Student Declaration of Authorship

HERIOT WATT UNIVERSITY

UK | DUBAI | MALAYSIA

Course code and name:	F21CN Computer Network Security
Type of assessment:	**Individual**
Coursework Title:	Symmetric Encryption
Student Name:	Salman Ansari
Student ID Number:	H00410360

Declaration of authorship. By signing this form:

- **I declare** that the work I have submitted for individual assessment OR the work I have contributed to a group assessment, is entirely my own. I have NOT taken the ideas, writings or inventions of another person and used these as if they were my own. My submission or my contribution to a group submission is expressed in my own words. Any uses made within this work of the ideas, writings or inventions of others, or of any existing sources of information (books, journals, websites, etc.) are properly acknowledged and listed in the references and/or acknowledgements section.

- I confirm that I have read, understood and followed the University's Regulations on plagiarism as published on the University's website, and that I am aware of the penalties that I will face should I not adhere to the University Regulations.

- I confirm that I have read, understood and avoided the different types of plagiarism explained in the University guidance on Academic Integrity and Plagiarism

Student Signature: *Salman Ansari*

Date: *25/10/2022*

COMPUTER NETWORK SECURITY

F21CN

Coursework 1

Symmetric Encryption

Name: Salman Ansari

HW ID: H00410360

Index

1. Introduction

Symmetric encryption is the first coursework for Computer Network Security (F21CN). Upon completion of this coursework, I hope to understand the different methodologies used in Symmetric Encryption. Through this coursework, I'm also hoping to get deeper understanding of the various encryption ciphers like aes-128-cbc, aes-192-cbc and other cipher modes, how frequency analysis is used to decrypt ciphertext and how padding works.

For Task 1, I expect to understand how frequency analysis is used to decrypt ciphertext.

For Task 2, I would observe how padding works for different file size in encryption and decryption.

For Task 3, I would like to observe what corruption does in different modes of encryption.

For Task 4, I hope to learn to write a script to match a word from dictionary.

To complete this coursework, I am using CentOS 9 installed on Oracle VM VirtualBox.

Operating System:	CentOS Stream 9
Kernel:	Linux 5.14.0-163.el9.x86_64
Architecture:	x86-64

2. Task 1: Frequency Analysis: Monoalphabetic Substitution Cipher

2.1. Objectives

- Using frequency analysis to decrypt the ciphertext to plaintext.
- Frequency analysis provides us with information how often a letter or combination of letters occur in English language.
- I am provided with a ciphertext file (cipher-task1-188). Also, provided a link where I can get the frequency analysis of alphabets occurring in the corpus, along with the bigram and trigram frequency. (Link: https://onlinetoolz.net/letter-frequency)
- With the help of given links, I will try to decrypt the ciphertext.

2.2. Implementation

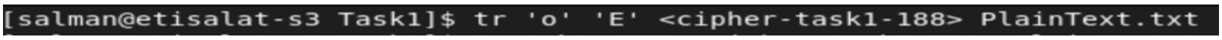
General Notation:

Lowercase → Cipher text

Uppercase → Plain text

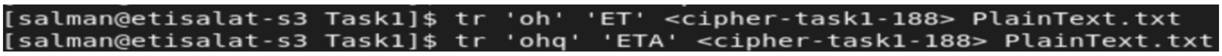
First, I calculated the letter frequency of the ciphertext using the provided website https://onlinetoolz.net/letter-frequency. From this website, I got the highest occurring alphabet followed by the alphabets in decreasing order of their occurrence. Then comparing it with the Wikipedia English letter frequency for single letter, bigrams, and trigrams.

The next step is to start replacing a single letter of the ciphertext with single plaintext letter.



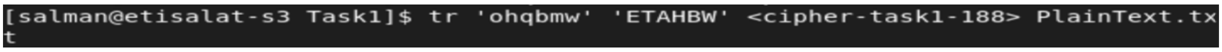
```
[salman@etisalat-s3 Task1]$ tr 'o' 'E' <cipher-task1-188> PlainText.txt
```

I start with replacing single letter 'o' from cipher text with English letter 'E' as it corresponded with the cipher text with highest the occurrence. Same for cipher text letter 'h' and 'q' with English letter 'T' and 'A' respectively.



```
[salman@etisalat-s3 Task1]$ tr 'oh' 'ET' <cipher-task1-188> PlainText.txt
[salman@etisalat-s3 Task1]$ tr 'ohq' 'ETA' <cipher-task1-188> PlainText.txt
```

The next cipher text letter that I chose is by looking at the trigram table for ‘hbo’ which had highest occurrence. Looking at the trigrams table in English language with highest occurrence which is ‘THE’, I figured that cipher text ‘b’ would be English letter ‘H’. (As I have already replaced ‘h’ with ‘T’ and ‘o’ with ‘E’, by logic ‘b’ would be ‘H’)



```
[salman@etisalat-s3 Task1]$ tr 'ohqbmw' 'ETAHBW' <cipher-task1-188> PlainText.tx
t
```

Some ciphertext word like ‘wbqh’ would be English word ‘WHAT’ as I already know ‘bqh’ would be ‘HAT’.

After replacing five ciphertext alphabets, looking at the ciphertext corpus, words start making sense and by logic I kept replacing those words letter by letter.

The entire command line screenshots are provided in the Appendices Task 1 for reference.

2.3. Letter Mapping

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

The above key was used to encrypt the ciphertext file. With the help of the same key, we have decrypted the ciphertext file.

The plaintext is provided in the Appendices Task 1 for reference.

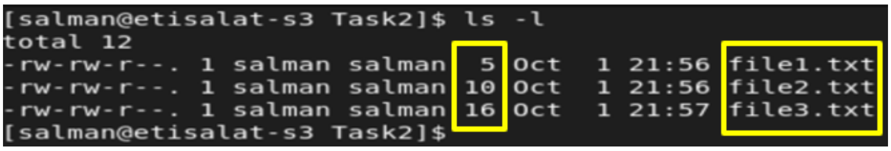
3. Task 2: Symmetric encryption: Padding

3.1. Objectives

- To understand how padding works.
- Explore how 'openssl enc' command works.
- Understand how cipher mode '-aes-128-cbc' encryption works.
- To observe padding by using hex tools such as 'xxd'.
- Observe how the file size changes with/without padding.

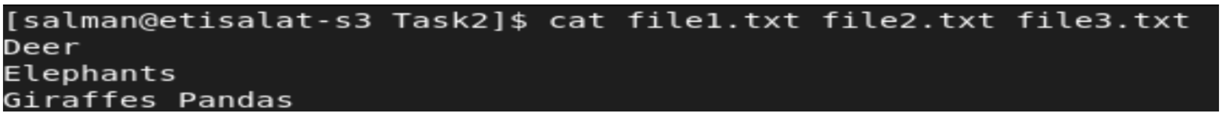
3.2. Implementation

First, I have created 3 files: file1.txt, file2.txt and file3.txt of 5,10 and 16 bytes respectively.



```
[salman@etisalat-s3 Task2]$ ls -l
total 12
-rw-rw-r--. 1 salman salman  5 Oct  1 21:56 file1.txt
-rw-rw-r--. 1 salman salman 10 Oct  1 21:56 file2.txt
-rw-rw-r--. 1 salman salman 16 Oct  1 21:57 file3.txt
[salman@etisalat-s3 Task2]$
```

