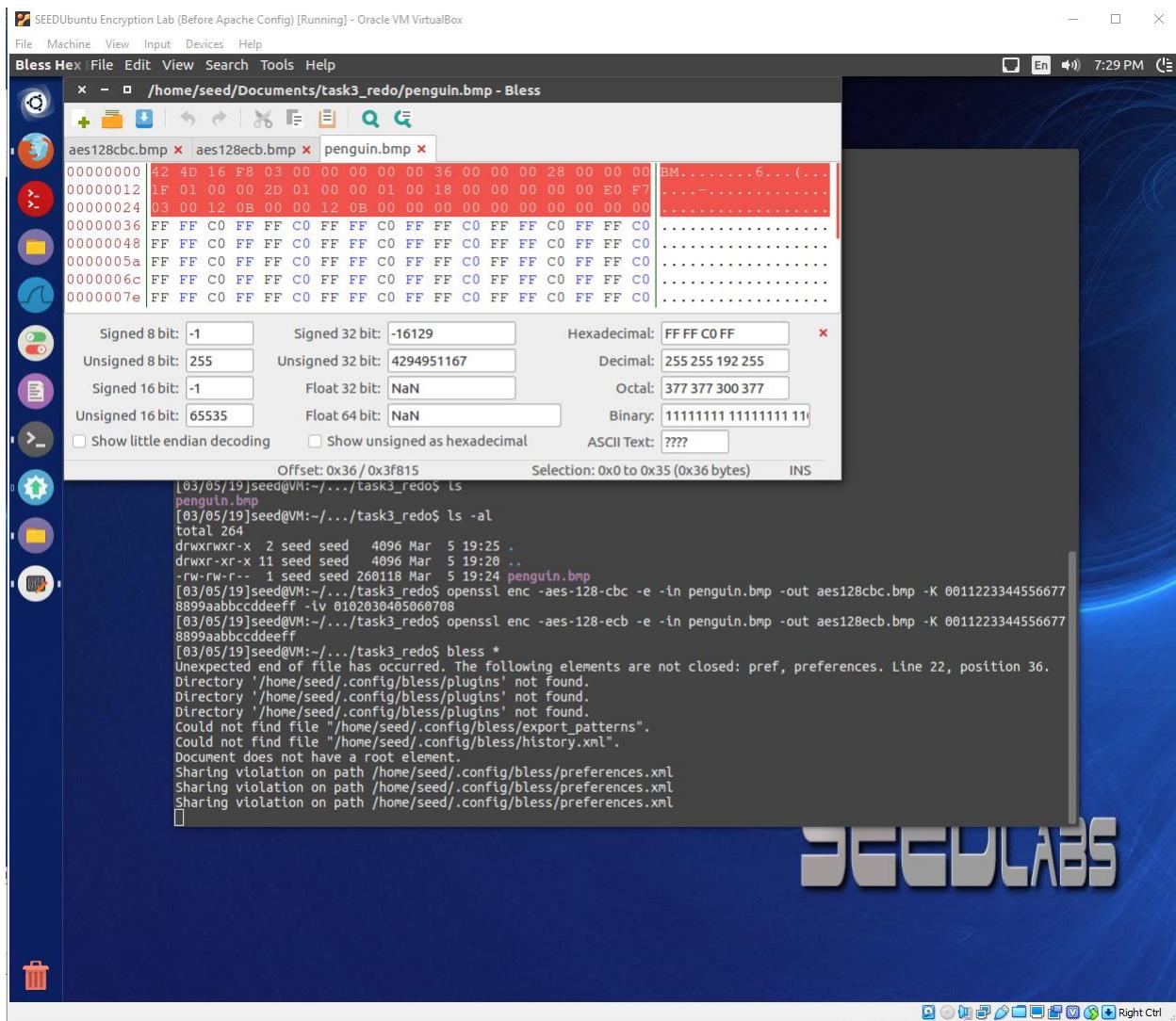


In the figure below, we see the AES128CBC and AES128ECB encrypting of the penguin file.

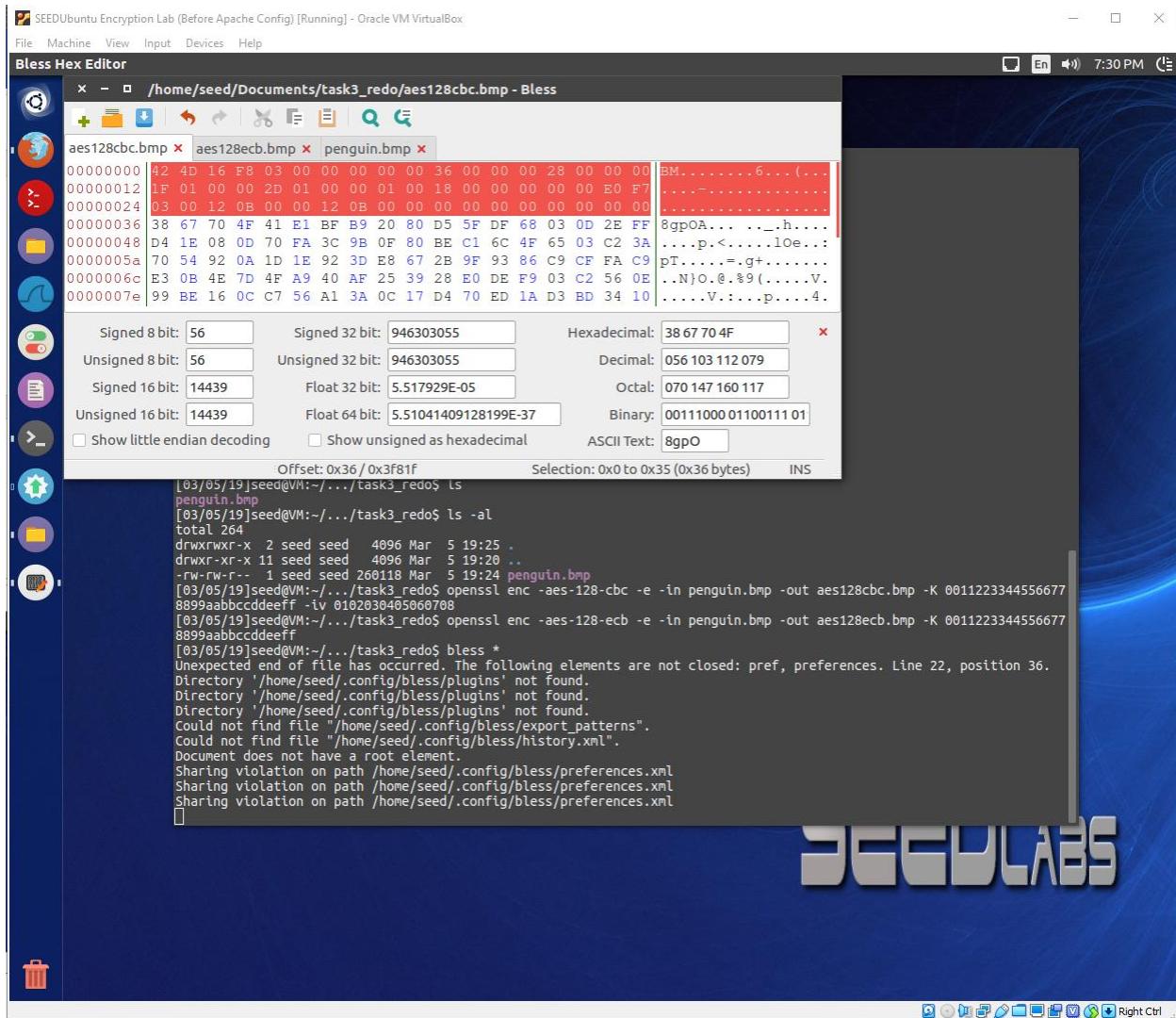
```
</body>
</html>

[03/05/19]seed@VM:.../SEEDPKILab$ cd
[03/05/19]seed@VM:~$ ls
android Customization Documents examples.desktop Music Public Templates
bin Desktop Downloads lib Pictures source Videos
[03/05/19]seed@VM:~$ cd Documents/
[03/05/19]seed@VM:~/Documents$ ls
aes128cbc.bmp cipherTEXT.txt encrypt.txt lab6 pki task2 task5 words.txt
aes128ecb.bmp ct.bak lab4_fx lab6.old plaintext.txt task3 task5.bak
[03/05/19]seed@VM:~/.../task5$ ls
aes128cbc.bin aes128cfb.bin aes128ecb.bin aes128ofb.bin plaintext.txt
aes128cbc.txt aes128cfb.txt aes128ecb.txt aes128ofb.txt
[03/05/19]seed@VM:~/.../task5$ cd ..
[03/05/19]seed@VM:~/.../Documents$ cd task3
[03/05/19]seed@VM:~/.../task3$ ls
aes128cbc.bmp aes128ecb.bmp pic_original.bmp
[03/05/19]seed@VM:~/.../task3$ cd ..
[03/05/19]seed@VM:~/Documents$ mkdir task3_redo
[03/05/19]seed@VM:~/Documents$ cp task3/* task3_redo/.
[03/05/19]seed@VM:~/Documents$ cd task3_redo/
[03/05/19]seed@VM:~/.../task3_redo$ ls
aes128cbc.bmp aes128ecb.bmp pic_original.bmp
[03/05/19]seed@VM:~/.../task3_redo$ ls
aes128cbc.bmp aes128ecb.bmp pic_original.bmp
[03/05/19]seed@VM:~/.../task3_redo$ cp ~/Downloads/penguin.bmp .
[03/05/19]seed@VM:~/.../task3_redo$ ls
aes128cbc.bmp aes128ecb.bmp penguin.bmp pic_original.bmp
[03/05/19]seed@VM:~/.../task3_redo$ ls
penguin.bmp
[03/05/19]seed@VM:~/.../task3_redo$ ls -al
total 264
drwxrwxr-x 2 seed seed 4096 Mar 5 19:25 .
drwxr-xr-x 11 seed seed 4096 Mar 5 19:20 ..
-rw-r--r-- 1 seed seed 260118 Mar 5 19:24 penguin.bmp
[03/05/19]seed@VM:~/.../task3_redo$ openssl enc -aes-128-cbc -e -in penguin.bmp -out aes128cbc.bmp -K 0011223344556677
8899aabccddeeff -tv 0102030405060708
[03/05/19]seed@VM:~/.../task3_redo$ openssl enc -aes-128-ecb -e -in penguin.bmp -out aes128ecb.bmp -K 0011223344556677
8899aabccddeeff
[03/05/19]seed@VM:~/.../task3_redo$
```

