Lab-8

-By Vikramadithya Ivaturi

**Task1**

**Code:**

#!/usr/bin/env python3

from collections import Counter

import re

TOP\_K = 20

N\_GRAM = 4

# Generate all the n-grams for value n

def ngrams(n, text):

for i in range(len(text) -n + 1):

# Ignore n-grams containing white space

if not re.search(r'\s', text[i:i+n]):

yield text[i:i+n]

# Read the data from the ciphertext

with open('ciphertext.txt') as f:

text = f.read()

# Count, sort, and print out the n-grams

for N in range(N\_GRAM):

print("-------------------------------------")

print("{}-gram (top {}):".format(N+1, TOP\_K))

counts = Counter(ngrams(N+1, text)) # Count

sorted\_counts = counts.most\_common(TOP\_K) # Sort

for ngram, count in sorted\_counts:

print("{}: {}".format(ngram, count)) # Print

Output:

First we start with the frequency analysis if English language. This can be fetched from the below link.

<https://www3.nd.edu/~busiforc/handouts/cryptography/Letter%20Frequencies.html>

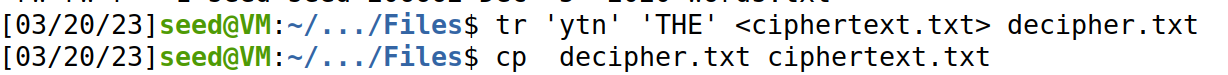
Now, we know which letters, bigrams, trigrams, and quadrigrams are the most frequent in English. With this, we are going to solve the problem.

Now, we fetch the frequency of letters, bigrams, trigrams, and quadrigrams(the code has been modified to include quadrigrams) in the given file.

After this, we compare the frequency ranking from our text as well as the frequency analysis of English.

Now, we try to see if we could make any substitutions in the cipher text depending on the frequency which might make sense.

For example, in the beginning we could see that ‘ytn’ is the most frequent trigram. This is most likely to be ‘THE’, which is the most frequent trigram in English.

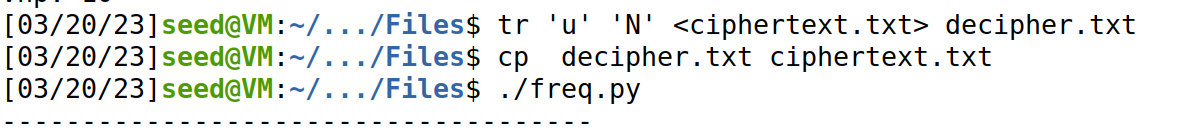


The above tr command replaces the characters respectively with one another from the ciphertext.txt file and place the whole text in decipher.txt file.

In the next command, I am copying the modified text back into the ciphertext.txt file.

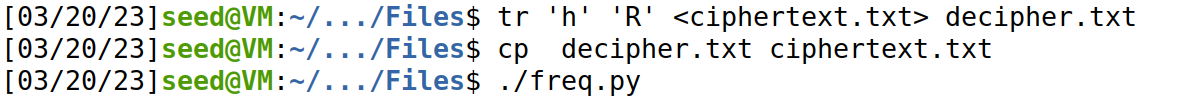
Now, we perform the frequency analysis again to update the stats.

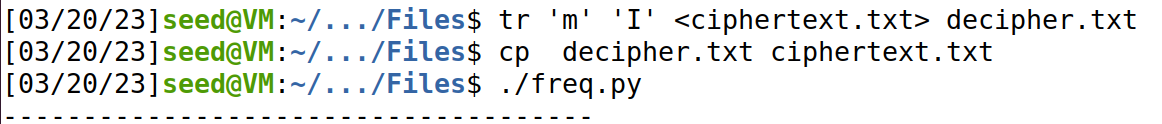
We go on and on with the above methodology, and get the below substitutions.