Image 1: Three files of 5, 10 & 16 bytes

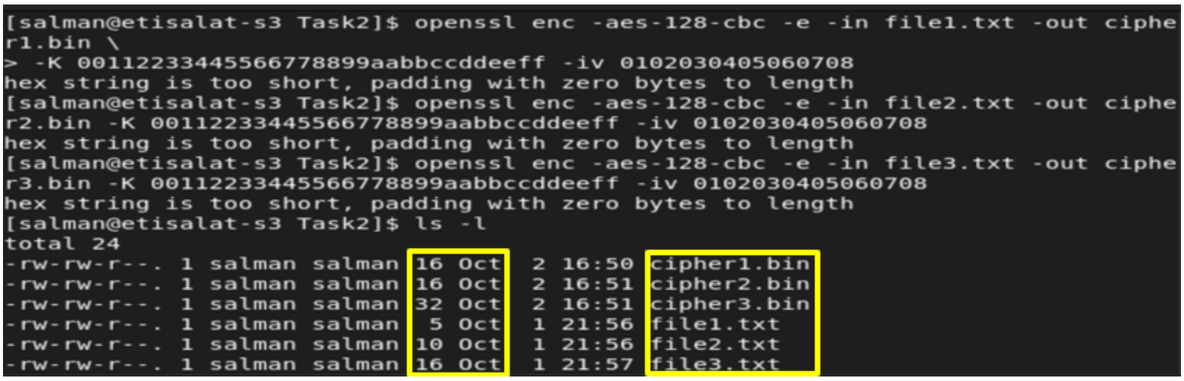


```
[salman@etisalat-s3 Task2]$ cat file1.txt file2.txt file3.txt
Deer
Elephants
Giraffes Pandas
```

Image 2: Viewing the content of the three files

Next, I encrypted all the three files. The cipher mode used is '-aes-128-cbc' which is 128-bit encryption. Padding is automatically added after encryption to each file. The amount of padding added to each file varies as each file is of different size. After encryption, file1.txt will be cipher1.bin. Similarly, file2.txt and file3.txt will be cipher2.bin and cipher3.bin respectively.

As we use 128-bit encryption (16 bytes), cipher1.bin and cipher2.bin will be rounded off to 16 bytes and cipher2.bin will be rounded off to the next multiple of 16 (i.e., 32 bytes) after padding.

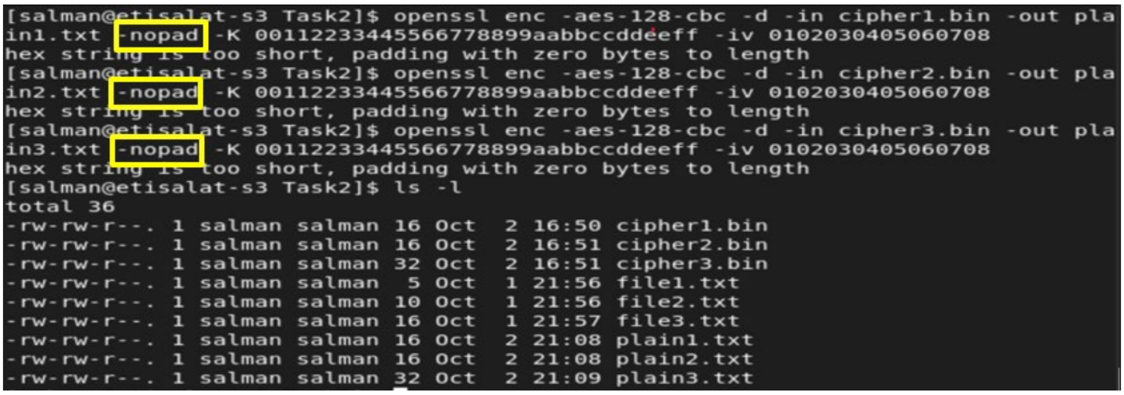


```
[salman@etisalat-s3 Task2]$ openssl enc -aes-128-cbc -e -in file1.txt -out ciphe
r1.bin \
> -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task2]$ openssl enc -aes-128-cbc -e -in file2.txt -out ciphe
r2.bin -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task2]$ openssl enc -aes-128-cbc -e -in file3.txt -out ciphe
r3.bin -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task2]$ ls -l
total 24
-rw-rw-r--. 1 salman salman 16 Oct  2 16:50 cipher1.bin
-rw-rw-r--. 1 salman salman 16 Oct  2 16:51 cipher2.bin
-rw-rw-r--. 1 salman salman 32 Oct  2 16:51 cipher3.bin
-rw-rw-r--. 1 salman salman  5 Oct  1 21:56 file1.txt
-rw-rw-r--. 1 salman salman 10 Oct  1 21:56 file2.txt
-rw-rw-r--. 1 salman salman 16 Oct  1 21:57 file3.txt
```

Image 3: Encrypting the three files

Next step is to decrypt the cipher files but using the ‘-nopad’ command while using the ‘openssl enc’ command to retain the padding. If we don’t use the ‘-nopad’ command, the padding is automatically removed while decrypting.

After decryption, we get three plaintext files: plain1.txt, plain2.txt and plain3.txt.

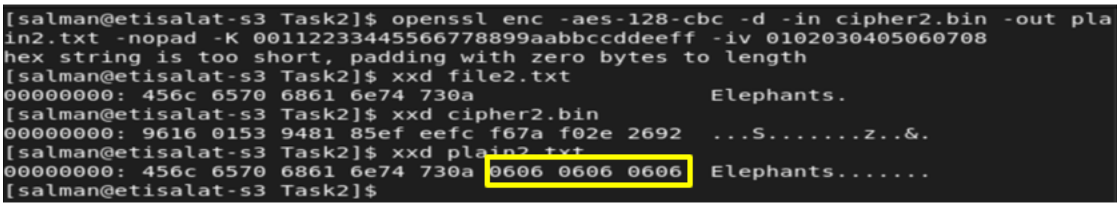


```
[salman@etisalat-s3 Task2]$ openssl enc -aes-128-cbc -d -in cipher1.bin -out pla
in1.txt -nopad -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task2]$ openssl enc -aes-128-cbc -d -in cipher2.bin -out pla
in2.txt -nopad -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task2]$ openssl enc -aes-128-cbc -d -in cipher3.bin -out pla
in3.txt -nopad -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task2]$ ls -l
total 36
-rw-rw-r--. 1 salman salman 16 Oct  2 16:50 cipher1.bin
-rw-rw-r--. 1 salman salman 16 Oct  2 16:51 cipher2.bin
-rw-rw-r--. 1 salman salman 32 Oct  2 16:51 cipher3.bin
-rw-rw-r--. 1 salman salman  5 Oct  1 21:56 file1.txt
-rw-rw-r--. 1 salman salman 10 Oct  1 21:56 file2.txt
-rw-rw-r--. 1 salman salman 16 Oct  1 21:57 file3.txt
-rw-rw-r--. 1 salman salman 16 Oct  2 21:08 plain1.txt
-rw-rw-r--. 1 salman salman 16 Oct  2 21:08 plain2.txt
-rw-rw-r--. 1 salman salman 32 Oct  2 21:09 plain3.txt
```

Image 4: Decrypting the three files with -nopad command to observe padding

We observe that the size of the plain text files is same as that of the cipher text files. This confirms that the padding is retained for all the files.

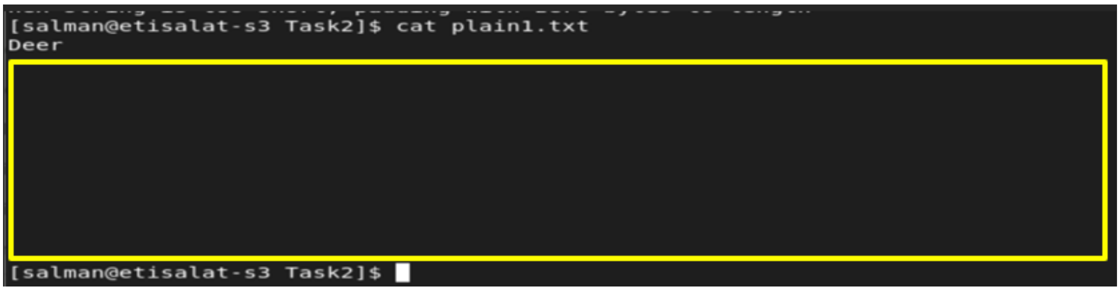
Next step is to observe padding. I use the ‘xxd’ command to observe padding. It will display the content of the file in a series of hexadecimal numbers.



```
[salman@etisalat-s3 Task2]$ openssl enc -aes-128-cbc -d -in cipher2.bin -out pla
in2.txt -nopad -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task2]$ xxd file2.txt
00000000: 456c 6570 6861 6e74 730a                Elephants.
[salman@etisalat-s3 Task2]$ xxd cipher2.bin
00000000: 9616 0153 9481 85ef eefc f67a f02e 2692  ...S.......z..&.
[salman@etisalat-s3 Task2]$ xxd plain2.txt
00000000: 456c 6570 6861 6e74 730a 0606 0606 0606  Elephants.......
[salman@etisalat-s3 Task2]$
```

Image 5: Padding bytes observed using ‘xxd’ command

We can observe in the image above that after decryption, the plaintext is visible along with some padding. We can also use the ‘cat’ command to observe the blank space, after decryption if ‘-nopad’ command is used.



```
[salman@etisalat-s3 Task2]$ cat plain1.txt
Deer








[salman@etisalat-s3 Task2]$
```

Image 6: Padding observed when viewing the file content using cat command

More screenshots are added for reference in Appendices Task 2.