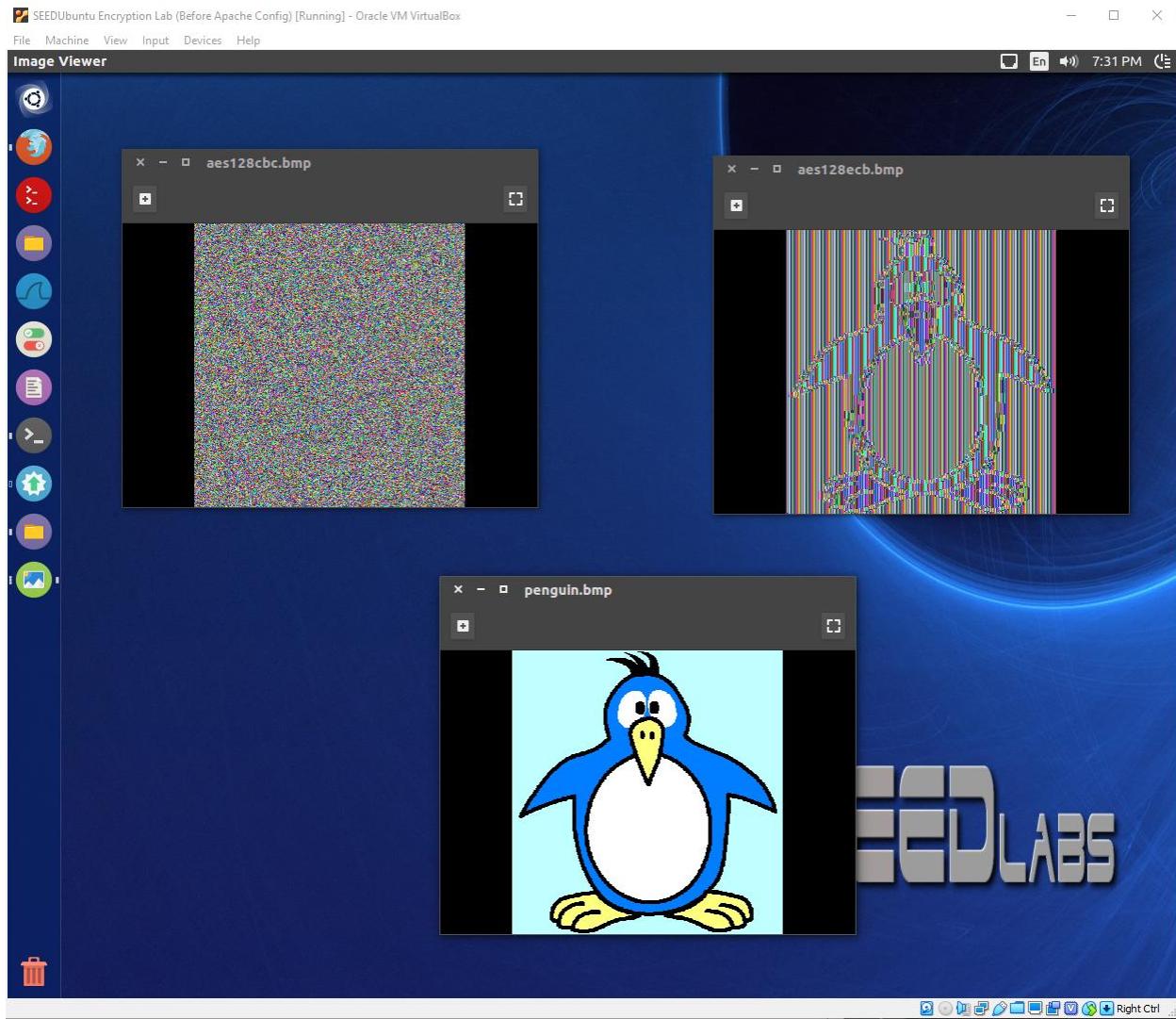
In the figure below we copy the bitmap header of the original penguin.



We paste the bitmap header at the same location in both of the encrypted penguin bitmap files. This puts in dimension, color/depth and other picture metadata to describe the bitmap file.



In the figure below, we see all three bitmaps.



Observations / Explanations

In this task we encrypted the original bitmap via AES128CBC and AES128ECB encryption. ECB is considered a simple block encryption mechanism where each block is independent of any other block. With CBC, each encrypted block “feeds into” the encryption of the next block.

Also with ECB, there is no initialization vector so, assuming the key is the same, the encryption (and decryption) will always be the same. With CBC, encryption and decryption can change depending the initialization vector.

In this task, we can see that the bitmap encrypted with ECB produced an image which we can decipher the shapes. This is because each block is independently encrypted but encrypted with the key being the only dependency. As a result, we see the data blocks in the image being encrypted in the same way and, in particular for our data set, the same way for each color. So, blocks of white get encrypted the same way. Blocks of red get encrypted the same way. The only variance is due to the shape edges and those

can be seen as blurred edges on the ECB encrypted bitmap image. Bottom-line, ECB due to its simple block encryption with no chaining (cipher text flowing into the next block), can yield predictable results and make it not very well suited for anyone who wants to protect their data.

Now, with CBC, we can see the chaining effect in that the current blocks ciphertext is XOR'd with the next block's plaintext. This yields a different encrypt for the next block even if the data is the same as the previous block. Plus, with the initialization vector, we can achieve entirely different encryptions for the same set of data. As can be seen in the CBC bitmap, the original picture cannot be seen or deciphered at all. Clearly a better encryption method when compared to ECB.