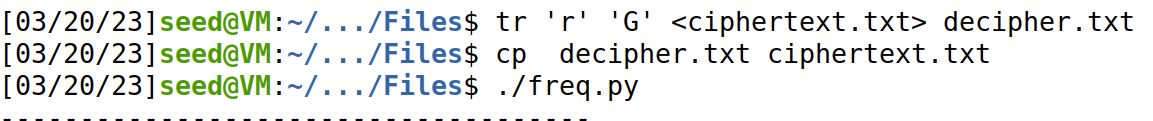


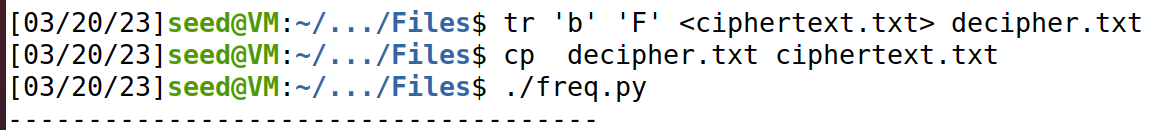
Text

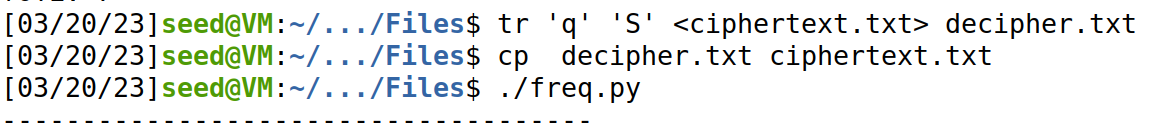
Description automatically generated

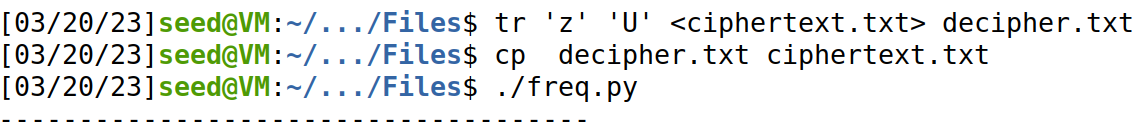


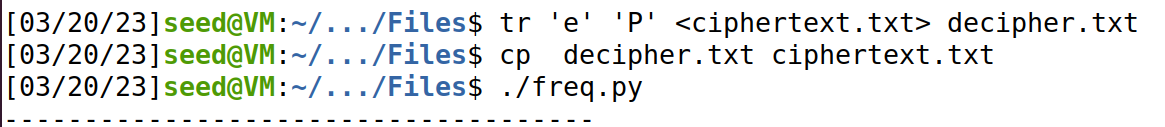


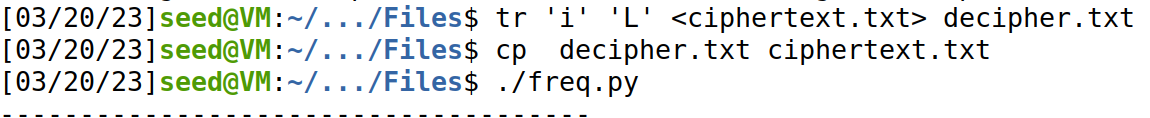


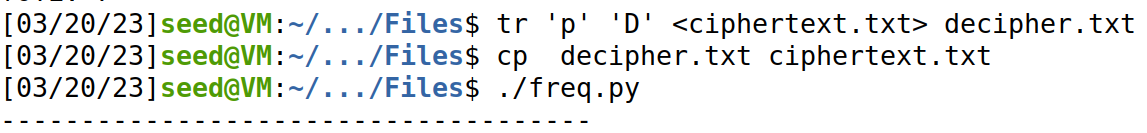


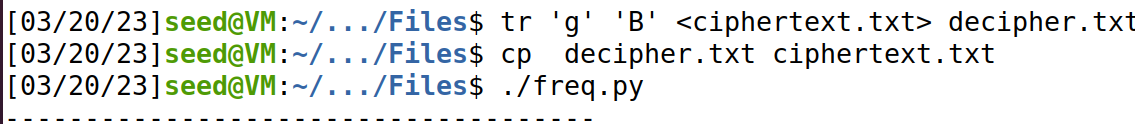


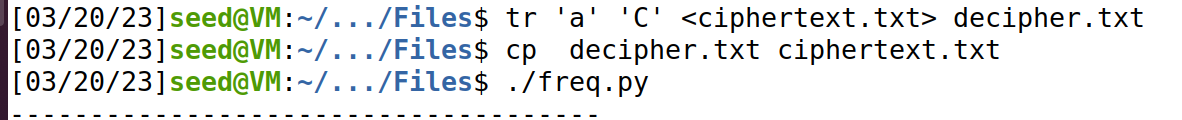


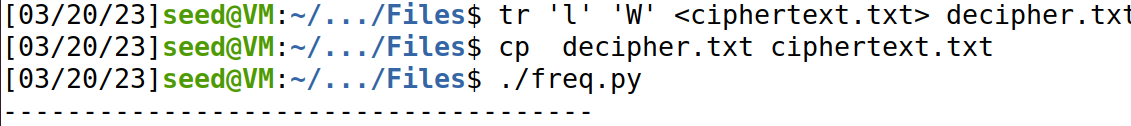


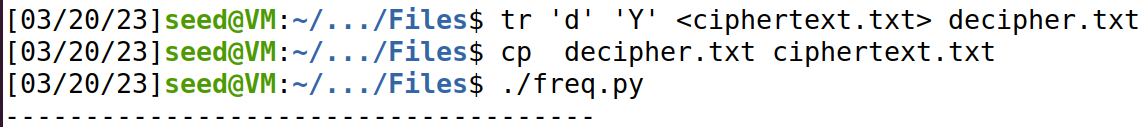


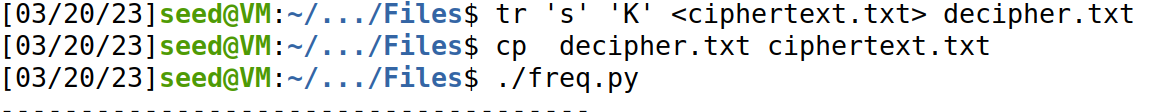