4. Task 3: Encryption Mode — Corrupted Cipher Text

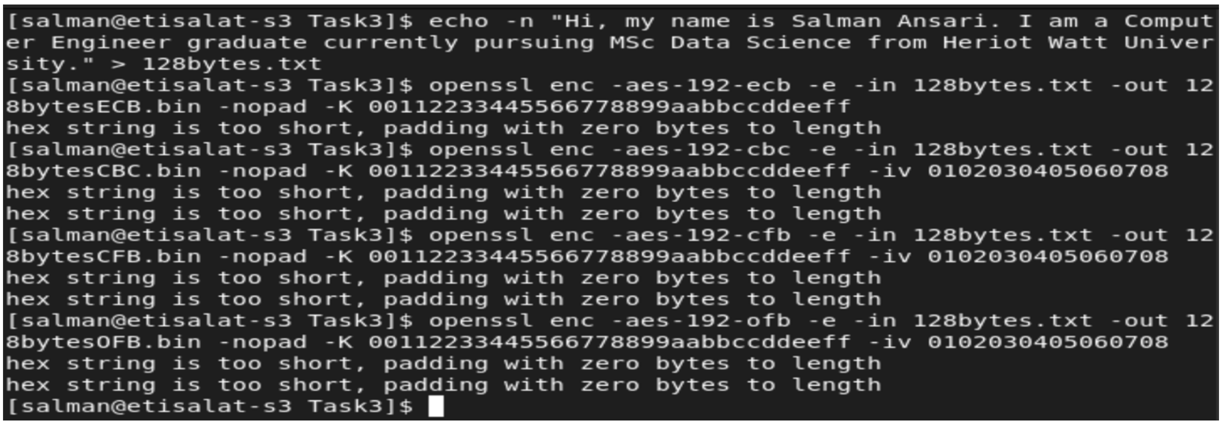
4.1. Objectives

- To understand various encryption modes like ECB, CBC, CFB, and OFB.
- To observe how a file would appear if the file was corrupted.
- Use the ‘aes-192’ encryption mode throughout.

4.2. Implementation

First, I created a file that is 128 bytes long using the ‘echo’ command provided in the coursework sheet. After creating the file, I encrypted the file four times using ECB, CBC, CFB, and OFB modes. I have used the ‘-nopad’ command while encrypting.

While encrypting with ECB mode, -iv (initialization vector) is not required.



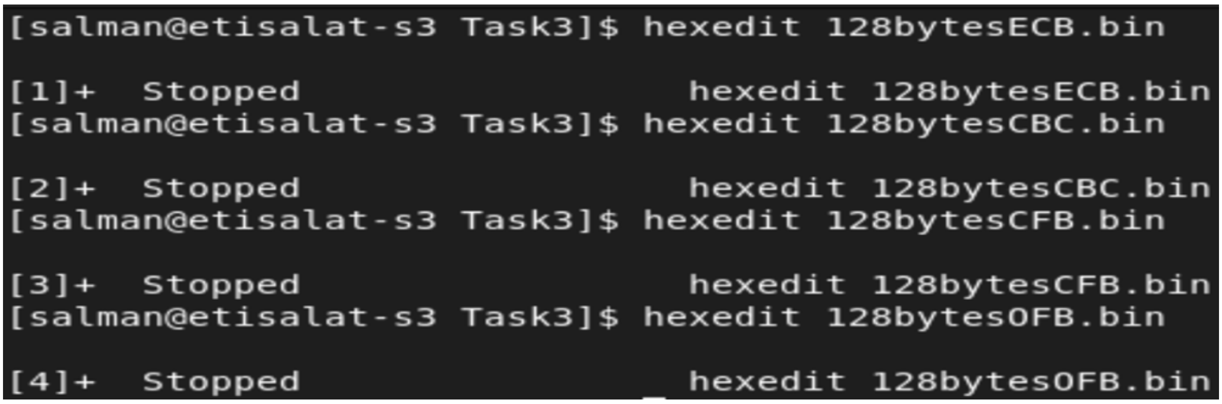
```
[salman@etisalat-s3 Task3]$ echo -n "Hi, my name is Salman Ansari. I am a Comput
er Engineer graduate currently pursuing MSc Data Science from Heriot Watt Univer
sity." > 128bytes.txt
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-ecb -e -in 128bytes.txt -out 12
8bytesECB.bin -nopad -K 00112233445566778899aabbccddeeff
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-cbc -e -in 128bytes.txt -out 12
8bytesCBC.bin -nopad -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-cfb -e -in 128bytes.txt -out 12
8bytesCFB.bin -nopad -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-ofb -e -in 128bytes.txt -out 12
8bytesOFB.bin -nopad -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task3]$ 
```

Image 7: Creating 128 bytes file and encrypting with four different cipher modes

Now, after encryption, the next step is to induce errors. We are supposed to modify a single bit of 46th byte of each ciphertext file (given). So, we use the ‘hexedit’ command to edit the byte value. I have used the ‘*yum install hexedit’* command from https://centos.pkgs.org/7/centos-x86_64/hexedit-1.2.13-5.el7.x86_64.rpm.html website.

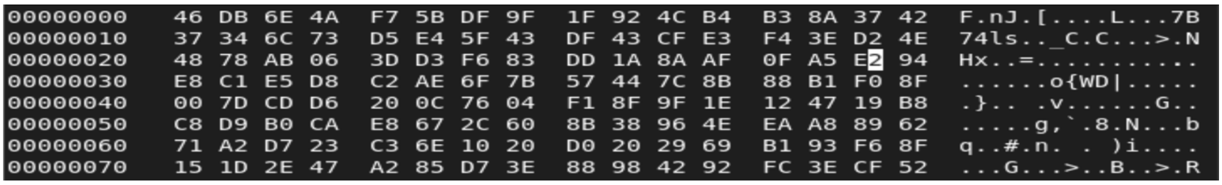
Hexedit tool allows to edit the byte value and save the changes.

We must also remove the 86th byte from each ciphertext file (given). So, I have replaced the 86th byte of each ciphertext file with 00.



