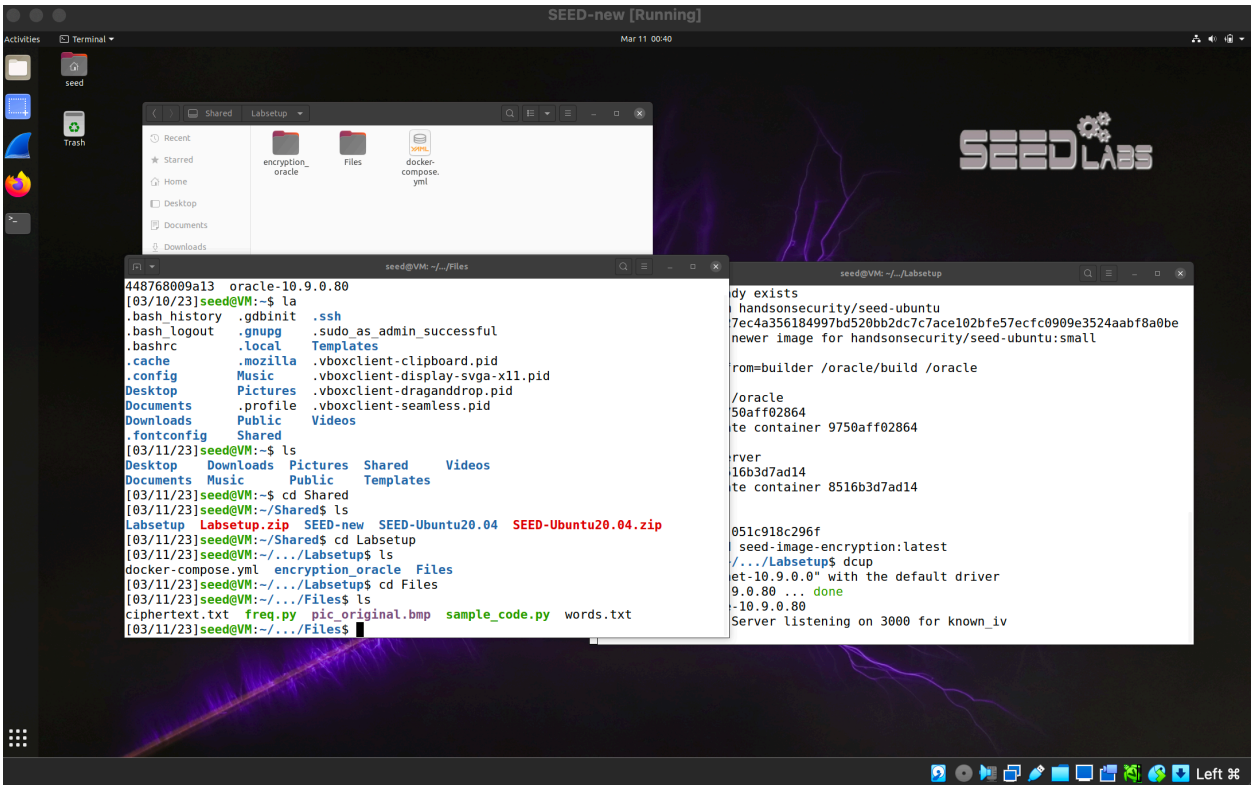
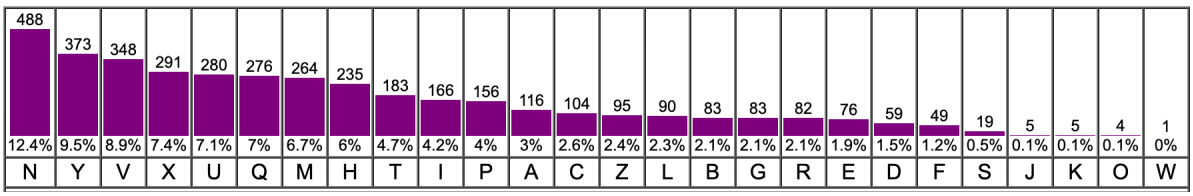
Christian Kuhn
Lab 1
March 12th, 2023