The same observation / conclusion applies to the penguin picture, although with the penguin picture we see some interesting effects due to the color of the background being something that has distinct values for RGB, as opposed to WHITE which is the same 255 value for R, G and B.

Task 5: Error Propagation – Corrupted Cipher Text

Encrypt, corrupt, decrypt and explain error propagation for each cipher mode ECB, CBC, CFB and OFB.

In the figure below, we can see the Plaintext.txt file that's being encrypted. This is the text file which I will encrypt with the following, ECB, CBC, CFB and OFB cipher modes. This is also the decrypted plaintext file used in Task 1!

The screenshot shows a Visual Studio Code window with the title "SEEDUbuntu Encryption Lab [Running] - Oracle VM VirtualBox". The menu bar includes File, Machine, View, Input, Devices, Help, and a status bar showing "7:52 PM". The main area displays two tabs: "encrypt.txt" and "plaintext.txt". The "encrypt.txt" tab contains the following text:

```

1 |the oscars turn on sunday which seems about right after this long strange
2 |awards trip the bagger feels like a nonagenarian too
3 |
4 |the awards race was bookended by the demise of harvey weinstein at its outset
5 |and the apparent implosion of his film company at the end and it was shaped by
6 |the emergence of metoo times up blackgown politics armcandy activism and
7 |a national conversation as brief and mad as a fever dream about whether there
8 |ought to be a president winfrey the season didnt just seem extra long it was
9 |extra long because the oscars were moved to the first weekend in march to
10 |avoid conflicting with the closing ceremony of the winter olympics thanks
11 |pyeongchang
12 |
13 |one big question surrounding this years academy awards is how or if the
14 |ceremony will address metoo especially after the golden globes which became
15 |a jubilant comingout party for times up the movement spearheaded by
16 |powerful hollywood women who helped raise millions of dollars to fight sexual
17 |harassment around the country
18 |
19 |signaling their support golden globes attendees swathed themselves in black
20 |spotted lapel pins and sounded off about sexist power imbalances from the red
21 |carpet and the stage on the air e was called out about pay inequity after
22 |its former anchor catt sadler quit once she learned that she was making far
23 |less than a male cohost and during the ceremony natalie portman took a blunt
24 |and satisfying dig at the allmale roster of nominated directors how could
25 |that be topped
26 |
27 |as it turns out at least in terms of the oscars it probably wont be
28 |
29 |women involved in times up said that although the globes signified the
30 |initiatives launch they never intended it to be just an awards season
31 |campaign or one that became associated only with redcarpet actions instead
32 |a spokeswoman said the group is working behind closed doors and has since
33 |amassed million for its legal defense fund which after the globes was
34 |flooded with thousands of donations of or less from people in some
35 |countries
36 |
37 |no call to wear black gowns went out in advance of the oscars though the
38 |movement will almost certainly be referenced before and during the ceremony
39 |especially since vocal metoo supporters like ashley judd laura dern and
40 |nicole kidman are scheduled presenters
41 |
42 |another feature of this season no one really knows who is going to win best
43 |picture arguably this happens a lot of the time inarguably the nailbiter
44 |narrative only serves the awards hype machine but often the people forecasting
45 |the race socalled oscarologists can make only educated quesses
46 |

```

The status bar at the bottom shows "Ln 1, Col 1" and "Spaces: 4" and "UTF-8". There are also icons for CRLF, Plain Text, and a smiley face.

In the figure below, we can see the encryption of `plaintext.txt` in ECB, CBC, CFB and OFB modes. We can also see the resultant binary files for each of the encryptions:

- `aes128ebc.bin`
- `aes128cbc.bin`
- `aes128cfb.bin`
- `aes128ofb.bin`

Once again, please note, `plaintext.txt` is the text file which is being encrypted for each of the cipher modes.

The screenshot shows a terminal window titled "Terminal" running on a SEEDUbuntu Encryption Lab [Running] - Oracle VM VirtualBox. The terminal output is as follows:

```

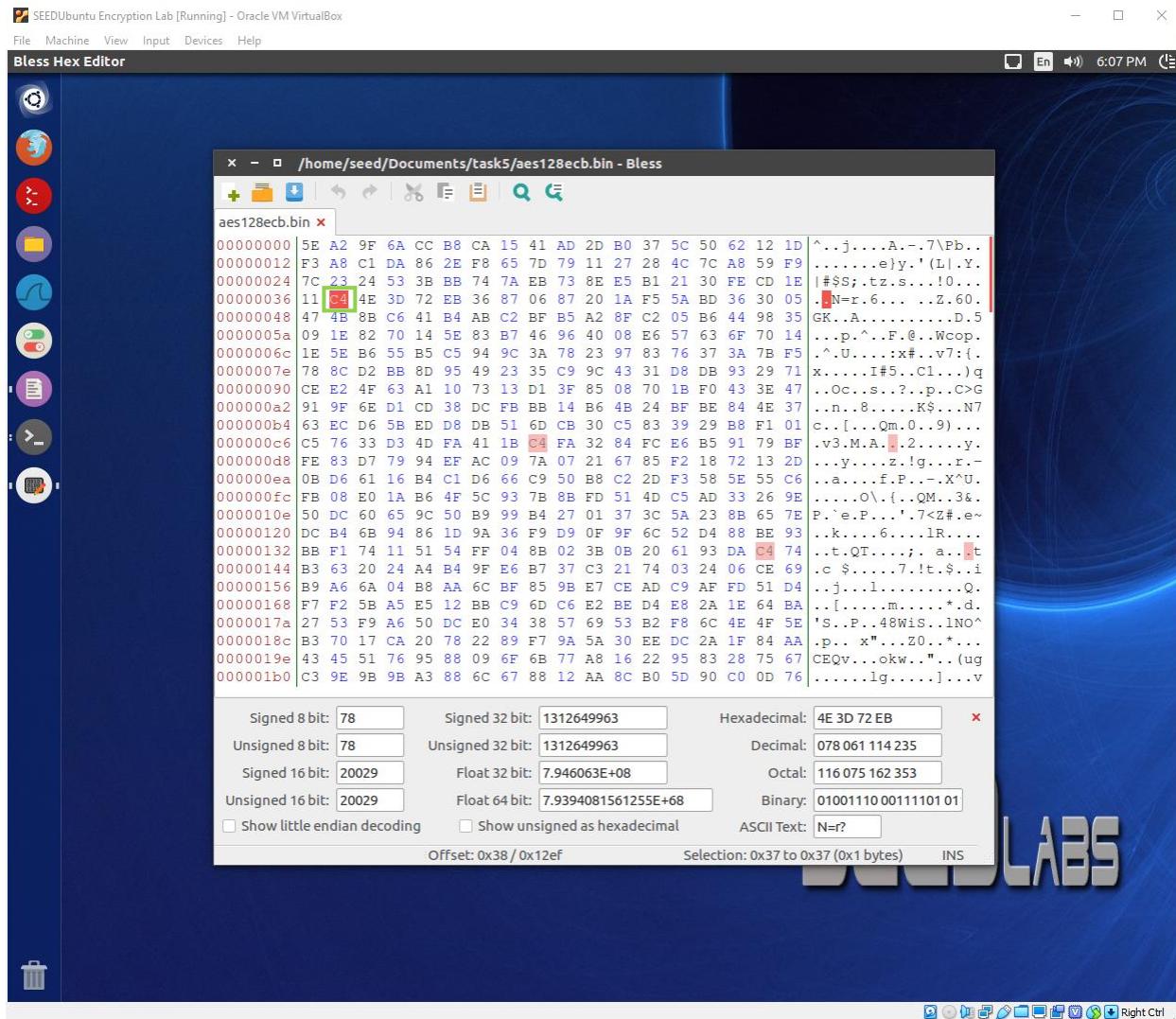
x - Terminal
Document does not have a root element.
Sharing violation on path /home/seed/.config/bless/preferences.xml
Sharing violation on path /home/seed/.config/bless/preferences.xml
Sharing violation on path /home/seed/.config/bless/preferences.xml
Document does not have a root element.
[02/23/19]seed@VM:~/.../task3$ cd ..
[02/23/19]seed@VM:~/Documents$ ls
aes128cbc.bmp aes128ecb.bmp ciphertext.txt ct.bak encrypt.txt task2 task3 words.txt
[02/23/19]seed@VM:~/Documents$ mkdir tas5
[02/23/19]seed@VM:~/Documents$ mv tas5 task5
[02/23/19]seed@VM:~/Documents$ cd task5
[02/23/19]seed@VM:~/.../task5$ ls
[02/23/19]seed@VM:~/.../task5$ l s-al
ls: cannot access 's-al': No such file or directory
[02/23/19]seed@VM:~/.../task5$ ls -al
total 8
drwxrwxr-x 2 seed seed 4096 Feb 23 16:23 .
drwxr-xr-x 5 seed seed 4096 Feb 23 16:23 ..
[02/23/19]seed@VM:~/.../task5$ ls
[02/23/19]seed@VM:~/.../task5$ cp ~/Documents/plaintext.txt ..
[02/23/19]seed@VM:~/.../task5$ ls -al
total 16
drwxrwxr-x 2 seed seed 4096 Feb 23 19:45 .
drwxr-xr-x 5 seed seed 4096 Feb 23 19:44 ..
-rwxrwx-- 1 seed seed 4846 Feb 23 19:45 plaintext.txt
[02/23/19]seed@VM:~/.../task5$ ls
plaintext.txt
[02/23/19]seed@VM:~/.../task5$ openssl enc -aes-128-ecb -e -in plain.txt -out aes128ecb.bin -K 00112233445566778889aabccdd
eeff
plain.txt: No such file or directory
3070293696:error:02001002:system library:fopen:No such file or directory:bss_file.c:398:fopen('plain.txt','r')
3070293696:error:20074002:BIO routines:FILE_CTRL:system lib:bss_file.c:400:
[02/23/19]seed@VM:~/.../task5$ openssl enc -aes-128-ecb -e -in plaintext.txt -out aes128ecb.bin -K 00112233445566778889aabb
ccddeeff
[02/23/19]seed@VM:~/.../task5$ openssl enc -aes-128-cbc -e -in plaintext.txt -out aes128cbc.bin -K 00112233445566778889aabb
ccddeeff -iv 0102030405060708
[02/23/19]seed@VM:~/.../task5$ openssl enc -aes-128-cbc -e -in plaintext.txt -out aes128cbc.bin -K 00112233445566778889aabb
ccddeeff -iv 0102030405060708
[02/23/19]seed@VM:~/.../task5$ openssl enc -aes-128-cfb -e -in plaintext.txt -out aes128cfb.bin -K 00112233445566778889aabb
ccddeeff -iv 0102030405060708
[02/23/19]seed@VM:~/.../task5$ openssl enc -aes-128-ofb -e -in plaintext.txt -out aes128ofb.bin -K 00112233445566778889aabb
ccddeeff -iv 0102030405060708
[02/23/19]seed@VM:~/.../task5$ ls -al
total 48
drwxrwxr-x 2 seed seed 4096 Feb 23 19:50 .
drwxr-xr-x 5 seed seed 4096 Feb 23 19:44 ..
-rw-rw-r-- 1 seed seed 4848 Feb 23 19:49 aes128cbc.bin
-rw-rw-r-- 1 seed seed 4846 Feb 23 19:49 aes128cfb.bin
-rw-rw-r-- 1 seed seed 4848 Feb 23 19:47 aes128ecb.bin
-rw-rw-r-- 1 seed seed 4846 Feb 23 19:50 aes128ofb.bin
-rwxrwx--- 1 seed seed 4846 Feb 23 19:45 plaintext.txt
[02/23/19]seed@VM:~/.../task5$
```