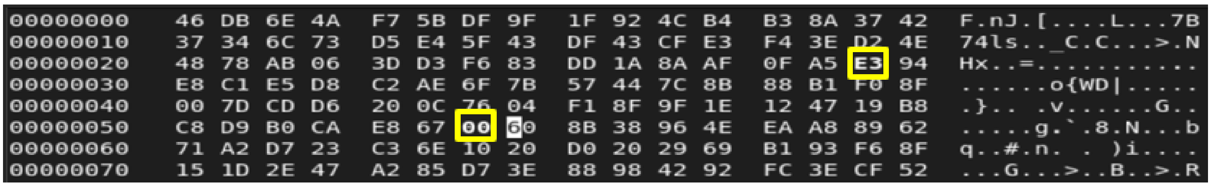
```
[salman@etisalat-s3 Task3]$ hexedit 128bytesECB.bin

[1]+  Stopped                 hexedit 128bytesECB.bin
[salman@etisalat-s3 Task3]$ hexedit 128bytesCBC.bin

[2]+  Stopped                 hexedit 128bytesCBC.bin
[salman@etisalat-s3 Task3]$ hexedit 128bytesCFB.bin

[3]+  Stopped                 hexedit 128bytesCFB.bin
[salman@etisalat-s3 Task3]$ hexedit 128bytesOFB.bin

[4]+  Stopped                 hexedit 128bytesOFB.bin
```

Image 8: hexedit command



```
00000000   46 DB 6E 4A  F7 5B DF 9F  1F 92 4C B4  B3 8A 37 42  F.nJ.[....L...7B
00000010   37 34 6C 73  D5 E4 5F 43  DF 43 CF E3  F4 3E D2 4E  74ls.._C.C...>.N
00000020   48 78 AB 06  3D D3 F6 83  DD 1A 8A AF  0F A5 E2 94  Hx..=...........
00000030   E8 C1 E5 D8  C2 AE 6F 7B  57 44 7C 8B  88 B1 F0 8F  ......o{WD|.....
00000040   00 7D CD D6  20 0C 76 04  F1 8F 9F 1E  12 47 19 B8  .}.. .v......G..
00000050   C8 D9 B0 CA  E8 67 2C 60  8B 38 96 4E  EA A8 89 62  .....g,`.8.N...b
00000060   71 A2 D7 23  C3 6E 10 20  D0 20 29 69  B1 93 F6 8F  q..#.n. . )i....
00000070   15 1D 2E 47  A2 85 D7 3E  88 98 42 92  FC 3E CF 52  ...G...>..B..>.R
```

Image 9: CBC encryption before modifying the 46th and 86th byte

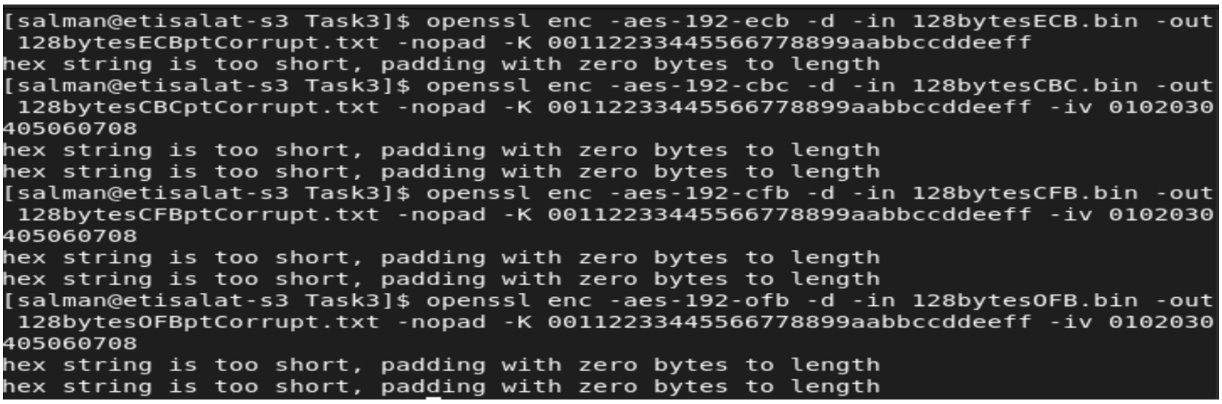


```
00000000   46 DB 6E 4A  F7 5B DF 9F  1F 92 4C B4  B3 8A 37 42  F.nJ.[....L...7B
00000010   37 34 6C 73  D5 E4 5F 43  DF 43 CF E3  F4 3E D2 4E  74ls.._C.C...>.N
00000020   48 78 AB 06  3D D3 F6 83  DD 1A 8A AF  0F A5 E3 94  Hx..=...........
00000030   E8 C1 E5 D8  C2 AE 6F 7B  57 44 7C 8B  88 B1 F0 8F  ......o{WD|.....
00000040   00 7D CD D6  20 0C 76 04  F1 8F 9F 1E  12 47 19 B8  .}.. .v......G..
00000050   C8 D9 B0 CA  E8 67 00 60  8B 38 96 4E  EA A8 89 62  .....g.`.8.N...b
00000060   71 A2 D7 23  C3 6E 10 20  D0 20 29 69  B1 93 F6 8F  q..#.n. . )i....
00000070   15 1D 2E 47  A2 85 D7 3E  88 98 42 92  FC 3E CF 52  ...G...>..B..>.R
```

Image 10: CBC encryption after modifying the 46th and 86th byte

The same changes are made for the other three ciphertext files. The images for those are added in the Appendices Task 3.

The next step is decrypting the corrupted ciphertext files. I have included the '-nopad' command while decrypting, keeping the key and iv same.



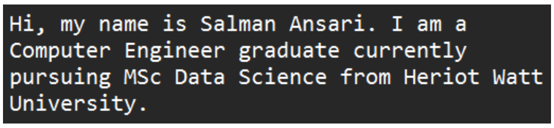
```
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-ecb -d -in 128bytesECB.bin -out
 128bytesECBptCorrupt.txt -nopad -K 00112233445566778899aabbccddeeff
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-cbc -d -in 128bytesCBC.bin -out
 128bytesCBCptCorrupt.txt -nopad -K 00112233445566778899aabbccddeeff -iv 0102030
405060708
hex string is too short, padding with zero bytes to length
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-cfb -d -in 128bytesCFB.bin -out
 128bytesCFBptCorrupt.txt -nopad -K 00112233445566778899aabbccddeeff -iv 0102030
405060708
hex string is too short, padding with zero bytes to length
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-ofb -d -in 128bytesOFB.bin -out
 128bytesOFBptCorrupt.txt -nopad -K 00112233445566778899aabbccddeeff -iv 0102030
405060708
hex string is too short, padding with zero bytes to length
hex string is too short, padding with zero bytes to length
```

Image 11: Decrypting the corrupted ciphertext files

4.3. Observations

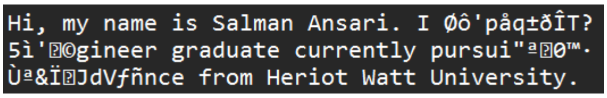
ECB mode of encryption

- In ECB mode on encryption, a plaintext block is encrypted independently. There is no link between adjacent blocks. So, each block is enciphered independently and as there is no link between the blocks, the block that has been corrupted will not be recoverable.



```
Hi, my name is Salman Ansari. I am a
Computer Engineer graduate currently
pursuing MSc Data Science from Heriot Watt
University.
```

Image 12: Plaintext

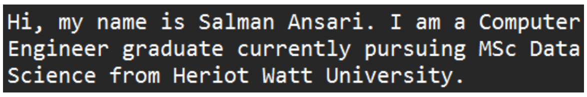


```
Hi, my name is Salman Ansari. I Øô'påq±ðÎT?
5ì'⍰©gineer graduate currently pursui"ª⍰0™·
Ùª&Ï⍰JdVƒñnce from Heriot Watt University.
```

Image 13: Corrupted Plaintext (ECB)

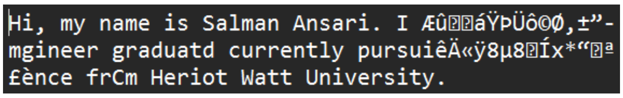
CBC mode of encryption

- CBC mode is an advancement to ECB mode of encryption. In CBC, the encryption algorithm uses the previous cipher block as input. XOR operation is done between the previous cipher block and current plaintext, thus producing the cipher block and so on.



```
Hi, my name is Salman Ansari. I am a Computer
Engineer graduate currently pursuing MSc Data
Science from Heriot Watt University.
```

Image 14: Plaintext

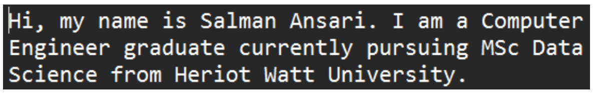


```
Hi, my name is Salman Ansari. I ÆûàáŸÞÜô©Ø,±”-
mgineer graduatd currently pursuiêÄ«ÿ8µ8⍰Íx*“⍰ª
£ènce frCm Heriot Watt University.
```

