Phat Le
Sept 10th 2020
Homework 1
CMPE 132

Homework 1

Task1

This task will perform the frequency analysis to decipher two different texts (ciphertext.txt and ciphertext-o.txt). The frequency analysis and decipher will use C++ program. Specifically, the program will read in the text line by line into a string array. Then, we will count the frequency of each letter into an STL map and print out the table using function **characterFrequency()** shown in *Figure 1* below.

```
void characterFrequency(string str[], int size);
void printText(string str[], int size);
void replaceCharacter1(string str[], int size);
void replaceCharacter2(string str[], int size);
```

Figure 1: List of functions use in Task 1

```
void characterFrequency(string str[],int size){
    map<char,int> map;   //use STL map to store frequency

    for(int j = 0; j < size; j++){                          // line number loop
        for(int i = 0; str[j][i] != '\0'; i++){             //each element in a line loop
            if(isalpha(str[j][i])){                         // count character only
                if(map.find(str[j][i]) == map.end()){       //if not in the map yet
                    map.insert(make_pair(str[j][i],1));
                }else{                                      //increment the element if found
                    map[str[j][i]]++;
                }
            }
        }
    }

    //print out the frequency table
    for(auto i = map.begin(); i != map.end(); i++){
        cout << i->first << " " << i->second << endl;        //print out the map
    }
}
```

Figure 2: List of functions use in Task 1

Based on the frequency of common English characters given from the lecture slide shown in *Figure 3*, we replace the highest occurrence characters of the ciphertext with the highest occurrence characters.

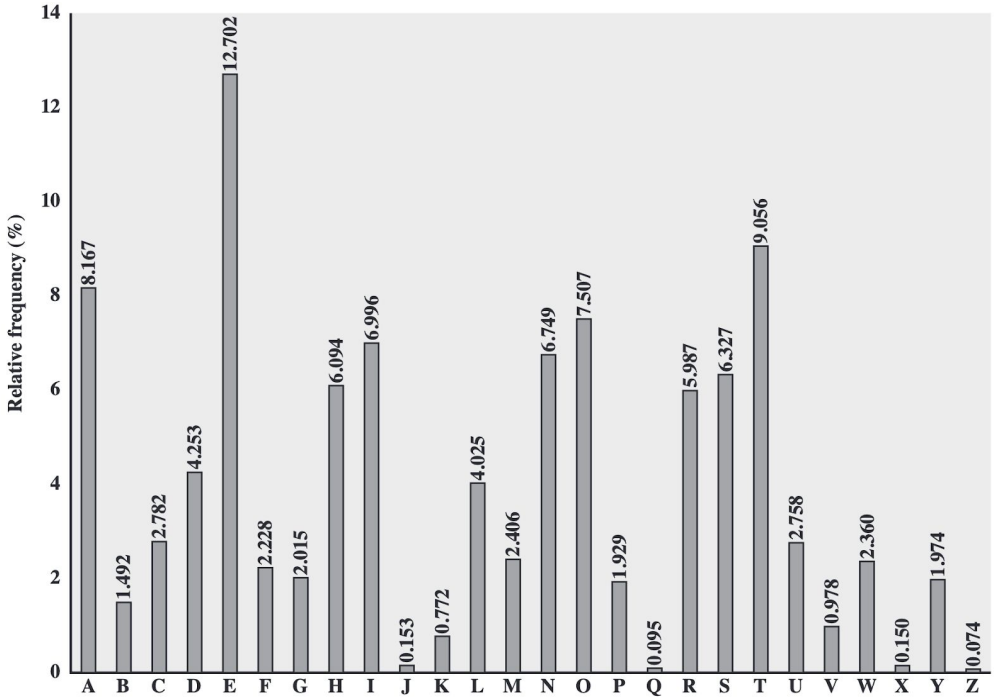

Figure 3: Relative Frequency of Letters in English Text

For easier deciphering, the next task is to replace lowercase letters with uppercase using **replaceCharacter()** function. The easiest method so far is to spot the word 'THE' by replacing the most common letters. More clues will appear as we swap out more letters with trial and errors of letters that have the similar occurrence in the text (*Figure 5*).

In the end, we will have two different plaintexts that have readable English words. In addition, we will be able to obtain 2 different keys maps for each text as shown in *Figure 4* below.