Lab Environment Setup: Here is my SEEDLabs VM setup and running



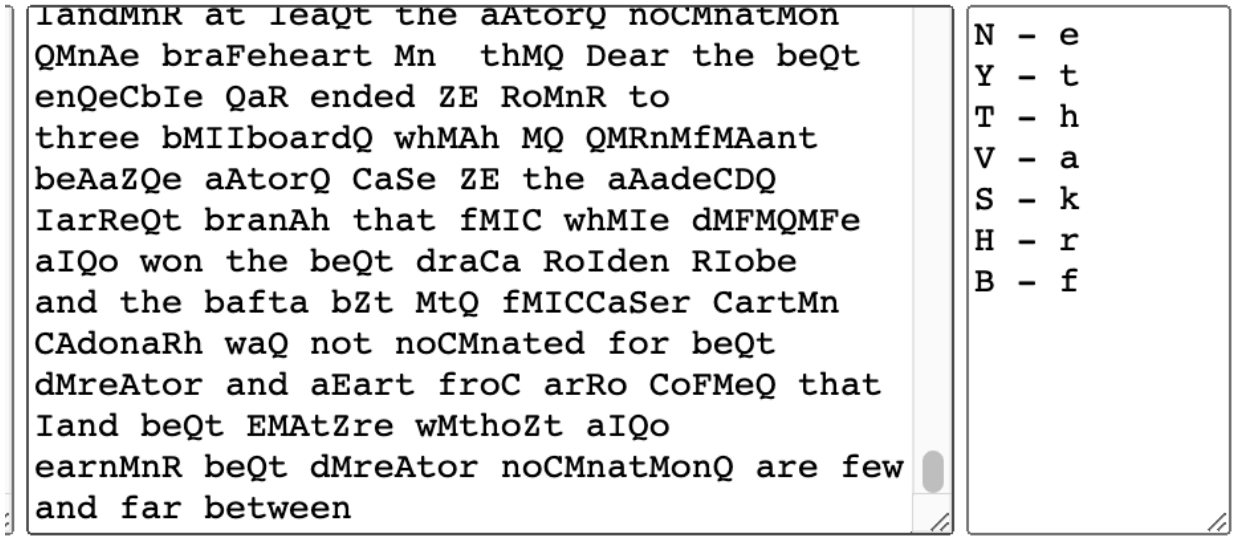
Task 1 Frequency Analysis:

Single Letter Frequencies:



```
[03/11/23]seed@VM:~/.../Files$ freq.py
------------------------------------
1-gram (top 20):
n: 488
y: 373
v: 348
x: 291
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
------------------------------------
2-gram (top 20):
yt: 115
tn: 89
mu: 74
nh: 58
vh: 57
hn: 57
vu: 56
nq: 53
xu: 52
up: 46
xh: 45
yn: 44
np: 44
vy: 44
nu: 42
qy: 39
```

Starting
to decrypt the message:



The last line gave me a very good starting point.
The following is the output text once I finished the frequency analysis:

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

the awards race was bookended by the demise of harvey weinstein at its outset and the apparent implosion of his film company at the end and it was shaped by the emergence of metoo times up blackgown politics armcandy activism and

a national conversation as brief and mad as a fever dream about whether there ought to be a president winfrey the season didnt just seem extra long it was extra long because the oscars were moved to the first weekend in march to avoid conflicting with the closing ceremony of the winter olympics thanks pyeongchang

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

signaling their support golden globes attendees swathed themselves in black sported lapel pins and sounded off about sexist power imbalances from the red carpet and the stage on the air e was called out about pay inequity after its former anchor catt sadler quit once she learned that she was making far less than a male cohost and during the ceremony natalie portman took a blunt and satisfying dig at the allmale roster of nominated directors how could that be topped

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

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

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”

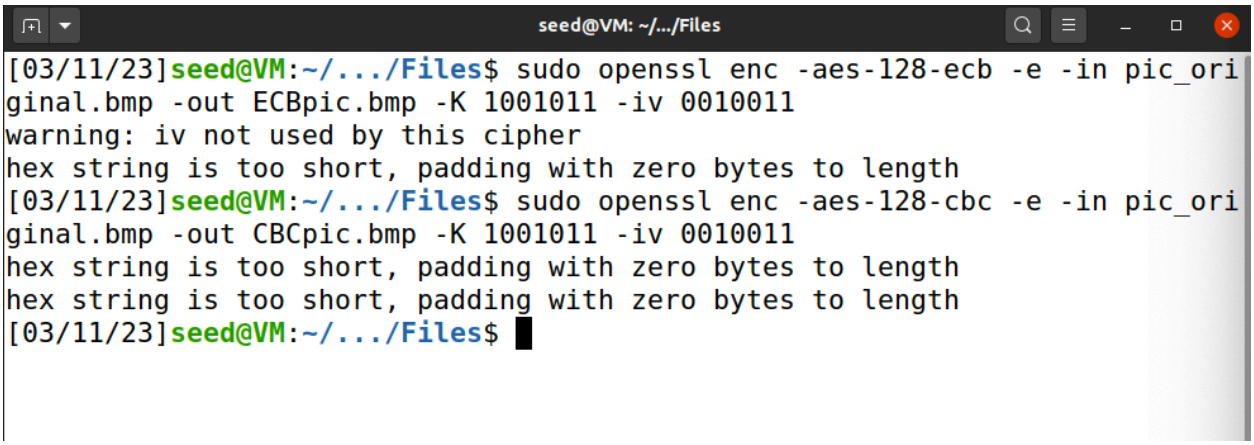
Task 2 Encryption using Different Ciphers and Modes:

Created three ciphers using the following:
-aes-128-cbc, -camellia-128-cfb, -cast5-cfb