Image 15: Corrupted Plaintext (CBC)

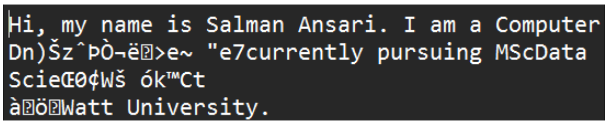
CFB mode of encryption

- CFB mode of encryption is like CBC mode of encryption. Here, any block is affected by the previously corrupted ciphertext block. It means that any block after the corrupted ciphertext block will become unrecoverable.



```
Hi, my name is Salman Ansari. I am a Computer
Engineer graduate currently pursuing MSc Data
Science from Heriot Watt University.
```

Image 16: Plaintext

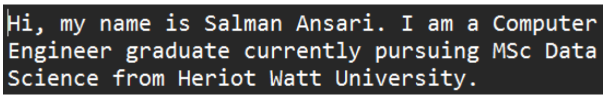


```
Hi, my name is Salman Ansari. I am a Computer
Dn)ŠzˆÞÒ¬ë⍰>e~ "e7currently pursuing MScData
ScieŒ0¢Wš ók™Ct
à⍰ö⍰Watt University.
```

Image 17: Corrupted Plaintext (CFB)

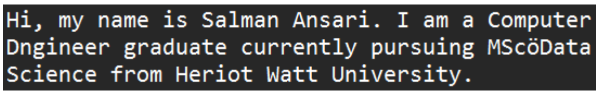
OFB mode of encryption

- In this type of encryption mode, the encryption is applied to the vector and not the plaintext itself. It means that only one bit change will affect only one vector which will in turn, only affect one bit after decryption.



```
Hi, my name is Salman Ansari. I am a Computer
Engineer graduate currently pursuing MSc Data
Science from Heriot Watt University.
```

Image 18: Plaintext



```
Hi, my name is Salman Ansari. I am a Computer
Dngineer graduate currently pursuing MScöData
Science from Heriot Watt University.
```

Image 19: Corrupted Plaintext (OFB)

5. Task 4: Encryption Mode — Corrupted Cipher Text

5.1. Objectives

- To create a shell script to match the password and the plaintext.
- Observe the change in plaintext with/without padding.
- To match the word in plaintext file with the dictionary file.

5.2. Implementation

We are given a linecount.sh file for reference. First, we create a plaintext file containing a word from the dictionary. Then we encrypt the file using openssl command (openssl enc -aes-128-cbc -e -in plain.txt -out cipher.txt -pass pass:apple1). We append a digit at the end of the password.

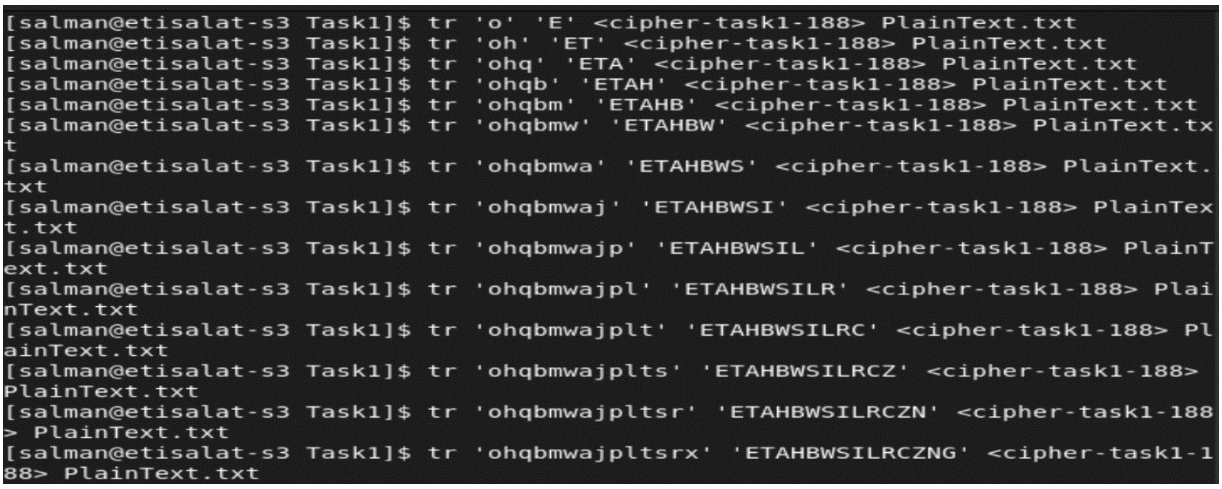
Then I created a while loop which will iterate line by line from the dictionary. Inside the while loop, I encrypted the plaintext file with a password that is taken while iterating from the dictionary.

Then I compare my initial ciphertext file which I encrypted using the openssl command with the ciphertext file that I get while encrypting with a password taken from the dictionary inside the while loop.

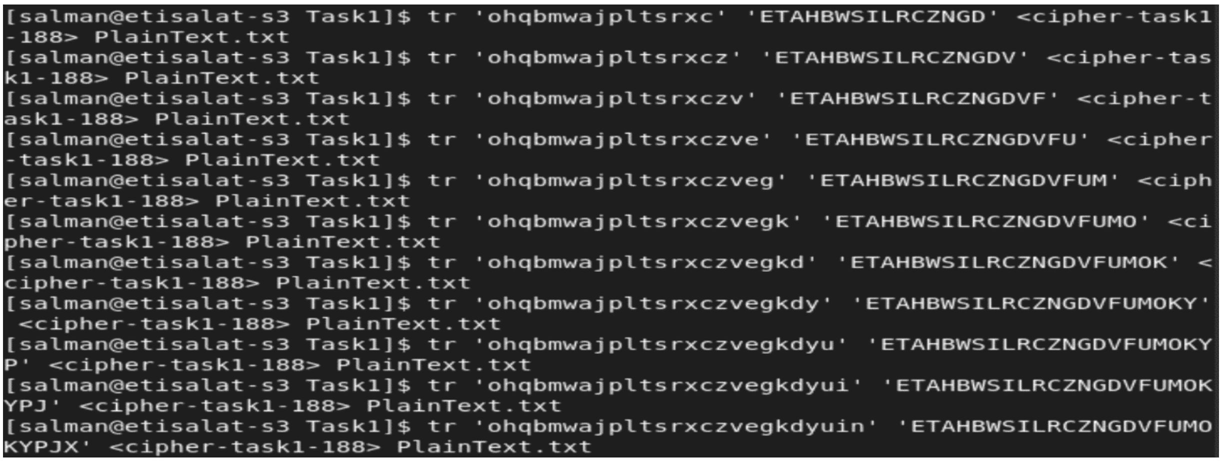
If it matches the word inside the dictionary, it will print the word is found and break the loop. Otherwise, it will keep on checking until the end of line in dictionary.