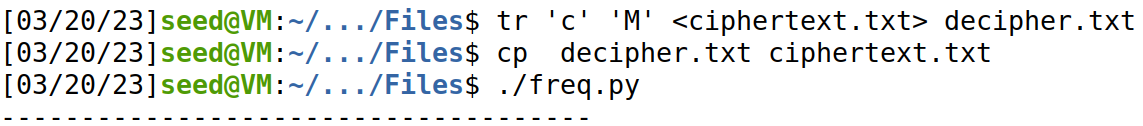


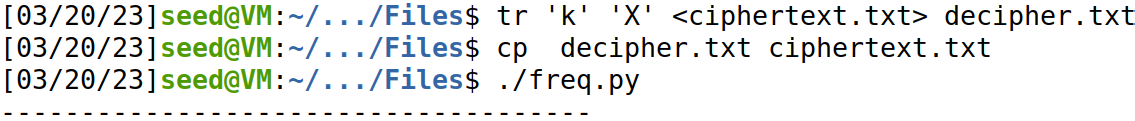


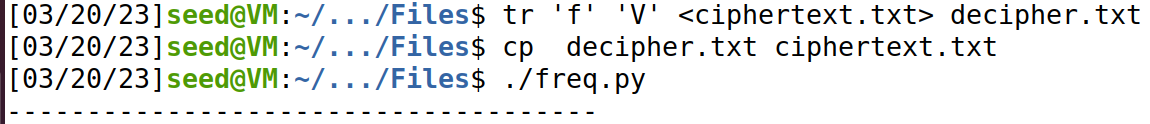


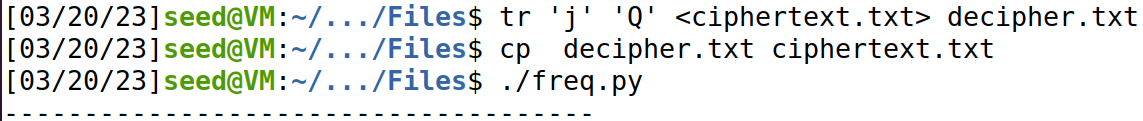


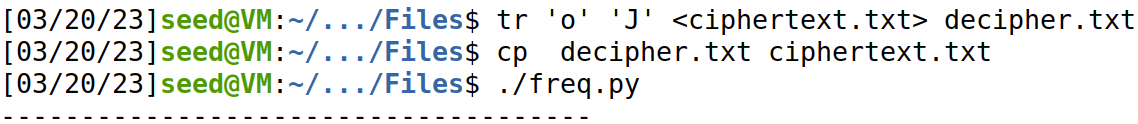


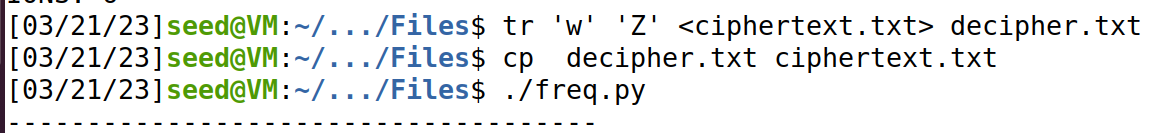












Therefore, the key is a follows.

‘ytnuvxhmrbqzeipgaldsckfjow = ‘THENAORIGFSUPLDBCWYKMXVQJZ’

The original plaintext given in the problem 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 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’

**Task2**

Output:

First we create a text file that has the plain text.



Now, we encrypt the existing plain txt using **AES in ECB mode**.

Graphical user interface, text, Word

Description automatically generated with medium confidence

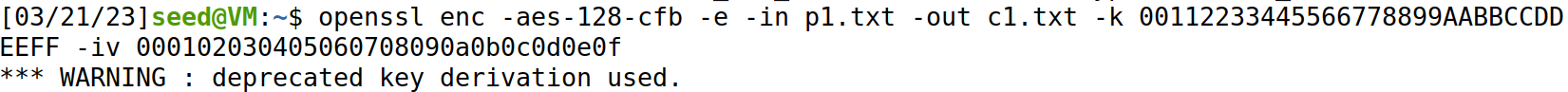
Now, we decrypt the file.

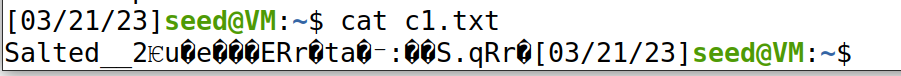
Graphical user interface, text

Description automatically generated with medium confidence

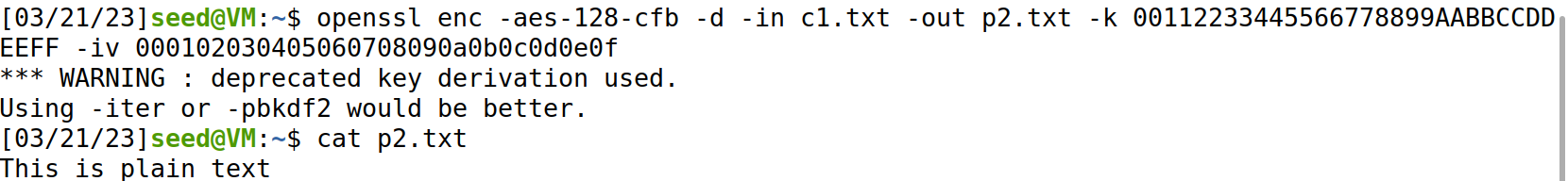
We can see in the above screenshot that we were able to successfully decrypt the file back to it’s original form.