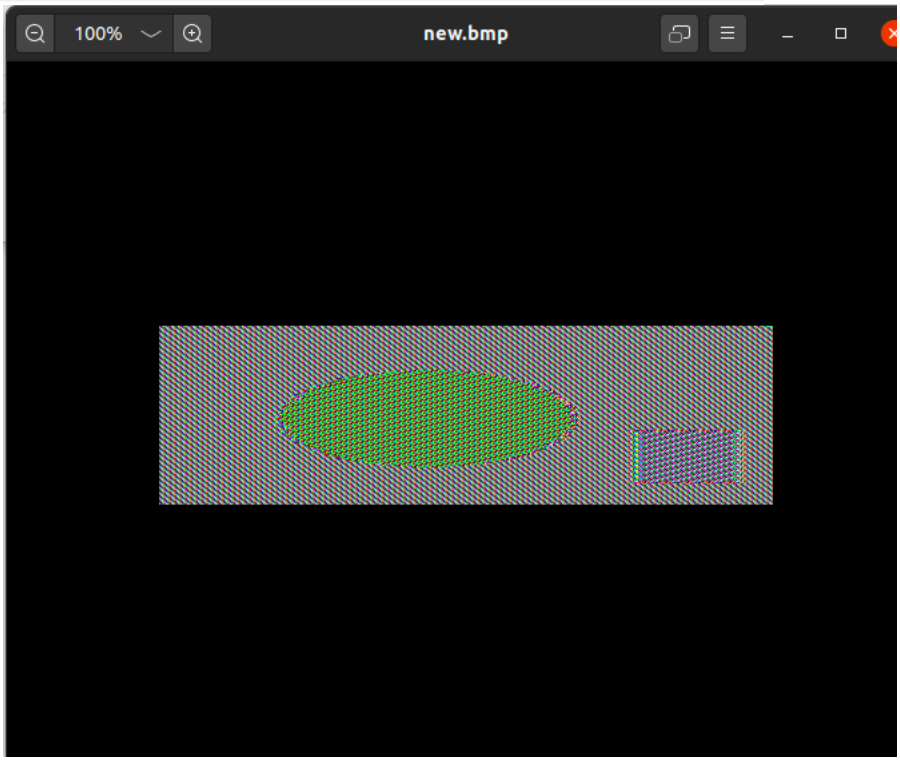
```
[03/11/23]seed@VM:~/.../Labsetup$ sudo openssl enc -aes-128-cbc -e -in plaintext.txt -out cipher1.bin -K 0011223
3445566778889aabbccddeeff -iv 00112233445566778889aabbccddeeff
[03/11/23]seed@VM:~/.../Labsetup$ ls
cipher1.bin  docker-compose.yml  encryption_oracle  Files  plaintext.txt
[03/11/23]seed@VM:~/.../Labsetup$ sudo openssl enc -camelia-128-cfb -e -in plaintext.txt -out cipher2.bin -K 001
12233445566778889aabbccddeeff -iv 00112233445566778889aabbccddeeff
enc: Unrecognized flag camelia-128-cfb
enc: Use -help for summary.
[03/11/23]seed@VM:~/.../Labsetup$ sudo openssl enc -camellia-128-cfb -e -in plaintext.txt -out cipher2.bin -K 00
112233445566778889aabbccddeeff -iv 00112233445566778889aabbccddeeff
[03/11/23]seed@VM:~/.../Labsetup$ ls
cipher1.bin  cipher2.bin  docker-compose.yml  encryption_oracle  Files  plaintext.txt
[03/11/23]seed@VM:~/.../Labsetup$ sudo openssl enc -cast5-fb -e -in plaintext.txt -out cipher3.bin -K 0011223344
5566778889aabbccddeeff -iv 00112233445566778889aabbccddeeff
enc: Unrecognized flag cast5-fb
enc: Use -help for summary.
[03/11/23]seed@VM:~/.../Labsetup$ sudo openssl enc -cast5-cfb -e -in plaintext.txt -out cipher3.bin -K 001122334
45566778889aabbccddeeff -iv 00112233445566778889aabbccddeeff
hex string is too long, ignoring excess
[03/11/23]seed@VM:~/.../Labsetup$ ls
cipher1.bin  cipher2.bin  cipher3.bin  docker-compose.yml  encryption_oracle  Files  plaintext.txt
```

Task 3 Encryption Mode ECB vs. CBC:

ECB & CBC encryption:

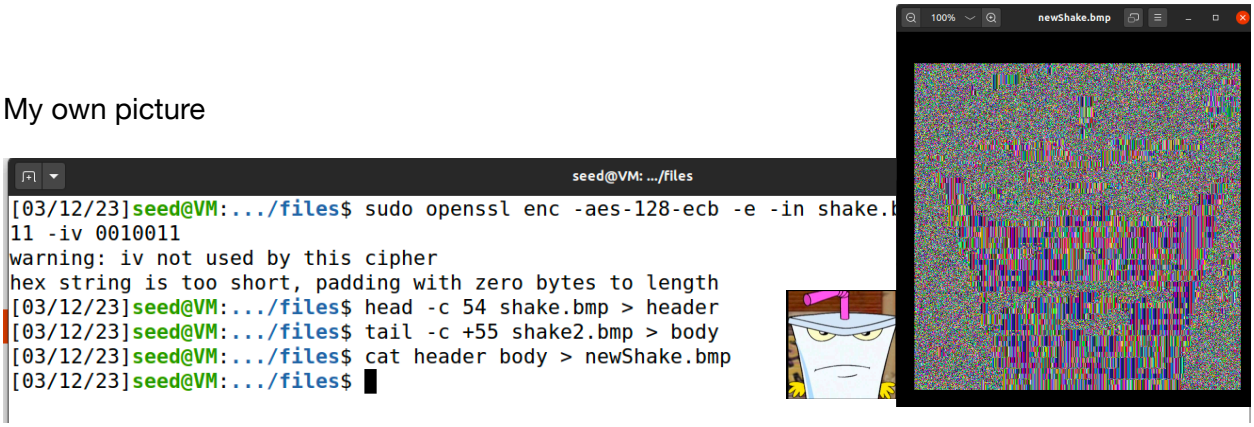



```
$ head -c 54 p1.bmp  > header
$ tail -c +55 p2.bmp > body
$ cat header body > new.bmp
```