6. Appendices Task 1

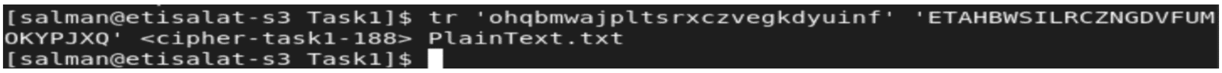
Command Line Screenshots



```
[salman@etisalat-s3 Task1]$ tr 'o' 'E' <cipher-task1-188> PlainText.txt
[salman@etisalat-s3 Task1]$ tr 'oh' 'ET' <cipher-task1-188> PlainText.txt
[salman@etisalat-s3 Task1]$ tr 'ohq' 'ETA' <cipher-task1-188> PlainText.txt
[salman@etisalat-s3 Task1]$ tr 'ohqb' 'ETAH' <cipher-task1-188> PlainText.txt
[salman@etisalat-s3 Task1]$ tr 'ohqbm' 'ETAHB' <cipher-task1-188> PlainText.txt
[salman@etisalat-s3 Task1]$ tr 'ohqbmw' 'ETAHBW' <cipher-task1-188> PlainText.tx
t
[salman@etisalat-s3 Task1]$ tr 'ohqbmwa' 'ETAHBWS' <cipher-task1-188> PlainText.
txt
[salman@etisalat-s3 Task1]$ tr 'ohqbmwaj' 'ETAHBWSI' <cipher-task1-188> PlainTex
t.txt
[salman@etisalat-s3 Task1]$ tr 'ohqbmwajp' 'ETAHBWSIL' <cipher-task1-188> PlainT
ext.txt
[salman@etisalat-s3 Task1]$ tr 'ohqbmwajpl' 'ETAHBWSILR' <cipher-task1-188> Plai
nText.txt
[salman@etisalat-s3 Task1]$ tr 'ohqbmwajplt' 'ETAHBWSILRC' <cipher-task1-188> Pl
ainText.txt
[salman@etisalat-s3 Task1]$ tr 'ohqbmwajplts' 'ETAHBWSILRCZ' <cipher-task1-188>
PlainText.txt
[salman@etisalat-s3 Task1]$ tr 'ohqbmwajpltsr' 'ETAHBWSILRCZN' <cipher-task1-188
> PlainText.txt
[salman@etisalat-s3 Task1]$ tr 'ohqbmwajpltsrx' 'ETAHBWSILRCZNG' <cipher-task1-1
88> PlainText.txt
```



```
[salman@etisalat-s3 Task1]$ tr 'ohqbmwajpltsrxc' 'ETAHBWSILRCZNGD' <cipher-task1
-188> PlainText.txt
[salman@etisalat-s3 Task1]$ tr 'ohqbmwajpltsrxcz' 'ETAHBWSILRCZNGDV' <cipher-tas
k1-188> PlainText.txt
[salman@etisalat-s3 Task1]$ tr 'ohqbmwajpltsrxczv' 'ETAHBWSILRCZNGDVF' <cipher-t
ask1-188> PlainText.txt
[salman@etisalat-s3 Task1]$ tr 'ohqbmwajpltsrxczve' 'ETAHBWSILRCZNGDVFU' <cipher
-task1-188> PlainText.txt
[salman@etisalat-s3 Task1]$ tr 'ohqbmwajpltsrxczveg' 'ETAHBWSILRCZNGDVFUM' <ciph
er-task1-188> PlainText.txt
[salman@etisalat-s3 Task1]$ tr 'ohqbmwajpltsrxczvegk' 'ETAHBWSILRCZNGDVFUMO' <ci
pher-task1-188> PlainText.txt
[salman@etisalat-s3 Task1]$ tr 'ohqbmwajpltsrxczvegkd' 'ETAHBWSILRCZNGDVFUMOK' <
cipher-task1-188> PlainText.txt
[salman@etisalat-s3 Task1]$ tr 'ohqbmwajpltsrxczvegkdy' 'ETAHBWSILRCZNGDVFUMOKY'
 <cipher-task1-188> PlainText.txt
[salman@etisalat-s3 Task1]$ tr 'ohqbmwajpltsrxczvegkdyu' 'ETAHBWSILRCZNGDVFUMOKY
P' <cipher-task1-188> PlainText.txt
[salman@etisalat-s3 Task1]$ tr 'ohqbmwajpltsrxczvegkdyui' 'ETAHBWSILRCZNGDVFUMOK
YPJ' <cipher-task1-188> PlainText.txt
[salman@etisalat-s3 Task1]$ tr 'ohqbmwajpltsrxczvegkdyuin' 'ETAHBWSILRCZNGDVFUMO
KYPJX' <cipher-task1-188> PlainText.txt
```



```
[salman@etisalat-s3 Task1]$ tr 'ohqbmwajpltsrxczvegkdyuinf' 'ETAHBWSILRCZNGDVFUM
OKYPJXQ' <cipher-task1-188> PlainText.txt
[salman@etisalat-s3 Task1]$ █
```