Now, we encrypt the existing plain txt using **AES in CFB mode**.



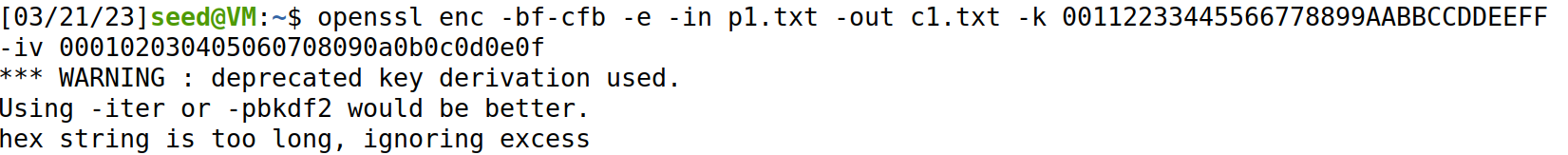


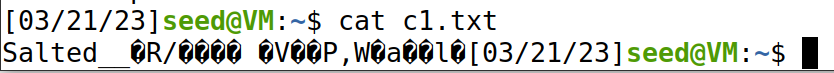
Now, we decrypt



We got the plain text back.

Now, we encrypt the existing plain txt using **Blowfish in CBC mode**.





Text

Description automatically generated with medium confidence

We got the plain text back.

**Task6**

**Task6.1**

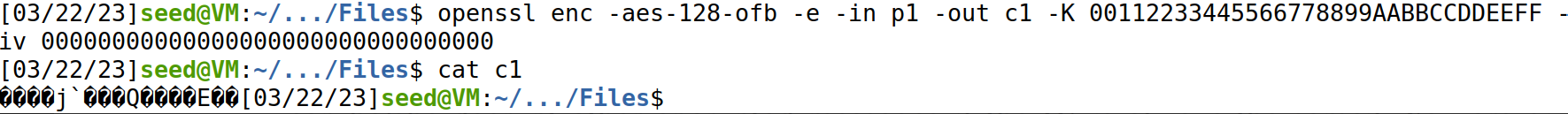
Output:

First, we make a file that has the desired plain text.

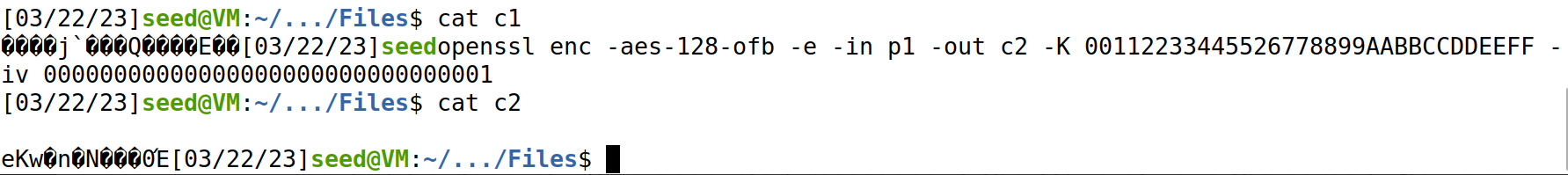
****

Now, you encrypt the file using AES in OFB mode

1. Using two different IVs



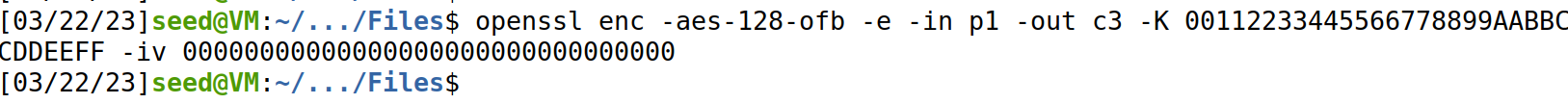
Now, we change the last character in the IV for the



We can clearly see that the ciphers for both the encryptions are different because of different IVs.