In the figure below, we can see the decryption of each of the encrypted files. The resultant decrypted files are:

- aes128ebc.txt
- aes128cbc.txt
- aes128cfb.txt
- aes128ofb.txt

After the decryption, we corrupted byte 55 of the encrypted binaries. This is byte 0x37. We used the “bless” hex editor to accomplish this. We can see the cursor on byte 0x37. We can then change the value by typing it in.

I just wanted to show the method used for editing the binary. The next figure will show the resultant binary differences within each file to show the diffs; i.e. the value for the corrupted byte 55 (0x37).



In the figure below, you can see the diffs for each encrypted binary file for aes128ecb.bin, aes128cbc.bin, aes128cfb.bin and aes128ofb.bin. Please note, only one byte was modified (byte 0x37; byte 55) and that only one bit was changed.

For the following figures and to show the binary differences within the file, I'm using "vbindiff" which is like "diff", but will visually show you binary differences between two files.

The figure shows four terminal windows side-by-side, each displaying the output of a command-line tool comparing two files. The top window shows the difference between `aes128ecb.txt` and `plaintext.txt`. The bottom window shows the difference between `aes128fb.txt` and `plaintext.txt`. The leftmost window shows the difference between `aes128cbc.txt` and `plaintext.txt`. The rightmost window shows the difference between `aes128cfb.txt` and `plaintext.txt`. Each terminal window has a title bar, a menu bar, and a status bar at the bottom. The status bar includes icons for file operations and the text "Right Ctrl". The terminal windows are running on a desktop environment with a blue background.

```

SEDEUbuntu Encryption Lab [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ubuntu Desktop
x - Terminal
aes128ecb.bin
0000 0000: 5E A2 9F 6A CC B8 CA 15 41 AD 2D B0 37 5C 50 62 ^...j.... A.-.7\Pb
0000 0010: 12 1D F3 A8 C1 D4 86 2E F8 65 7D 79 11 27 28 4C .N.....e)y.'(L
0000 0020: 7C A8 59 F7 C3 23 53 3B B8 74 EA 73 8E E5 |.Y.|#SS|:tz.s..
0000 0030: B1 21 30 FE CD 1E 11 CA 4E 3D 72 EB 36 87 86 87 .10.....N=r.s..
0000 0040: 28 1A F5 5A BD 36 05 47 4B 8B C6 41 B4 AB C2 .Z.68. GK..A..
0000 0050: BF B5 A2 8F C2 85 B6 44 98 35 09 1E 82 70 14 5E .....D 5...p.^
0000 0060: B3 B7 46 90 48 0E E6 57 63 6F 70 14 1E 5E B6 55 .F@.W cop.^U
0000 0070: B5 C5 94 9C 3A 78 23 97 83 76 37 3A 7B F5 78 8C ....:x#. .v?:(x.

./task5.bak/aes128ecb.bin
0000 0000: 5E A2 9F 6A CC B8 CA 15 41 AD 2D B0 37 5C 50 62 ^...j.... A.-.7\Pb
0000 0010: 12 1D F3 A8 C1 D4 86 2E F8 65 7D 79 11 27 28 4C .N.....e)y.'(L
0000 0020: 7C A8 59 F7 C3 23 53 3B B8 74 EA 73 8E E5 |.Y.|#SS|:tz.s..
0000 0030: B1 21 30 FE CD 1E 11 CA 4E 3D 72 EB 36 87 86 87 .10.....N=r.s..
0000 0040: 28 1A F5 5A BD 36 05 47 4B 8B C6 41 B4 AB C2 .Z.68. GK..A..
0000 0050: BF B5 A2 8F C2 85 B6 44 98 35 09 1E 82 70 14 5E .....D 5...p.^
0000 0060: B3 B7 46 90 48 0E E6 57 63 6F 70 14 1E 5E B6 55 .F@.W cop.^U
0000 0070: B5 C5 94 9C 3A 78 23 97 83 76 37 3A 7B F5 78 8C ....:x#. .v?:(x.

Arrow keys move F find RET next difference ESC quit T move top
C ASCII/EBCDIC E edit file G goto position Q quit B move bottom

x - Terminal
aes128cbc.bin
0000 0000: 3F 8F 65 D1 09 AE 99 71 42 A2 C6 78 7B E8 32 9C ?.e....q B..{[.2.
0000 0010: 2E E5 4E 91 EB D6 07 FD 38 C8 48 FD A3 65 D9 .N...s. 8.0..e
0000 0020: FE 63 52 47 97 15 39 02 53 8A BE 90 56 22 36 6E .CRG..9. S..V'6
0000 0030: AA F1 97 B6 CA B3 3E 04 00 22 A4 E1 CA C5 EA 08 .....> .
0000 0040: 4B BB 57 68 8C 7C C1 5E 30 84 69 72 E3 1D 66 K.W.|.^ .i.r..f
0000 0050: A2 94 70 47 01 1F B2 2C D9 B3 18 44 E3 1F 3F 2D .pG... .D.?
0000 0060: B3 32 7F 72 45 F8 A6 A8 18 A5 8F 51 F6 3E 3E 3B .2.F... .Q.>>8
0000 0070: 35 18 86 A4 2F FD A8 D1 D7 5B 99 A4 56 04 F1 26 5.../.H..[.V..&
0000 0080: D5 3C 89 95 18 47 DC C4 23 8F 15 33 CD 98 9C 16 ..<...G. #.3. ....
./task5.bak/aes128cbc.bin
0000 0000: 3F 0F 65 D1 09 AE 99 71 42 A2 C6 78 7B E8 32 9C ?.e....q B..{[.2.
0000 0010: 2E E5 4E 91 EB D6 07 FD 38 C8 48 FD A3 65 D9 .N...s. 8.0..e
0000 0020: FE 63 52 47 97 15 39 02 53 8A BE 90 56 22 36 6E .CRG..9. S..V'6
0000 0030: AA F1 97 B6 CA B3 3E 04 00 22 A4 E1 CA C5 EA 08 .....> .
0000 0040: 4B BB 57 68 8C 7C C1 5E 30 84 69 72 E3 1D 66 K.W.|.^ .i.r..f
0000 0050: A2 94 70 47 01 1F B2 2C D9 B3 18 44 E3 1F 3F 2D .pG... .D.?
0000 0060: B3 32 7F 72 45 F8 A6 A8 18 A5 8F 51 F6 3E 3E 3B .2.F... .Q.>>8
0000 0070: 35 18 86 A4 2F FD A8 D1 D7 5B 99 A4 56 04 F1 26 5.../.H..[.V..&
0000 0080: D5 3C 89 95 18 47 DC C4 23 8F 15 33 CD 98 9C 16 ..<...G. #.3. ....
./task5.bak/aes128fb.bin
0000 0000: F3 EE EA 05 AE 4C D9 B0 DD ED 9F 69 00 62 32 4D ....L. ...l.b2M
0000 0010: EF 36 ED 88 A6 6E AF 5E 90 FC BD D7 23 32 B6 4A .6...n.^ ...#2.J
0000 0020: 0E C6 CD C1 12 F8 2C D1 04 83 0C 0F F7 74 29 D4 .....> @.^.J.S.
0000 0030: DD F6 81 04 53 83 E2 3D 40 81 8A 27 4A 1C 35 C4 .S..> @.^.J.S.
0000 0040: 36 DD A9 B9 B7 79 50 D9 04 00 04 FE 1F ED 86 C7 6...y.P. .....