Plaintext

GE OF

TODAY THERES ONLY ONE COUNTRY THATS NOT REACHABLE FROM YOUR TELEPHONE

ALBANIA WHAT DOES THIS MEAN FOR THE FUTURE OF ESPIONAGE

YOW WHAT AM I THINKING ABOUT IM NOT A SPY IM JUST AN ASTRONOMER WHOS BEEN

AWAY FROM SCIENCE FOR TOO LONG

AS I TURNED OFF MY MONITORS AND WOUND UP THE CABLES I REALIZED THAT FOR A

YEAR ID BEEN CAUGHT IN A MAZE ID THOUGHT ID BEEN SETTING TRAPS ACTUALLY ID

BEEN TRAPPED THE WHOLE WHILE WHILE THE HACKER WAS SEARCHING MILITARY COMPUTERS I

WAS EXPLORING DIFFERENT COMMUNITIES ON THE NETWORKS AND IN THE GOVERNMENT HIS

JOURNEY TOOK HIM INTO THIRTY OR FORTY COMPUTERS MINE REACHED INTO A DOZEN

ORGANIZATIONS

MY OWN QUEST HAD CHANGED I THOUGHT I WAS HUNTING FOR A HACKER ID IMAGINED

THAT MY WORK HAD NOTHING TO DO WITH MY HOME OR COUNTRY AFTER ALL I WAS JUST

DOING MY JOB

NOW WITH MY COMPUTERS SERVICED AND HOLES PATCHED I BIKED HOME PICKED A FEW

STRAWBERRIES AND MIXED SOME MILKSHAKES FOR MARTHA AND CLAUDIA

CUCKOOS WILL LAY THEIR EGGS IN OTHER NESTS IM RETURNING TO ASTRONOMY

PAGE OF

EPILOGUE

WHILE I WAS DESPERATELY TRYING TO WRAP UP THE HACKER CHASE WE ALSO HAD A

WEDDING TO PLAN IT WAS A HECTIC TIME AND I CURSED MY WORK AND HESS FOR

DISTRACTING ME FROM MY HOME LIFE WE WERE GOING TO BE MARRIED AT THE END OF MAY SO

THE APRIL REVELATIONS WERE PARTICULARLY AWKWARD MARTHA ENDING UP WITH MORE THAN

HER SHARE OF THE PREPARATIONS

SHE WAS COPING HOWEVER FIRMLY RESOLVED TO MAKE THE WEDDING TRUE TO WHO WE

WERE WE SILKSCREENED OUR OWN INVITATIONS SAYING THAT THE TWO OF US ALONG WITH

OUR FAMILIES WERE DOING THE INVITING NATURALLY THE INK ON THE SILKSCREEN LEAKED

THROUGH AND HALF THE INVITATIONS HAD OUR FINGERPRINTS BUT THATS A PART OF THE

HOME BREW

MARTHA DECKED OUT IN A WHITE DRESS AND VEIL AND ME IN A TUX ABSURD AND

LAURIE IN A BRIDESMAIDS OUTFIT NOBODY EVER MADE LAURIE WEAR A DRESS FOR ANY

REASON SOMEHOW WE MANAGED LAURIE WORE WHITE LINEN PANTS AND A TAILORED JACKET

MARTHA MADE A SIMPLE PALE YELLOW DRESS AND I SEWED MY OWN COTTON SHIRT TRY

SEWING YOUR OWN SHIRT SOMETIME YOULL LEARN A NEW RESPECT FOR SHIRT MAKERS

ESPECIALLY AFTER YOU SEW THE CUFFS ON BACKWARD

SO IT RAINED ON OUR WEDDING AND THERE WASNT A PLACE TO HIDE IN THE ROSE

GARDEN CLAUDIAS STRING QUARTET UNRAVELED A TARP PROTECTING THEIR VIOLINS FROM

THE DOWNPOUR MY SISTER JEANNIE SHOWED UP STRAIGHT FROM HER LAST CLARM AT NAVY WAR

COLLEGE AND STRAIGHT INTO A POLITICAL ARGUMENT WITH LAURIE OF COURSE AFTER THE

CEREMONY WE GOT LOST DRIVING TO A REMOTE INN BY THE OCEAN

IT WAS WONDERFUL ALL THE SAME SAY WHAT YOU WILL ABOUT MARRIAGE THIS WAS THE

HAPPIEST DAY OF MY LIFE

SURE I COULD HAVE JUST STAYED LIVING WITH MARTHA NEVER QUITE COMMITTING

MYSELF BEYOND NEXT MONTHS RENT ID LIVED WITH SEVERAL OTHER PEOPLE IN THIS CASUAL

WAY SAYING WE WERE IN LOVE BUT ALWAYS READY TO SPLIT IF THINGS GOT TOUGH WE