1. Using same IV for different messages

Now, we encrypt the same file p1 with the same key another time.



Now, we check the file’s contents.

Text

Description automatically generated

We can see that it is the exact same replica of c1. So, using the same IV with the same key and data gives out the same cipher.

**Task6.2**

Code:

The below program is created for the XOR functionality between two HEX strings.

Text

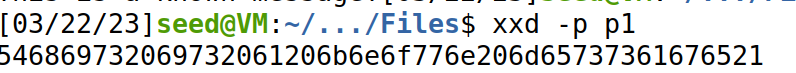
Description automatically generated

Output:

First we create a file that has the given text p1.



Now, we convert the ASCII text into HEX string.



Now, we use the above program to XOR p1 with c1

After that, we use the same program to XOR c2 and the XOR result obtained from the previous step.

After we receive the final HEX string, we convert that back into ASCII string.

Text

Description automatically generated

So, we have successfully decrypted p2.

**Task6.3**

First we get the Hex string for ‘Yes’ which we guessed to be bob’s encrypted message.

A picture containing chart

Description automatically generated

Now, we pad the HEX with 0d which is the Hex value for 13, which is repeated 13 times.

13 is selected as the total number of bytes in the hex should be 16, and the current hex is 3 bytes.

5965730d0d0d0d0d0d0d0d0d0d0d0d0d.

Now, we start the docker container for the oracle server. Text

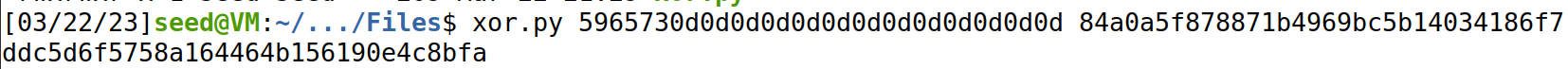
Description automatically generated with medium confidence

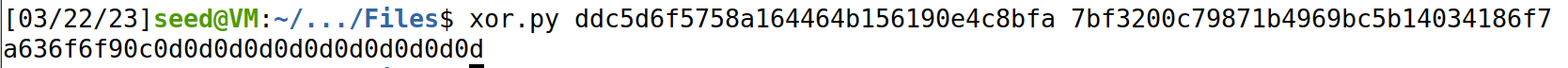
Now we connect to the server from our machine on port 3000.

Text

Description automatically generated

We XOR the padded Hex value of ‘Yes’ with the IV used to obtain a HEX, we XOR that output with the next (predicted) IV. This output is provided as the input to the server.





Now, we see in the encrypted reply from the server that original Bob’s cipher is the same as the current cipher (highlighted). Which means that the input that we have given ‘Yes’ is the correct.

Graphical user interface, text

Description automatically generated

We have successfully performed the attack.

**Task7**

Code:

#!/usr/bin/python3

from Crypto.Cipher import AES

from Crypto.Util import Padding

import re

with open('words.txt','r') as f:

for x in f:

if len(x) <= 16:

key\_string=x.rstrip().ljust(16,'#')

#print(key\_string)

key = bytes.fromhex(key\_string.encode('utf-8').hex())

iv\_hex\_string = 'aabbccddeeff00998877665544332211'

iv = bytes.fromhex(iv\_hex\_string)

data= b'This is a top secret.'

expected\_ciphertext = "3879c71b232cd0d2fc6f5ffcc1d76f074c0fcbe007d9cc53939fdeebf1d6ffd2"

cipher = AES.new(key, AES.MODE\_CBC, iv)

ciphertext = cipher.encrypt(Padding.pad(data, 16))

# print("Ciphertext: {0}".format(ciphertext.hex()))

if (ciphertext.hex() == expected\_ciphertext):

print(x)

Output:

A picture containing text

Description automatically generated