0000 0050: 33 74 BD 8F 74 80 DB 8D 82 4F 54 F2 99 6D 3A A7 3t..t... .OT..m.
0000 0060: F3 67 BE 03 0A 03 B2 51 06 EE CE 3E 76 7F 11 59 .o...Q ...>v.Y
0000 0070: 6E 00 30 FE 74 91 A6 FB CB 57 57 38 85 06 EA 46 n.0.t... .WH8...F
0000 0080: D4 A7 45 41 BA 18 32 13 23 8F E9 80 05 89 C9 0C ..EA..2. #. .....
./task5.bak/aes128fb.bin
0000 0000: F3 EE EA 05 AE 4C D9 B0 DD ED 9F 69 00 62 32 4D ....L. ...l.b2M
0000 0010: EF 36 ED 88 A6 6E AF 5E 90 FC BD D7 23 32 B6 4A .6...n.^ ...#2.J
0000 0020: 0E C6 CD C1 12 F8 2C D1 04 83 0C 0F F7 74 29 D4 .....> @.^.J.S.
0000 0030: DD F6 81 04 53 83 E2 3D 40 81 8A 27 4A 1C 35 C4 .S..> @.^.J.S.
0000 0040: 36 DD A9 B9 B7 79 50 D9 04 00 04 FE 1F ED 86 C7 6...y.P. .....
0000 0050: 33 74 BD 8F 74 80 DB 8D 82 4F 54 F2 99 6D 3A A7 3t..t... .OT..m.
0000 0060: F3 67 BE 03 0A 03 B2 51 06 EE CE 3E 76 7F 11 59 .o...Q ...>v.Y
0000 0070: 6E 00 30 FE 74 91 A6 FB CB 57 57 38 85 06 EA 46 n.0.t... .WH8...F
0000 0080: D4 A7 45 41 BA 18 32 13 23 8F E9 80 05 89 C9 0C ..EA..2. #. .....
Arrow keys move F find RET next difference ESC quit T move top
C ASCII/EBCDIC E edit file G goto position Q quit B move bottom

```

In the figure below, we can see the binary difference between `aes128ecb.txt` (top) and `plaintext.txt` (bottom).

```

SEEDUbuntu Encryption Lab [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
x - Terminal
aes128cbc.txt
0000 0000: 74 68 65 20 6F 73 63 61 72 73 20 74 75 72 6E 20 the oscars turn
0000 0010: 20 6F 6E 20 73 75 6E 64 61 79 20 77 68 69 63 68 on sunday which
0000 0020: 20 73 65 65 6D 73 20 61 62 6F 75 74 20 72 69 67 seems about rig
0000 0030: E9 11 DB C1 C7 0B F2 BE 05 E7 39 91 63 06 E6 6F ..... .9.c.o
0000 0040: 6E 67 20 73 74 72 61 6E 67 65 0D 0A 61 77 61 72 ng strange..awar
0000 0050: 64 73 20 74 72 69 70 20 74 68 65 20 62 61 67 67 ds trip the bagg
0000 0060: 65 72 20 66 65 65 6C 73 20 6C 69 68 65 20 61 20 er feels like a
0000 0070: 6E 6F 6E 61 67 65 6E 61 72 69 61 6E 20 74 6F 6F nonagenarian too
0000 0080: 6D 0A 00 0A 74 68 65 20 61 77 61 72 64 73 20 72 ....the awards r
0000 0090: 61 63 65 20 77 61 73 20 62 6F 68 65 6E 64 65 ace was bookende
0000 00A0: 64 20 62 79 20 74 68 65 20 64 65 60 69 73 65 20 d by the demise
0000 00B0: 6F 66 20 68 61 72 76 65 79 20 77 65 69 6E 73 74 of harvey weinst
0000 00C0: 65 69 66 20 61 74 20 69 74 73 65 ein at its outse
0000 00D0: 74 00 0A 61 6E 64 20 74 68 65 20 68 65 20 61 70 78 61 72 t..and the appar
0000 00E0: 65 6E 74 20 69 66 6D 70 6C 6F 73 69 6F 6E 20 6F 66 ent impl ostion of
0000 00F0: 20 68 69 73 20 66 69 6C 6D 20 63 6F 6D 70 61 6E his fil m compan
0000 0100: 79 20 61 74 20 74 68 65 20 65 6E 64 20 61 6E 64 y at the end and
0000 0110: 20 69 74 20 77 61 73 20 73 68 61 70 65 64 20 62 it was shaped b
0000 0120: 79 0D 0A 74 68 65 20 65 65 72 67 65 6E 63 65 y..the emergence
0000 0130: 20 6F 66 20 6D 61 65 74 6F 6F 20 74 69 60 65 73 20 of meto o times
0000 0140: 75 70 20 62 66 61 63 6B 67 6F 77 6E 20 70 6F 6C up black gown pol
0000 0150: 69 74 69 63 73 20 61 72 6D 63 61 6E 64 79 20 61 itics ar mcandy a
0000 0160: 63 74 69 76 69 73 6D 20 61 6E 64 0D 0A 61 20 6E ctivism and..a n
plaintext.txt
0000 0000: 74 68 65 20 6F 73 63 61 72 73 20 74 75 72 6E 20 the oscars turn
0000 0010: 20 6F 6E 20 73 75 6E 64 61 79 20 77 68 69 63 68 on sunday which
0000 0020: 20 73 65 65 6D 73 20 61 62 6F 75 74 20 72 69 67 seems about rig
0000 0030: E8 74 20 61 66 74 65 72 20 74 68 69 73 20 6C 6F ht after this lo
0000 0040: 6E 67 20 73 74 72 61 6E 67 65 0D 0A 61 77 61 72 ng strange..awar
0000 0050: 64 73 20 74 72 69 70 20 74 68 65 20 62 61 67 67 ds trip the bagg
0000 0060: 65 72 20 66 65 65 6C 73 20 6C 69 68 65 20 61 20 er feels like a
0000 0070: 6E 6F 6E 61 67 65 6E 61 72 69 61 6E 20 74 6F 6F nonagenarian too
0000 0080: 6D 0A 00 0A 74 68 65 20 61 77 61 72 64 73 20 72 ....the awards r
0000 0090: 61 63 65 20 77 61 73 20 62 6F 68 65 6E 64 65 ace was bookende
0000 00A0: 64 20 62 79 20 74 68 65 20 64 65 60 69 73 65 20 d by the demise
0000 00B0: 6F 66 20 68 61 72 76 65 79 20 77 65 69 6E 73 74 of harvey weinst
0000 00C0: 65 69 66 20 61 74 20 69 74 68 65 20 65 6E 64 20 61 6E 64 ein at its outse
0000 00D0: 74 0D 0A 61 6E 64 20 74 68 65 20 68 65 20 61 70 78 61 72 t..and the appar
0000 00E0: 65 6E 74 20 69 66 6D 70 6C 6F 73 69 6F 6E 20 6F 66 ent impl ostion of
0000 00F0: 20 68 69 73 20 66 69 6C 6D 20 63 6F 6D 70 61 6E his fil m compan
0000 0100: 79 20 61 74 20 74 68 65 20 65 6E 64 20 61 6E 64 y at the end and
0000 0110: 20 69 74 20 77 61 73 20 73 68 61 70 65 64 20 62 it was shaped b
0000 0120: 79 0D 0A 74 68 65 20 65 65 72 67 65 6E 63 65 y..the e mergence
0000 0130: 20 6F 66 20 6D 65 74 6F 6F 20 74 69 60 65 73 20 of meto o times
0000 0140: 75 70 20 62 66 61 63 6B 67 6F 77 6E 20 70 6F 6C up black gown pol
0000 0150: 69 74 69 63 73 20 61 72 6D 63 61 6E 64 79 20 61 itics ar mcandy a
0000 0160: 63 74 69 76 69 73 6D 20 61 6E 64 0D 0A 61 20 6E ctivism and..a n
Arrow keys move F find      RET next difference  ESC quit T move top
C ASCII/EBCDIC E edit file G goto position Q quit B move bottom