From this image, we can make out the general size and shape of objects in the image.

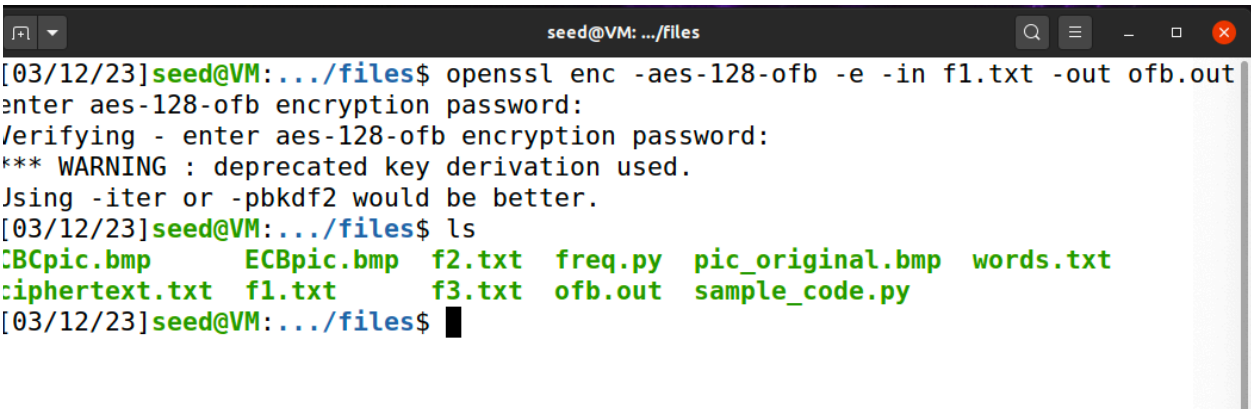
My own picture



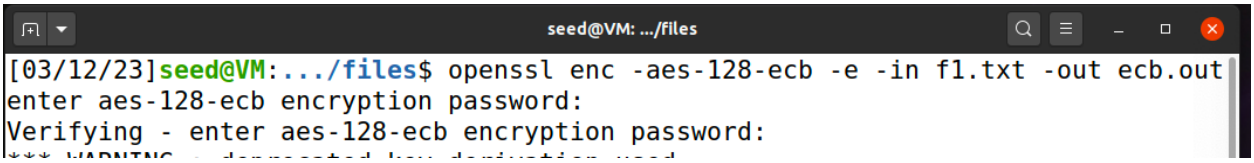
Task 4 Padding:

Create three files which contain 5 bytes, 10 bytes, 16 bytes, respectively

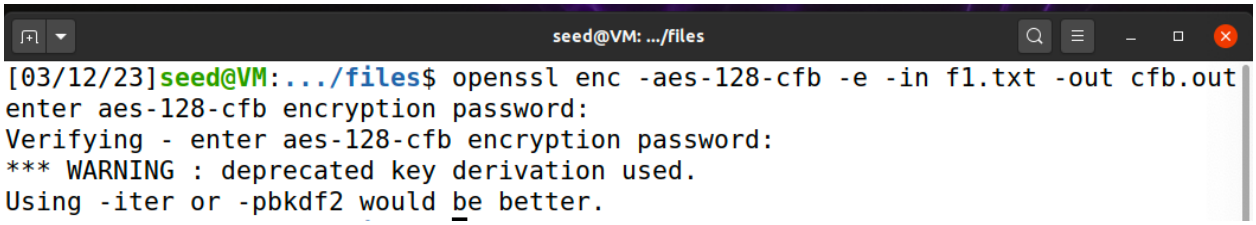
OFB:



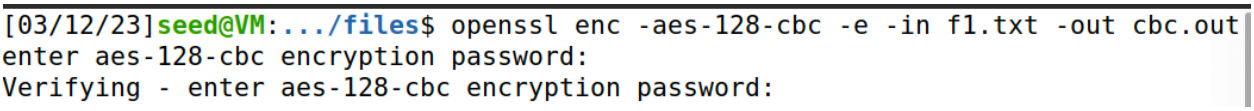
ECB:



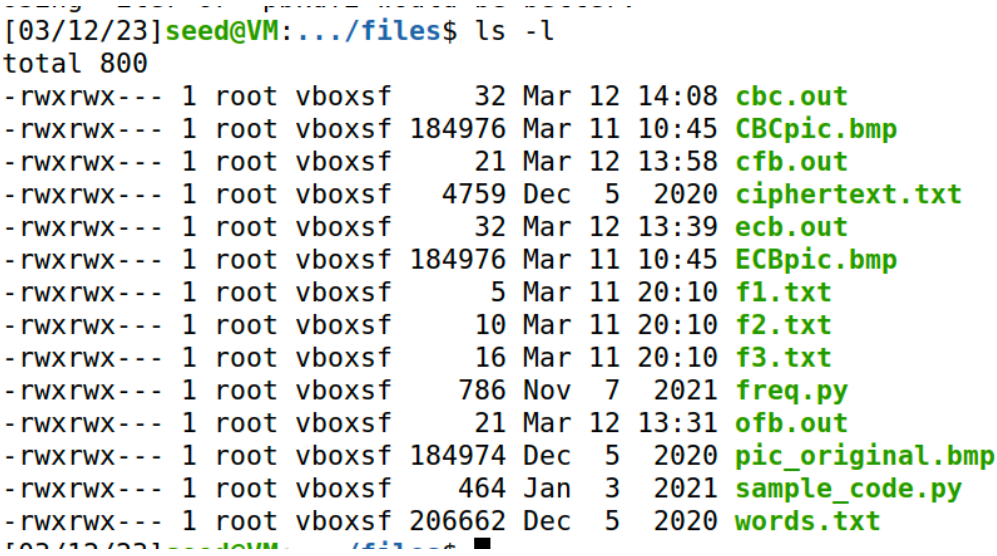
CFB:



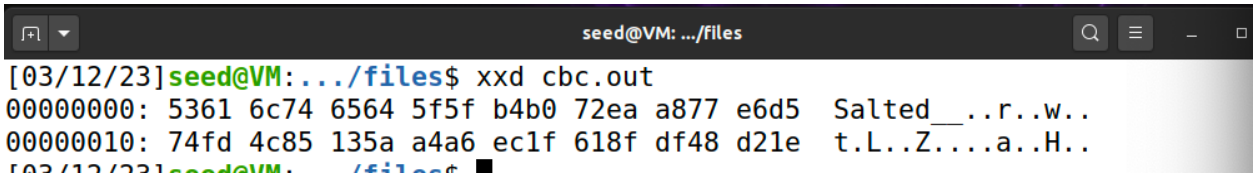
CBC:



Result:

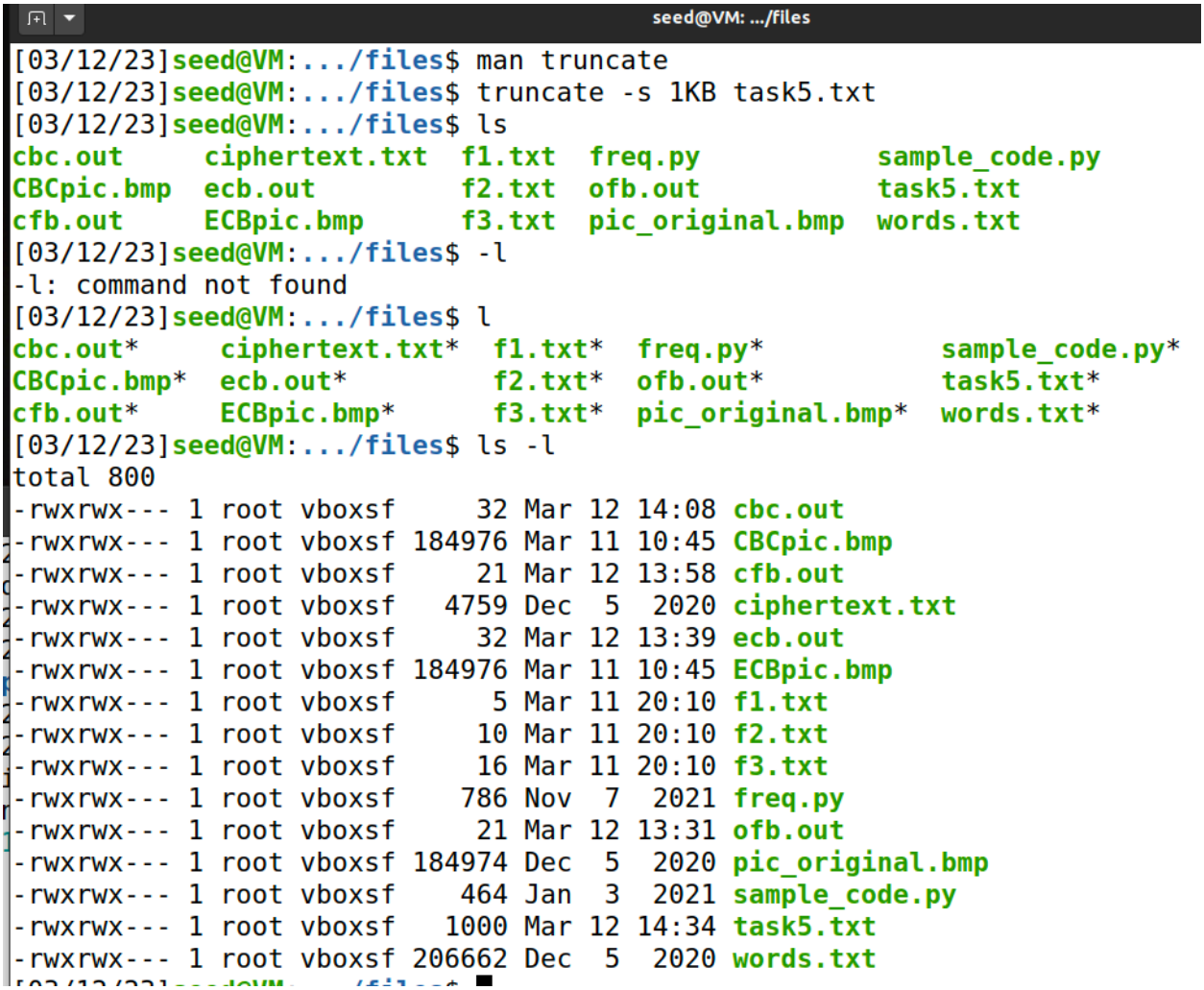


From this screenshot I can see that padding is only needed for ecb and cbc modes. This is because they are block ciphers. Ofb and cfb will not require padding because they are stream ciphers.
File encrypted with cbc

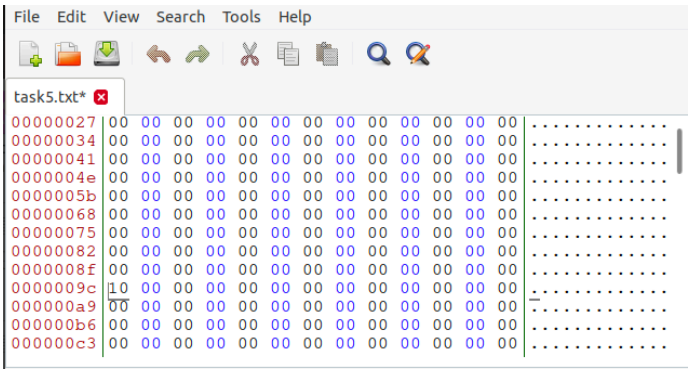


Task 5 Error Propagation:

My predictions
ECB: single bit corruption in one block of the ciphertext will only affect the corresponding block of plaintext, but not the rest of the file.
CBC: single bit corruption in one block of the ciphertext will affect the corresponding block of plaintext as well as the next block of plaintext
CFB: single bit corruption in one block of the ciphertext will affect the corresponding block of plaintext as well as the next several blocks of plaintext
OFB: single bit corruption in one block of the ciphertext will not affect any subsequent blocks of the plaintext
Created a text file that is 1000bytes long:



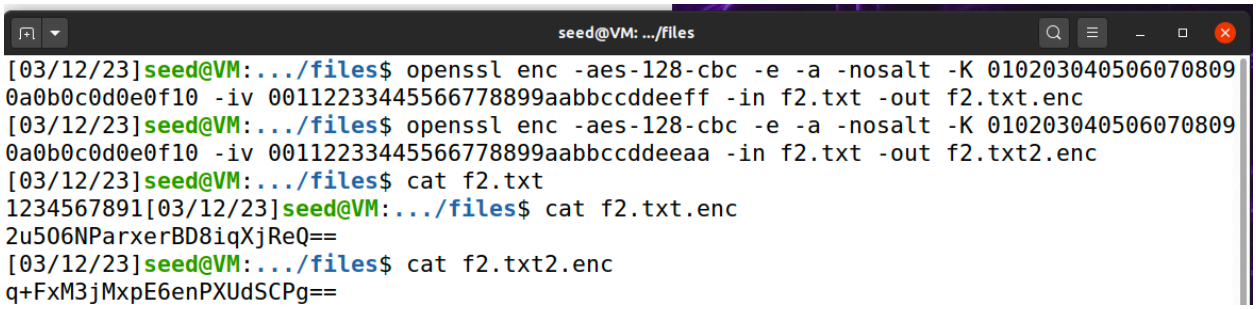
Encrypt the file using a AES-128 cipher(cbc):



After flipping the bit and then decrypting task5.txt I observed no changes in this file. My answer for CBC was wrong.

Task 6 IV and Common Mistakes:

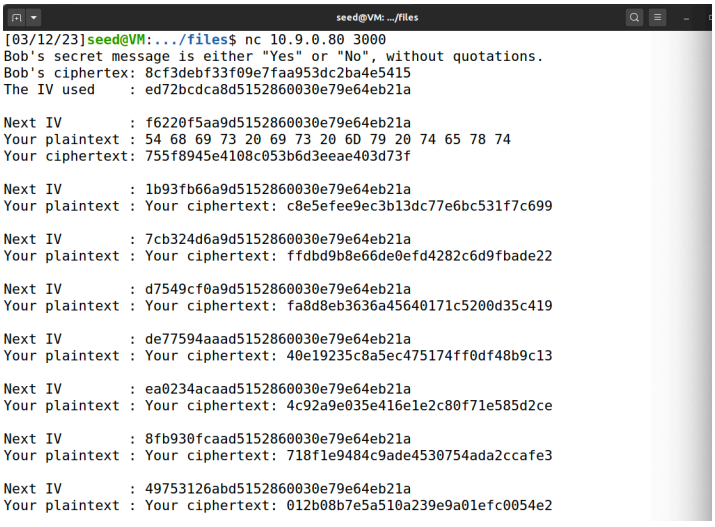
IV Experiment:



I can observe that the encrypted text is changed by changing iv.