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

Figure 4: Mapped key letter for each ciphertext

	Occurrences	
Letters	**ciphertext.txt**	**ciphertext-o.txt**
a	116	495
b	83	184
c	104	5
d	59	10
e	76	212
f	49	1174
g	83	104
h	235	241
i	166	861
j	5	636
k	5	141
l	90	288
m	264	433
n	488	825
o	4	295
p	156	3
q	276	860
r	82	126
s	19	753
t	183	10
u	280	339
v	348	751
w	1	179
x	291	75
y	373	723
z	95	589

Figure 4: Occurrence of Letters

To make sure that two keys are correct, I used them to decipher the text again in the linux command terminal as shown in *Figure 5* and *6* below.

```
/bin/bash
/bin/bash 82x24
[09/11/20]seed@VM:~$ cd Downloads
[09/11/20]seed@VM:~/Downloads$ tr 'abcdefghijklmnopqrstuvwxyz' 'CFMIPVBRLQXWIEJD
SGKHNAZOTU' <ciphertext.txt> plaintext.txt
[09/11/20]seed@VM:~/Downloads$ cat plaintext.txt
THE OSCARS TURN  ON SUNDAI WHICH SEEMS ABOUT RIGHT AFTER THIS LONG STRANGE
AWARDS TRIP THE BAGGER FEELS LIKE A NONAGENARIAN TOO

THE AWARDS RACE WAS BOOKENDED BI THE DEMISE OF HARVEI WEINSTEIN AT ITS OUTSET
AND THE APPARENT IMPLOSION OF HIS FILM COMPANI AT THE END AND IT WAS SHAPED BI
THE EMERGENCE OF METOO TIMES UP BLACKGOWN POLITICS ARMCANDI ACTIVISM AND
A NATIONAL CONVERSATION AS BRIEF AND MAD AS A FEVER DREAM ABOUT WHETHER THERE
OUGHT TO BE A PRESIDENT WINFREI 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 CEREMONI OF THE WINTER OLIMPICS THANKS
PIEONGCHANG

ONE BIG QUESTION SURROUNDING THIS IEARS ACADEMI AWARDS IS HOW OR IF THE
CEREMONI WILL ADDRESS METOO ESPECIALLI AFTER THE GOLDEN GLOBES WHICH BECAME
A JUBILANT COMINGOUT PARTI FOR TIMES UP THE MOVEMENT SPEARHEADED BI
POWERFUL HOLLIWOOD WOMEN WHO HELPED RAISE MILLIONS OF DOLLARS TO FIGHT SEXUAL
HARASSMENT AROUND THE COUNTRI

SIGNALING THEIR SUPPORT GOLDEN GLOBES ATTENDEES SWATHED THEMSELVES IN BLACK
SPORTED LAPEL PINS AND SOUNDED OFF ABOUT SEXIST POWER IMBALANCES FROM THE RED
```