```

In the figure below, we can see the binary difference between aes128cbc.txt (top) and plaintext.txt (bottom).

```

SEEDUbuntu Encryption Lab [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
x - Terminal
aes128cbc.txt
0000 0000: 74 68 65 20 6F 73 63 61 72 73 20 74 75 72 6E 20 the oscars turn
0000 0010: 20 6F 6E 20 73 75 6E 64 61 79 20 77 68 69 63 68 on sunday which
0000 0020: 20 73 65 65 6D 73 20 61 62 6F 75 74 20 72 69 67 seems about rig
0000 0030: 3C 6F 56 38 1A 37 80 E9 0F 78 22 85 11 07 94 83 <vB.7... .("...
0000 0040: 6E 67 20 73 74 72 61 6F 67 65 00 0A 61 77 61 72 ng straoge..awar
0000 0050: 64 73 20 74 72 69 70 20 74 68 65 20 62 61 67 67 ds trip the bagg
0000 0060: 65 72 20 66 65 65 6C 73 20 6C 69 68 65 20 61 20 er feels like a
0000 0070: 6E 6F 6E 61 67 65 6E 61 72 69 61 6E 20 74 6F 6F nonagenarian too
0000 0080: 60 62 62 79 20 74 68 65 20 61 77 61 72 64 73 20 72 ....the awards r
0000 0090: 61 63 65 20 77 61 73 20 62 6F 68 65 6E 64 65 ace was bookende
0000 00A0: 64 20 62 79 20 74 68 65 20 64 65 6D 69 73 65 20 d by the demise
0000 00B0: 6F 66 20 68 61 72 76 65 79 20 77 65 69 6E 73 74 of harvey weinst
0000 00C0: 65 69 6E 20 61 74 20 69 74 65 20 68 65 20 61 72 ein at its outse
0000 00D0: 74 00 0A 6E 64 20 74 65 72 68 65 20 65 20 61 72 t..and he appar
0000 00E0: 65 6E 74 20 69 60 66 70 6C 6F 73 69 6F 6E 20 6F 66 ent impl ostion of
0000 00F0: 20 68 69 73 20 66 69 6C 6D 20 63 6F 60 70 61 6E his film compan
0000 0100: 79 20 61 74 20 74 68 65 20 65 6E 64 20 61 6E 64 y at the end and
0000 0110: 20 69 74 20 77 61 73 20 73 68 61 70 65 64 20 62 it was shaped b
0000 0120: 79 00 0A 74 68 65 20 65 6D 65 73 20 65 62 67 65 6E 63 65 y..the emergence
0000 0130: 20 6F 66 20 6D 65 74 6F 6F 20 74 69 60 65 73 20 of metoo times
0000 0140: 75 70 20 62 6C 61 63 68 67 6F 77 6E 20 78 6F 6C up black gown pol
0000 0150: 69 74 69 63 73 20 61 72 6D 63 61 6E 64 79 20 61 itics ar mcdandy a
0000 0160: 63 74 69 76 69 73 6D 20 61 6E 64 00 0A 61 20 6E ctivism and..a n
plaintext.txt
0000 0000: 74 68 65 20 6F 73 63 61 72 73 20 74 75 72 6E 20 the oscars turn
0000 0010: 20 6F 6E 20 73 75 6E 64 61 79 20 77 68 69 63 68 on sunday which
0000 0020: 20 73 65 65 6D 73 20 61 62 6F 75 74 20 72 69 67 seems about rig
0000 0030: 68 74 20 61 66 74 65 72 20 74 68 69 73 20 6C 6F ht after this lo
0000 0040: 6E 67 20 73 74 72 61 6E 67 65 00 0A 61 77 61 72 ng straoge..awar
0000 0050: 64 73 20 74 72 69 70 20 74 68 65 20 62 61 67 67 ds trip the bagg
0000 0060: 65 72 20 66 65 65 6C 73 20 6C 69 68 65 20 61 20 er feels like a
0000 0070: 6E 6F 6E 61 67 65 6E 61 72 69 61 6E 20 74 6F 6F nonagenarian too
0000 0080: 60 6A 00 0A 74 66 65 65 20 61 77 61 72 64 73 20 72 ....the awards r
0000 0090: 61 63 65 20 77 61 73 20 62 6F 68 65 6E 64 65 ace was bookende
0000 00A0: 64 20 62 79 20 74 68 65 20 64 65 6D 69 73 65 20 d by the demise
0000 00B0: 6F 66 20 68 61 72 76 65 79 20 77 65 69 6E 73 74 of harvey weinst
0000 00C0: 65 69 6E 20 61 74 20 69 69 6F 74 73 20 6F 75 74 73 65 ein at its outse
0000 00D0: 74 00 0A 6E 64 20 74 65 72 68 65 20 65 20 61 72 t..and he appar
0000 00E0: 65 6E 74 20 69 60 70 6C 6F 73 69 6F 6E 20 6F 66 ent impl ostion of
0000 00F0: 20 68 69 73 20 66 69 6C 6D 20 63 6F 60 70 61 6E his film compan
0000 0100: 79 20 61 74 20 74 68 65 20 65 6E 64 20 61 6E 64 y at the end and
0000 0110: 20 69 74 20 77 61 73 20 73 68 61 70 65 64 20 62 it was shaped b
0000 0120: 79 00 0A 74 68 65 20 65 6D 65 73 20 65 62 67 65 6E 63 65 y..the e mergece
0000 0130: 20 6F 66 20 6D 65 74 6F 6F 20 74 69 60 65 73 20 of metoo times
0000 0140: 75 70 20 62 6C 61 63 68 67 6F 77 6E 20 78 6F 6C up black gown pol
0000 0150: 69 74 69 63 73 20 61 72 6D 63 61 6E 64 79 20 61 itics ar mcdandy a
0000 0160: 63 74 69 76 69 73 6D 20 61 6E 64 00 0A 61 20 6E ctivism and..a n

Arrow keys move F find RET next difference ESC quit T move top
c ASCII/EBCDIC E edit file G goto position Q quit B move bottom