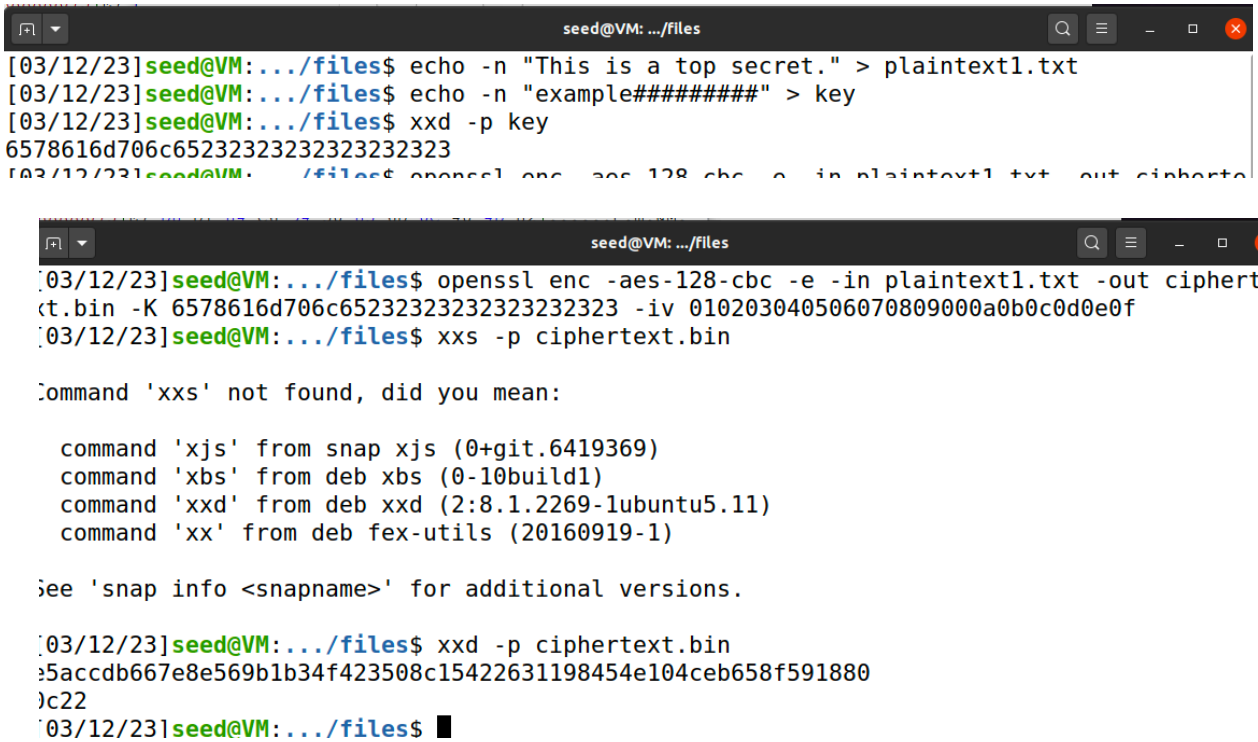
Common Mistake Use the Same IV:
Using CFB mode instead of OFB may potentially allow an attacker to recover more information about P2, as a single bit corruption in the ciphertext in CFB mode is more localized and affects only a few bits of the corresponding plaintext. In contrast, a single bit corruption in OFB mode can propagate and affect the entire block of plaintext.

Common Mistake Use a Predictable IV:



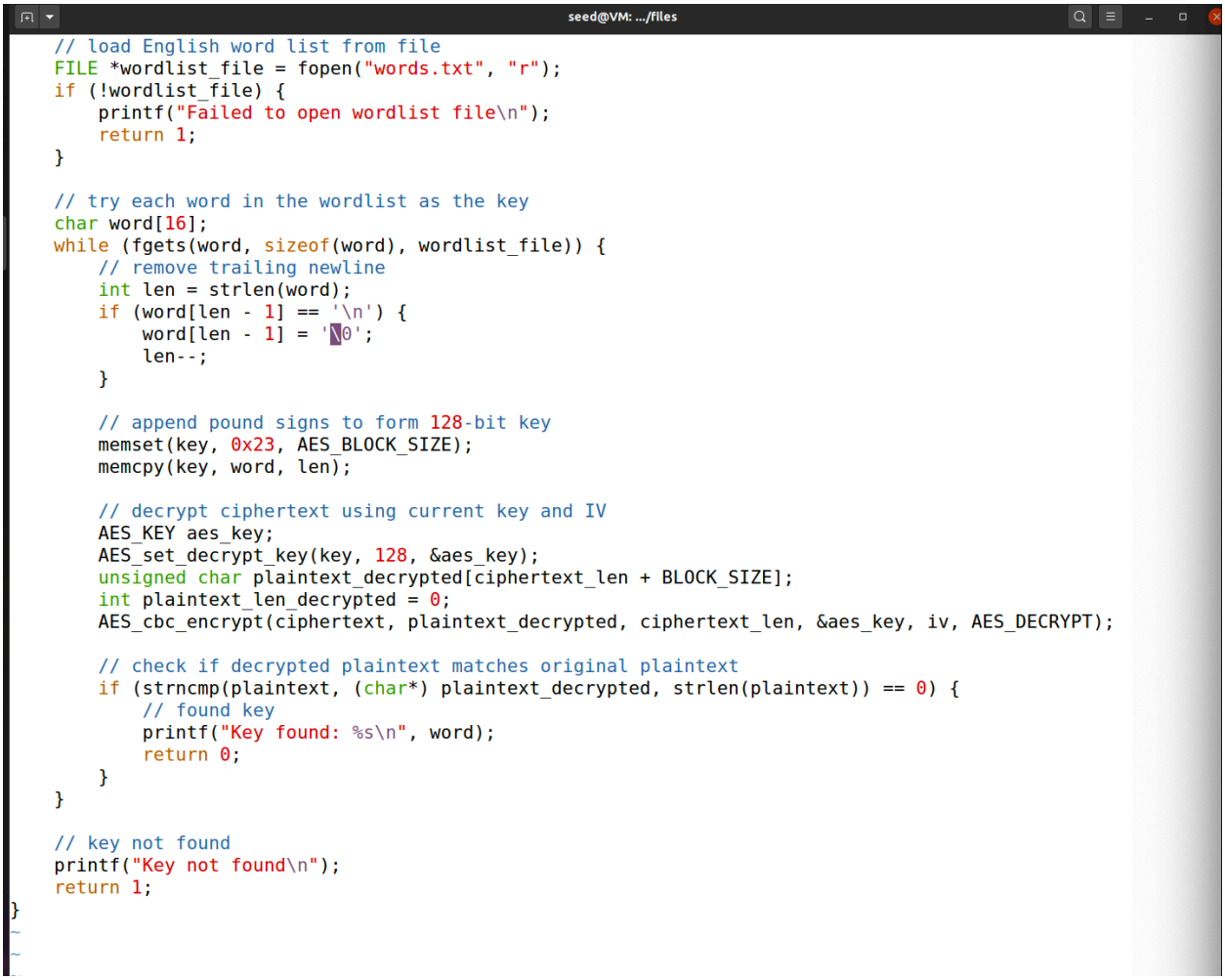
Task 7 Programming Using The Crypto Library:

Plaintext is encrypted with a key



Running the program:

```
[03/12/23]seed@VM:.../files$ ls
body            ciphertext.txt  f2.txt2.enc  header       new.bmp           task5.txt
cbc.out         ecb.out         f2.txt.enc   key          ofb.out           words.txt
CBCpic.bmp      ECBpic.bmp      f3.txt       main         pic_original.bmp
cfb.out         f1.txt          file         main.c       plaintext1.txt
ciphertext.bin  f2.txt          freq.py      message.enc  sample_code.py
[03/12/23]seed@VM:.../files$ gcc -o findkey main.c -lcrypto
[03/12/23]seed@VM:.../files$ ls
body            ciphertext.txt  f2.txt2.enc  freq.py  message.enc       sample_code.py
cbc.out         ecb.out         f2.txt.enc   header   new.bmp           task5.txt
CBCpic.bmp      ECBpic.bmp      f3.txt       key      ofb.out           words.txt
cfb.out         f1.txt          file         main     pic_original.bmp
ciphertext.bin  f2.txt          findkey      main.c   plaintext1.txt
[03/12/23]seed@VM:.../files$ ./findkey "This is a top secret." 764aa26b55a4da654df6b19e4
ce00f4ed05e09346fb0e762583cb7da2ac93a2
Key not found
[03/12/23]seed@VM:.../files$
```


seed@VM: .../files
// load English word list from file
FILE *wordlist_file = fopen("words.txt", "r");
if (!wordlist_file) {
printf("Failed to open wordlist file\n");
return 1;
}
// try each word in the wordlist as the key
char word[16];
while (fgets(word, sizeof(word), wordlist_file)) {
// remove trailing newline
int len = strlen(word);
if (word[len - 1] == '\n') {
word[len - 1] = '\0';
len--;
}
// append pound signs to form 128-bit key
memset(key, 0x23, AES_BLOCK_SIZE);
memcpy(key, word, len);
// decrypt ciphertext using current key and IV
AES_KEY aes_key;
AES_set_decrypt_key(key, 128, &aes_key);
unsigned char plaintext_decrypted[ciphertext_len + BLOCK_SIZE];
int plaintext_len_decrypted = 0;
AES_cbc_encrypt(ciphertext, plaintext_decrypted, ciphertext_len, &aes_key, iv, AES_DECRYPT);
// check if decrypted plaintext matches original plaintext
if (strncmp(plaintext, (char*) plaintext_decrypted, strlen(plaintext)) == 0) {
// found key
printf("Key found: %s\n", word);
return 0;
}
}
// key not found
printf("Key not found\n");
return 1;
}