Figure 5: Decipher ciphertext.txt using terminal

```
/bin/bash
/bin/bash 82x24

[09/11/20]seed@VM:~/Downloads$ tr 'abcdefghijklmnopqrstuvwxyz' 'DWQJCEVUTSPFLRMX
OZGIBKNH' <ciphertext-o.txt> plaintext-o.txt
[09/11/20]seed@VM:~/Downloads$ cat plaintext-o.txt
THE FELLOWSHIP OF THE RING
MAIN ARTICLE THE LORD OF THE RINGS THE FELLOWSHIP OF THE RING

IN THE SECOND AGE OF MIDDLEEARTH THE LORDS OF ELVES DWARVES AND MEN ARE GIVEN RI
S OF POWER UNBEKNOWNST TO THEM THE DARK LORD SAURON FORGES THE ONE RING IN MOUNT
OOM INFUSING INTO IT A GREAT PART OF HIS POWER TO DOMINATE THROUGH IT AND AT A D
TANCE THE OTHER RINGS SO HE MIGHT CONQUER MIDDLEEARTH A FINAL ALLIANCE OF MEN AN
ELVES BATTLES SAURONS FORCES IN MORDOR WHERE PRINCE ISILDUR OF GONDOR SEVERS SAU
NS FINGER AND THE RING WITH IT THEREBY DESTROYING HIS PHYSICAL FORM WITH SAURONS
IRST DEFEAT THE THIRD AGE OF MIDDLEEARTH BEGINS UNFORTUNATELY THE RINGS INFLUENC
CORRUPTS ISILDUR AND RATHER THAN DESTROY THE RING ISILDUR TAKES IT FOR HIMSELF I
LDUR IS LATER KILLED BY ORCS AND THE RING IS LOST FOR  YEARS UNTIL IT IS FOUND B
GOLLUM WHO OWNS IT FOR FIVE CENTURIES THE RING IS THEN FOUND BY A HOBBIT NAMED B
BO BAGGINS WHO TURNS INVISIBLE WHEN HE PUTS IT ON BUT IS UNAWARE OF ITS HISTORY

SIXTY YEARS LATER BILBO CELEBRATES HIS TH BIRTHDAY IN THE SHIRE REUNITING WITH H
 OLD FRIEND GANDALF THE GREY BILBO REVEALS THAT HE INTENDS TO LEAVE THE SHIRE FO
ONE LAST ADVENTURE AND HE LEAVES HIS INHERITANCE INCLUDING THE RING TO HIS NEPHE
FRODO ALTHOUGH BILBO HAS BEGUN TO BECOME CORRUPTED BY THE RING AND TRIES TO KEEP
T FOR HIMSELF GANDALF INTERVENES GANDALF SUSPICIOUS OF THE RING TELLS FRODO TO K
```

Figure 6: Decipher ciphertext-o.txt using terminal

Task 2

For this task, we will perform encryption cursing different methods. The original text is plaintask2.txt shown in *Figure 7* below. *Figure 8, 9 and 10* are three different methods that hide the text information.