```

In the figure below, we can see the binary difference between aes128cfb.txt (top) and plaintext.txt (bottom).

```

SEEDUbuntu Encryption Lab [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
x - Terminal
aes128cfb.txt
0000 0000: 74 68 65 20 6F 73 63 61 72 73 20 74 75 72 6E 20 the oscars turn
0000 0010: 20 6F 6E 20 73 75 6E 64 61 79 20 77 68 69 63 68 on sunday which
0000 0020: 20 73 65 65 6D 73 20 61 62 6F 75 74 20 72 69 67 seems about rig
0000 0030: 68 74 20 61 66 74 65 62 20 74 68 69 73 20 6C 6F ht after this lo
0000 0040: 03 EE 20 78 9B 91 EC CA 15 1A 1A 0B ED 27 64 7E .. x;.... .d-
0000 0050: 64 73 20 74 72 69 70 20 74 68 65 20 62 61 67 67 ds trip the bagg
0000 0060: 65 72 20 66 65 65 6C 73 20 6C 69 68 65 20 61 20 er feels like a
0000 0070: 6E 6F 6E 61 67 65 6E 61 72 69 61 6E 20 74 6F 6F nonagenarian too
0000 0080: 00 0A 00 0A 74 65 65 20 61 77 61 72 64 73 20 72 ....the awards r
0000 0090: 61 63 65 20 77 61 73 20 62 6F 68 65 6E 64 65 ace was bookende
0000 00A0: 64 20 62 79 20 74 68 65 20 64 65 60 69 73 65 20 d by the demise
0000 00B0: 66 20 68 61 72 76 65 79 20 77 65 69 6E 73 74 of harvey weinst
0000 00C0: 65 69 6E 20 61 74 20 69 74 73 20 6F 75 74 73 65 ein at its outside
0000 00D0: 74 00 0A 61 6E 64 20 74 68 65 20 68 65 20 61 70 70 61 72 t..and t he appar
0000 00E0: 65 6E 74 20 69 60 70 6C 6F 73 69 6F 6E 20 6F 66 ent impl osion of
0000 00F0: 20 68 69 73 20 66 69 6C 60 20 63 6F 60 70 61 6E his fil m compan
0000 0100: 79 20 61 74 20 74 68 65 20 65 6E 64 20 61 6E 64 y at the end and
0000 0110: 20 69 74 20 77 61 73 20 73 68 61 70 65 64 20 62 it was shaped b
0000 0120: 79 00 0A 74 68 65 20 65 60 65 72 67 65 6E 63 65 y..the e mergence
0000 0130: 20 6F 66 20 60 65 74 6F 6F 20 74 69 60 65 73 20 of metoo times
0000 0140: 75 70 20 62 6C 61 63 68 67 6F 77 6E 20 70 6F 6C up black gown pol
0000 0150: 69 74 69 63 73 20 61 72 60 63 61 6E 64 79 20 61 itics ar mcdandy a
0000 0160: 63 74 69 76 69 73 6D 20 61 6E 64 0D 0A 61 20 6E ctivism and..a n
plainText.txt
0000 0000: 74 68 65 20 6F 73 63 61 72 73 20 74 75 72 6E 20 the oscars turn
0000 0010: 20 6F 6E 20 73 75 6E 64 61 79 20 77 68 69 63 68 on sunday which
0000 0020: 20 73 65 65 6D 73 20 61 62 6F 75 74 20 72 69 67 seems about rig
0000 0030: 68 74 20 61 66 74 65 72 20 74 68 69 73 20 6C 6F ht after this lo
0000 0040: 0E 67 20 73 74 72 61 6E 67 65 00 0A 61 77 61 72 ng stran ge..awar
0000 0050: 64 73 20 74 72 69 70 20 74 68 65 20 62 61 67 67 ds trip the bagg
0000 0060: 65 72 20 66 65 65 6C 73 20 6C 69 68 65 20 61 20 er feels like a
0000 0070: 6E 6F 6E 61 67 65 6E 61 72 69 61 6E 20 74 6F 6F nonagenarian too
0000 0080: 00 0A 00 0A 74 68 65 20 61 77 61 72 64 73 20 72 ....the awards r
0000 0090: 61 63 65 20 77 61 73 20 62 6F 68 65 6E 64 65 ace was bookende
0000 00A0: 64 20 62 79 20 74 68 65 20 64 65 60 69 73 65 20 d by the demise
0000 00B0: 6F 66 20 68 61 72 76 65 79 20 77 65 69 6E 73 74 of harvey weinst
0000 00C0: 65 69 6E 20 61 74 20 69 65 74 73 20 6F 75 74 73 65 ein at its outside
0000 00D0: 74 00 0A 61 6E 64 20 74 68 65 20 68 65 20 61 70 70 61 72 t..and t he appar
0000 00E0: 65 6E 74 20 69 60 70 6C 6F 73 69 6F 6E 20 6F 66 ent impl osion of
0000 00F0: 20 68 69 73 20 66 69 6C 60 20 63 6F 60 70 61 6E his fil m compan
0000 0100: 79 20 61 74 20 74 68 65 20 65 6E 64 20 61 6E 64 y at the end and
0000 0110: 20 69 74 20 77 61 73 20 73 68 61 70 65 64 20 62 it was shaped b
0000 0120: 79 00 0A 74 68 65 20 65 60 65 72 67 65 6E 63 65 y..the e mergence
0000 0130: 20 6F 66 20 60 65 74 6F 6F 20 74 69 60 65 73 20 of metoo times
0000 0140: 75 70 20 62 6C 61 63 68 67 6F 77 6E 20 70 6F 6C up black gown pol
0000 0150: 69 74 69 63 73 20 61 72 60 63 61 6E 64 79 20 61 itics ar mcdandy a
0000 0160: 63 74 69 76 69 73 6D 20 61 6E 64 0D 0A 61 20 6E ctivism and..a n

```

Arrow keys move F find RET next difference ESC quit T move top
C ASCII/EBCDIC E edit file G goto position Q quit B move bottom

In the figure below, we can see the binary difference between aes128cfb.txt (top) and plaintext.txt (bottom).

```

SEEDUbuntu Encryption Lab [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ubuntu Desktop
x - Terminal
aes128ofb.txt
0000 0000: 74 68 65 20 6F 73 63 61 72 73 20 74 75 72 6E 20 the oscars turn
0000 0010: 20 6F 6E 20 73 75 6E 64 61 79 20 77 68 69 63 68 on sunday which
0000 0020: 20 73 65 65 6D 73 20 61 62 6F 75 74 20 72 69 67 seems about rig
0000 0030: 68 74 20 61 66 74 65 73 20 74 68 69 73 20 6C 6F after this lo
0000 0040: 6E 67 20 73 74 72 61 6E 67 65 0D 0A 61 77 61 72 ng strange..awar
0000 0050: 64 73 20 74 72 69 70 20 74 68 65 20 62 61 67 67 ds trip the bagg
0000 0060: 65 72 20 66 65 65 6C 73 20 6C 68 68 65 20 61 20 er feels like a
0000 0070: 6E 6F 6E 61 67 65 6E 61 72 69 61 6E 20 74 6F 6F nonagenarian too
0000 0080: 6D 0A 00 0A 74 68 65 20 61 77 61 72 64 73 20 72 ...the awards r
0000 0090: 61 63 65 20 77 61 73 20 62 6F 68 65 6E 64 65 ace was bookende
0000 00A0: 64 20 62 79 20 74 68 65 20 64 65 60 69 73 65 20 d by the demise
0000 00B0: 6F 66 20 68 61 72 76 65 79 20 77 65 69 6E 73 74 of harvey weinst
0000 00C0: 65 69 6E 20 61 74 20 69 74 65 73 20 73 20 6F 75 74 73 65 ein at its outse
0000 00D0: 74 00 0A 61 6E 64 20 74 68 65 74 65 20 61 70 78 61 72 ..and they appear
0000 00E0: 65 6E 74 20 69 69 6D 70 6C 6F 73 69 6F 6E 20 6F 66 ent impl ostion of
0000 00F0: 20 68 69 73 20 66 69 6C 6D 20 63 6F 6D 70 61 6E his film compan
0000 0100: 79 20 61 74 20 74 68 65 20 65 6E 64 20 61 6E 64 y at the end and
0000 0110: 20 69 74 20 77 61 73 20 73 68 61 70 65 64 20 62 it was shaped b
0000 0120: 79 0D 0A 74 68 65 20 65 65 72 67 65 6E 63 65 y..the emergence
0000 0130: 20 6F 66 20 62 61 65 74 6F 6F 20 74 69 60 65 73 20 of metoo times
0000 0140: 75 70 20 62 61 63 68 67 6F 77 6E 20 70 70 6F 6C up black gown pol
0000 0150: 69 74 69 63 73 20 61 72 6D 63 61 6E 64 79 20 61 itics ar mcandy a
0000 0160: 63 74 69 76 69 73 6D 20 61 6E 64 0D 0A 61 20 6E ctivism and..a n
plaintext.txt
0000 0000: 74 68 65 20 6F 73 63 61 72 73 20 74 75 72 6E 20 the oscars turn
0000 0010: 20 6F 6E 20 73 75 6E 64 61 79 20 77 68 69 63 68 on sunday which
0000 0020: 20 73 65 65 6D 73 20 61 62 6F 75 74 20 72 69 67 seems about rig
0000 0030: 68 74 20 61 66 74 65 73 20 74 68 69 73 20 6C 6F after this lo
0000 0040: 6E 67 20 73 74 72 61 6E 67 65 0D 0A 61 77 61 72 ng strange..awar
0000 0050: 64 73 20 74 72 69 70 20 74 68 65 20 62 61 67 67 ds trip the bagg
0000 0060: 65 72 20 66 65 65 6C 73 20 6C 69 68 65 20 61 20 er feels like a
0000 0070: 6E 6F 6E 61 67 65 6E 61 72 69 61 6E 20 74 6F 6F nonagenarian too
0000 0080: 6D 0A 00 0A 74 68 65 20 61 77 61 72 64 73 20 72 ...the awards r
0000 0090: 61 63 65 20 77 61 73 20 62 6F 68 65 6E 64 65 ace was bookende
0000 00A0: 64 20 62 79 20 74 68 65 20 64 65 60 69 73 65 20 d by the demise
0000 00B0: 6F 66 20 68 61 72 76 65 79 20 77 65 69 6E 73 74 of harvey weinst
0000 00C0: 65 69 6E 20 61 74 20 69 65 69 73 20 73 20 6F 75 74 73 65 ein at its outse
0000 00D0: 74 00 0A 61 6E 64 20 74 68 65 74 65 20 61 70 78 61 72 ..and they appear
0000 00E0: 65 6E 74 20 69 69 6D 70 6C 6F 73 69 6F 6E 20 6F 66 ent impl ostion of
0000 00F0: 20 68 69 73 20 66 69 6C 6D 20 63 6F 6D 70 61 6E his film compan
0000 0100: 79 20 61 74 20 74 68 65 20 65 6E 64 20 61 6E 64 y at the end and
0000 0110: 20 69 74 20 77 61 73 20 73 68 61 70 65 64 20 62 it was shaped b
0000 0120: 79 0D 0A 74 68 65 20 65 65 72 67 65 6E 63 65 y..the emergence
0000 0130: 20 6F 66 20 62 61 65 74 6F 6F 20 74 69 60 65 73 20 of metoo times
0000 0140: 75 70 20 62 61 63 68 67 6F 77 6E 20 70 70 6F 6C up black gown pol
0000 0150: 69 74 69 63 73 20 61 72 6D 63 61 6E 64 79 20 61 itics ar mcandy a
0000 0160: 63 74 69 76 69 73 6D 20 61 6E 64 0D 0A 61 20 6E ctivism and..a n
Arrow keys move F find      RET next difference ESC quit T move top
C ASCII/EBCDIC E edit file G goto position Q quit B move bottom

```

Observations / Explanations

Please answer the following question: How much information can you recover by decrypting the corrupted file, if the encryption mode is ECB, CBC, CFB, or OFB, respectively?

Please recall, we corrupted the 55'th byte of the encrypted binaries for each of the cipher modes. This is byte 0x37 in hexadecimal. We then decrypted each of the binaries using their respective cipher modes. Finally, we did a vbindiff of each decrypted file with the original plaintext.txt file to see the binary differences.

Regarding data recovery, the table below shows which data **are corrupted** per the corruption of the 55'th byte **after decryption**. The rest of the data decrypted ok.

Added block numbers per Redo.

Cipher Mode	Data Not Recovered; Corrupted bytes and blocks	Why?

ECB	0x30 – 0x3E in block 4	ECB is the simplest block cipher mode in that there is no dependency from one block to the next. Byte 55 was corrupt and the decryption affected that one block only. While we only discovered bytes up to 0x3E that were corrupt, we may have lucked-out here since the block affected is 0x30-0x3F so the entire block should've been corrupt including the last byte. It could be that the last byte is padding which would then make sense.
CBC	0x30 – 0x3F in block 4 0x47 in block 5	In CBC, the entire block of the corrupted byte will be corrupt since the ciphertext block is passed through the block cipher decryption. This will result in a corrupted block Byte 0x47 is the byte in the next block (0x40-0x4F) that is corrupt. If we further examine, the corrupt byte's value is 0x6F versus 0x6E which is one bit off – which directly correlates to the single bit we changed.
CFB	0x37 in block 4 0x40-0x4F in block 5	In CFB, the ciphertext's will be XOR'd with the plaintext. In our case, the corrupted ciphertext byte in 0x37 is XOR'd with the plaintext, therefore we see 0x37 in the plaintext corrupt. In fact, we see byte 0x37 as 0x62 in the resultant decrypted plaintext versus 0x72 which is one bit off due to our corruption. 0x40-0x4F is fully corrupt due to the cipher text of the previous block 0x30-0x3F being corrupt and then running through the block cipher encryption. This results in the enter block being corrupted.
OFB	0x37 in block 4	In OFB, the cipher text is XOR's with the output of the block cipher of the IV/KEY (or in the next block it's 'block cipher encryption'). Since this is the case, only the current block is affected. To be clear, the ciphertext is XOR'd *after* the block encryption and is not used as input to the next block, so only the current block is affected. In our case, we corrupted byte 55 (0x37) so only that byte and, in particular, the specific bit affects the result since we are bitwise XOR'ing. For byte 0x37, the value is 0x73 vs 0x72, which is one bit off in the final decrypted plaintext.

In this lab, we corrupted one bit of the encrypted binary. We then decrypted the binary and observed the results as compared to what the results should be. In observing each block cipher mode, we were able to determine what and why the entire current block, entire next block, or particular byte (or bits) were affected by the corruption.

Each of the cipher modes were different and resulted in different results. At a high-level:

- ECB only affected the block in which the byte was changed. The whole block was affected by the corruption.
- CBC affected the current block in which the byte was changed and the particular byte / bit that was in the next block. This was due to the XOR with the previous blocks ciphertext.
- CFB affected the next entire block due to the current block's ciphertext being used as input to the block cipher encryption.

- OFB only affect the particular byte / bit of the current block. Since ciphertext is XOR'd after the block cipher encryption, only the byte (in our case bit) is affected.

By running the experiments with the various cipher block modes, we can see how a corruption in the encrypted binaries can affect the current and/or next decrypted blocks.