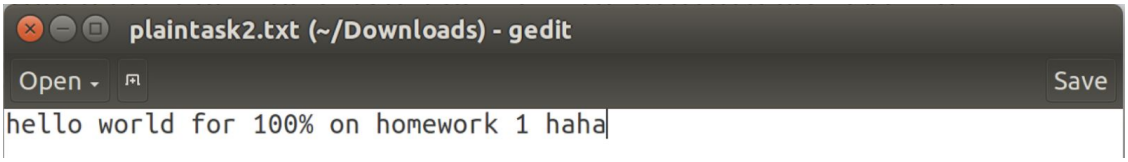

Figure 7: Encryption using -aes-128-cbc

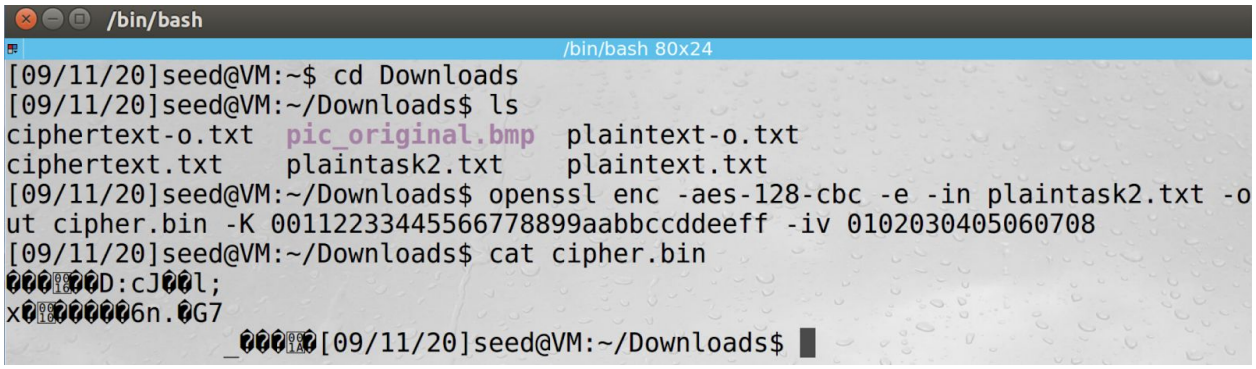

Figure 8: Encryption using -aes-128-cbc

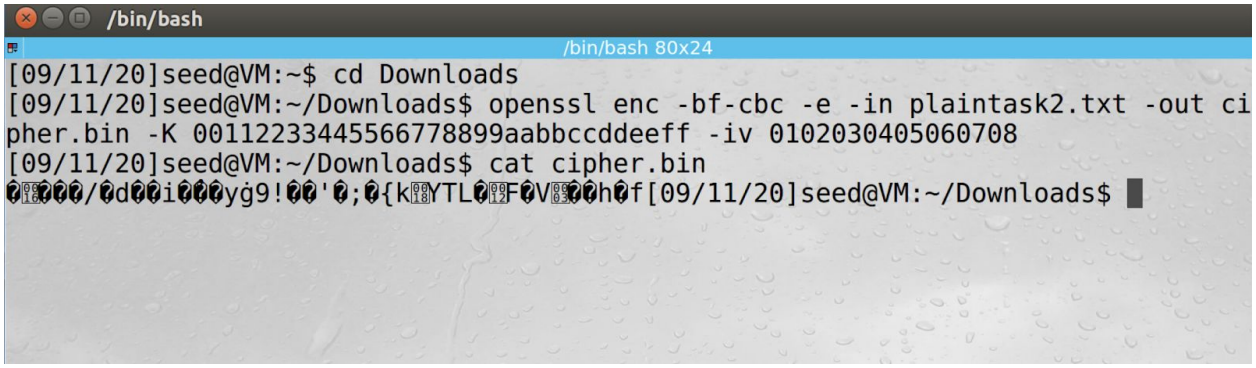

Figure 9: Encryption using -bf-cbc

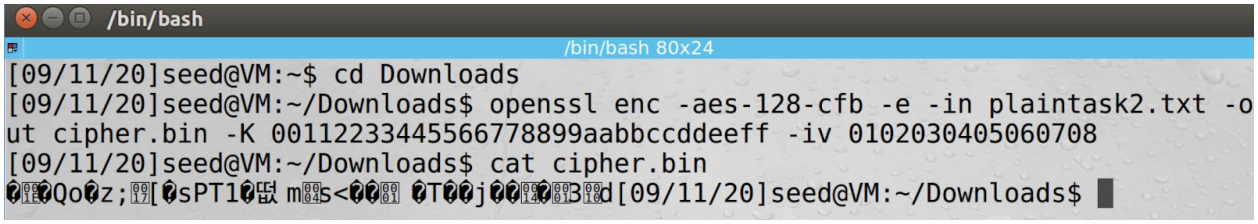

Figure 10: Encryption using -aes-128-cfb

Task 3

For this task, we encrypted an image called pic_original using ECB and CBC mode. According to Figure 11 and 12, it seems that the CBC encryption is the better method since the encrypted image is totally different from original. One thing to notice is that the ECB does not need an initial vector (-iv).

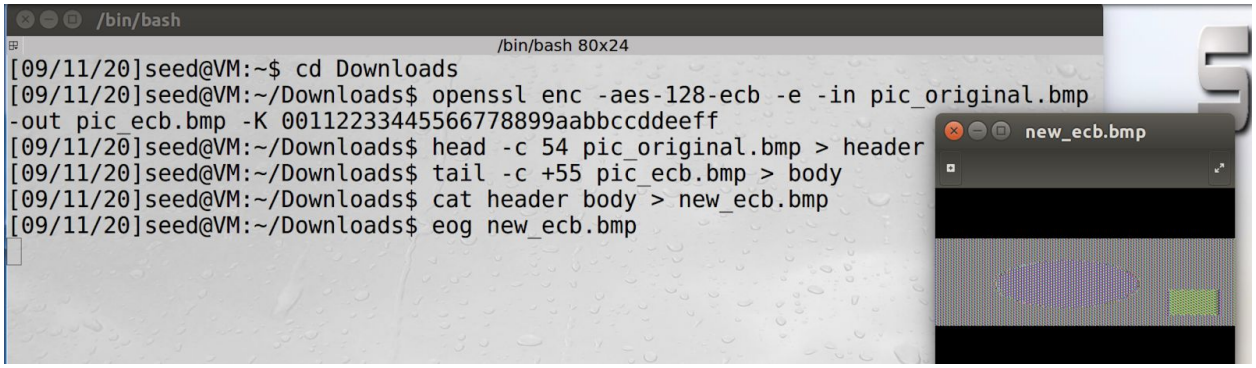

Figure 11: Encryption using ecb mode

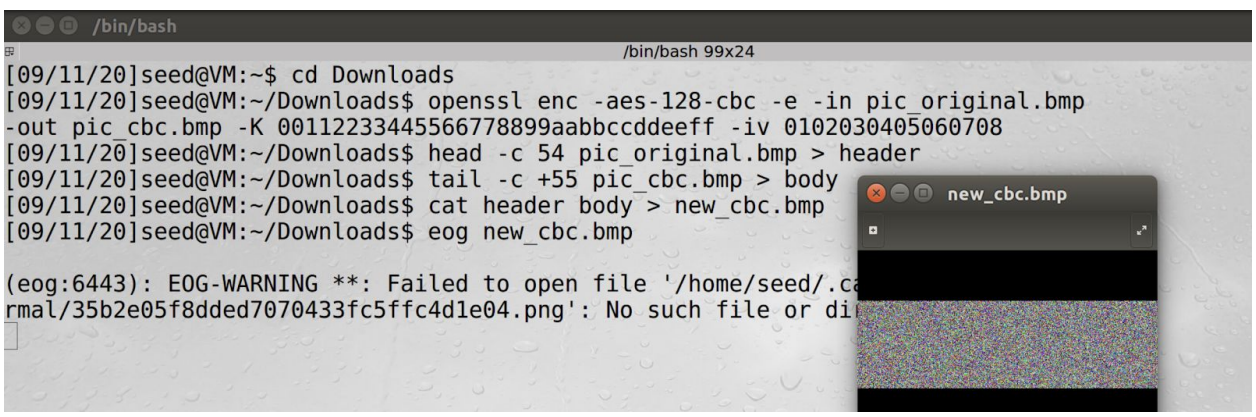

Figure 12: Encryption using cbc mode

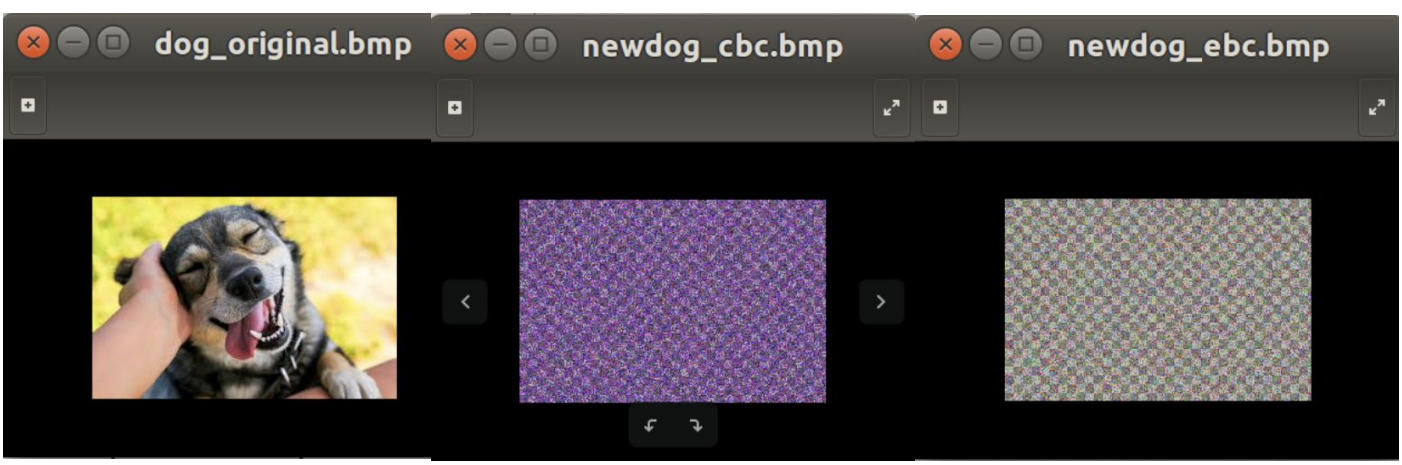

Figure 13: Encryption using a different image

When testing a more complex image, it seems that all encryption methods are doing well at hiding color and shape information.