DRESSED IT UP WITH TALK ABOUT OPENNESS AND FREEDOM FROM OPPRESSIVE CONVENTIONS BUT

FOR ME IT WAS JUST AN EXCUSE THE TRUTH WAS I HAD NEVER DARED TO GIVE MYSELF FULLY

TO ANYONE COMMITTING MYSELF TO MAKE IT WORK NO MATTER WHAT BUT NOW ID FOUND

SOMEONE I LOVED AND TRUSTED ENOUGH TO GATHER MY COURAGE AND STAND BY NOT JUST FOR

NOW BUT FOREVER

BUT DOMESTIC HAPPINESS DOESNT SOLVE EVERYTHING I STILL HAD TO FIGURE OUT WHAT

TO DO NEXT WITH HESS UNMASKED I COULD RETURN TO ASTRONOMY OR AT LEAST

COMPUTING NOT QUITE TRACKING AN INTERNATIONAL SPY RING BUT THEN THERES RESEARCH

TO DO EVERYWHERE THE BEST PART IS NOT KNOWING WHERE YOUR SCIENCE WILL LEAD YOU

IT WASNT THE SAME THE COMPUTER PEOPLE FELT ID WASTED THE PAST COUPLE YEARS

RUBBING SHOULDERS WITH SPIES THE SPIES DIDNT HAVE MUCH USE FOR ME WHO NEEDS AN

ASTRONOMER AND THE ASTRONOMERS KNEW ID BEEN AWAY FROM THE FIELD FOR TWO YEARS

WHERE DO I GO FROM HERE

MARTHA HAD PARMED HER BAR EXAM AND WAS CLERKING FOR A JUDGE ACROSS THE BAY IN

SAN FRANCISCO SHE LOVED IT TAKING NOTES ON TRIALS RESEARCHING CASE LAW HELPING

TO WRITE DECISIONS A SORT OF GRAD SCHOOL FOR LAW

SHE FOUND ANOTHER CLERKSHIP IN BOSTON STARTING IN AUGUST OVER A

STRAWBERRY MILKSHAKE SHE DESCRIBED HER POSSIBILITIES

ID CLERK FOR THE CIRCUIT COURT IN BOSTON ITLL BE MORE ACADEMIC THERE NO

PAGE OF

TRIALS JUST APPEALS MIGHT BE FUN

AND THE ALTERNATIVES

WELL IM THINKING ABOUT RETURNING TO SCHOOL TO FINISH MY DEGREE IN

JURISPRUDENCE THATLL TAKE A FEW MORE YEARS ALWAYS THE ACADEMIC

WOULD I LEAVE BERKELEY TO FOLLOW HER TO MARMACHUSETTS

SIMPLE DECISION ID FOLLOW HER ANYWHERE IF SHES GOING TO BOSTON ID DREDGE

UP A JOB THERE FORTUNATELY THE HARVARD SMITHSONIAN CENTER FOR ASTROPHYSICS WAS

LOOKING FOR A HALFBREED ASTRONOMERCOMPUTER JOCKEY SOMEONE TO PLAY WITH THEIR X

RAY ASTRONOMY DATABASE

I CAN MESS UP A DATABASE AS WELL AS THE NEXT PERSON AND THEY DIDNT MIND MY

HIATUS FROM ASTRONOMY AND BEING ASTRONOMERS THEY WERE ALREADY ACCUSTOMED TO

PEOPLE SHOWING UP LATE AND SLEEPING UNDER DESKS

IT WASNT EASY TO LEAVE BERKELEY THE STRAWBERRIES THE STREET VENDORS THE

SUNSHINE BUT WE SIGNED A NONAGGRESSION PACT WITH OUR ROOMMATES WE COULD VISIT

ANYTIME AND WOULDNT HAVE TO WASH THE DISHES IN RETURN THEY COULD STAY AT OUR

PLACE IN MARMACHUSETTS SO LONG AS THEY BROUGHT SOME CALIFORNIA KIWI FRUIT

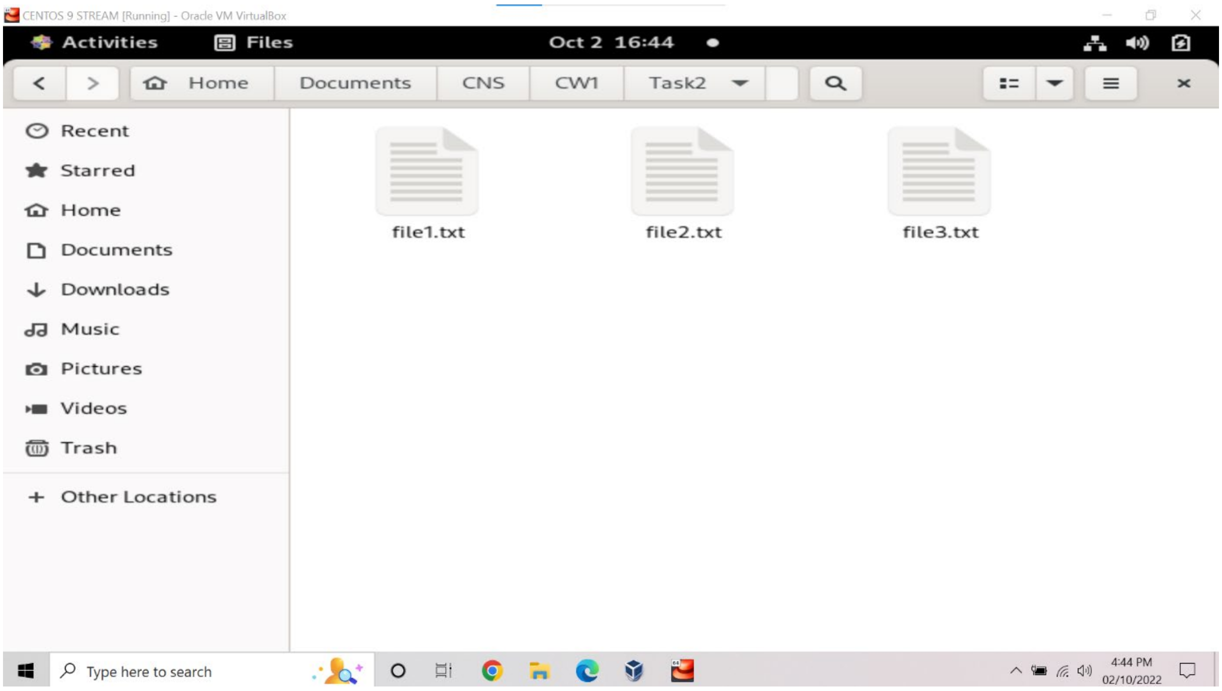
THE HARDEST PART WAS LEAVING OUR ROOMMATE CLAUDIA ID GROWN ACCUSTOMED TO HER

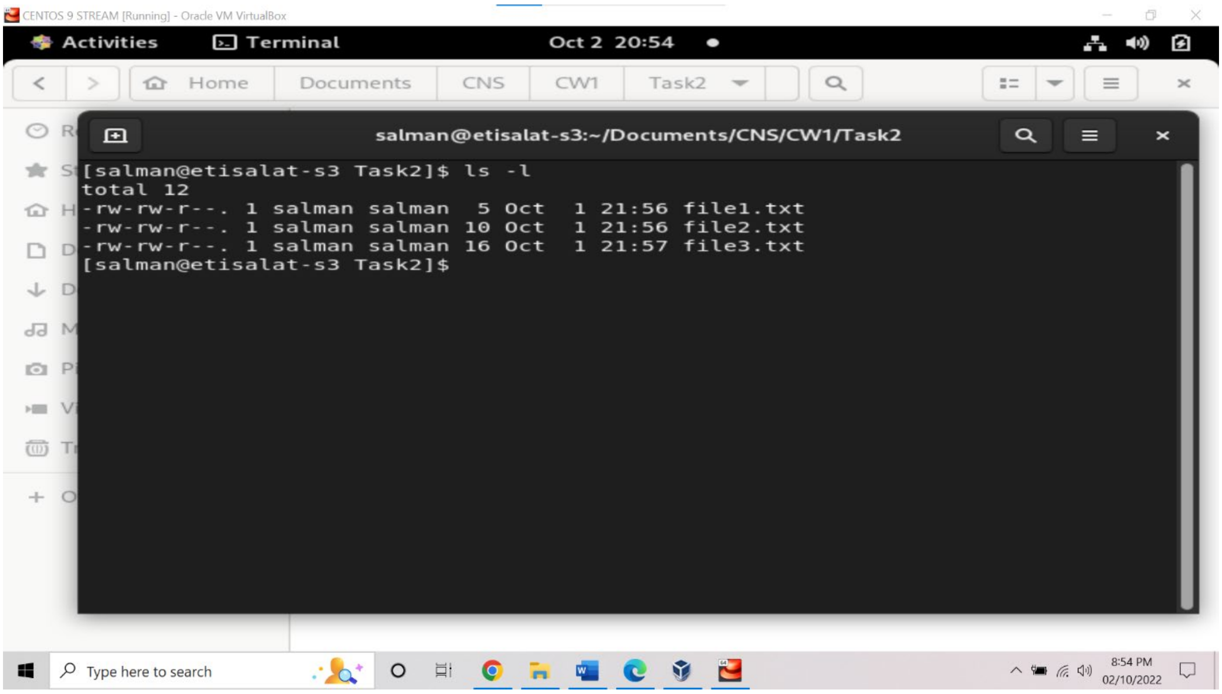
LATENIGHT MOZART PRACTICING A LONG WAY FROM THE BERKELEY GRATEFUL DEAD

CONCERTS

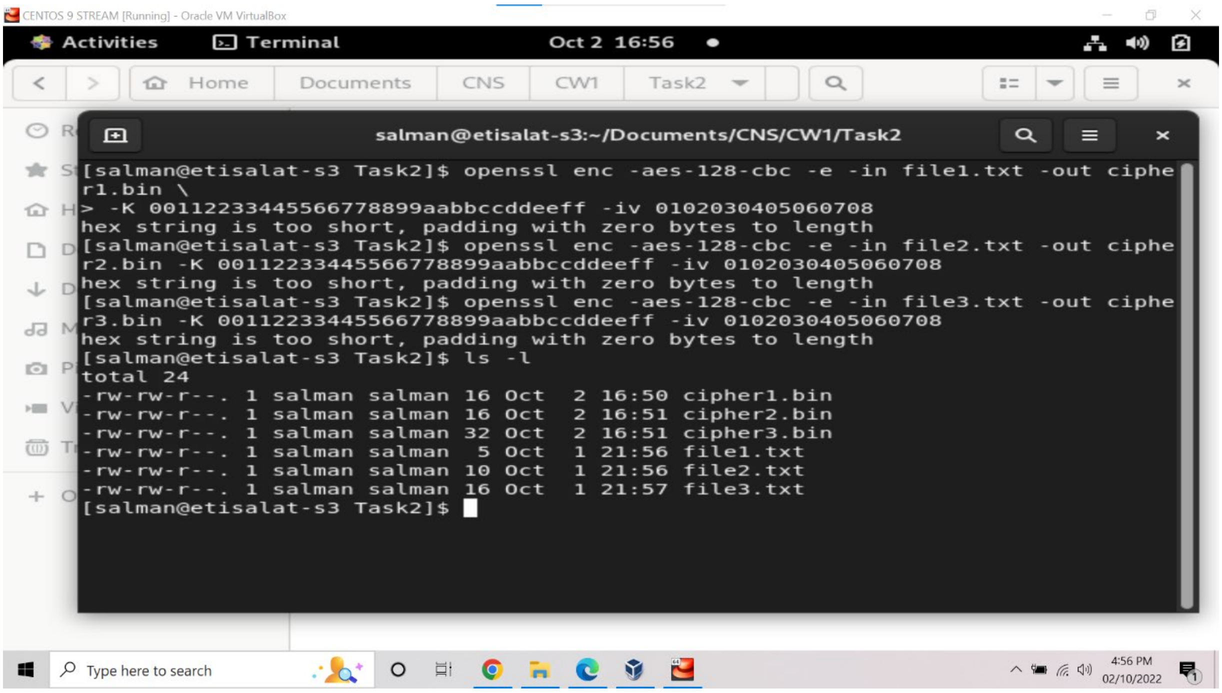
7. Appendices Task 2

Screenshots

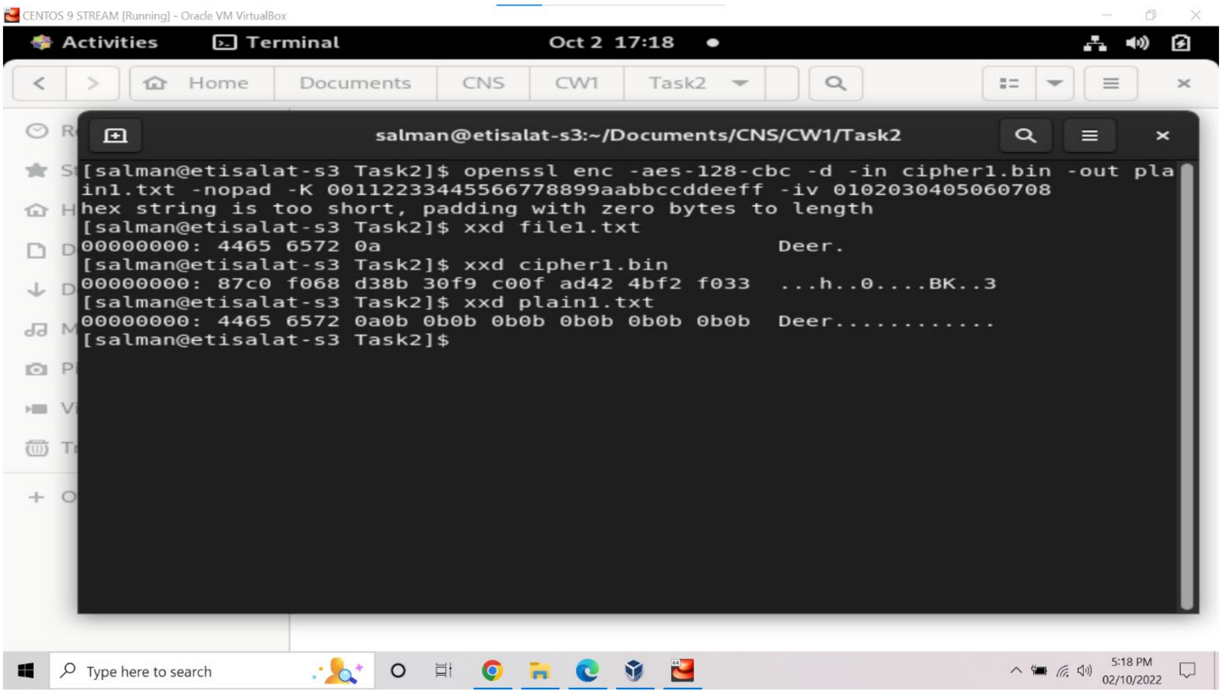



CENTOS 9 STREAM [Running] - Oracle VM VirtualBox
Activities
Terminal
Oct 2 20:54
Home
Documents
CNS
CW1
Task2
salman@etisalat-s3:~/Documents/CNS/CW1/Task2
Type here to search
8:54 PM
02/10/2022

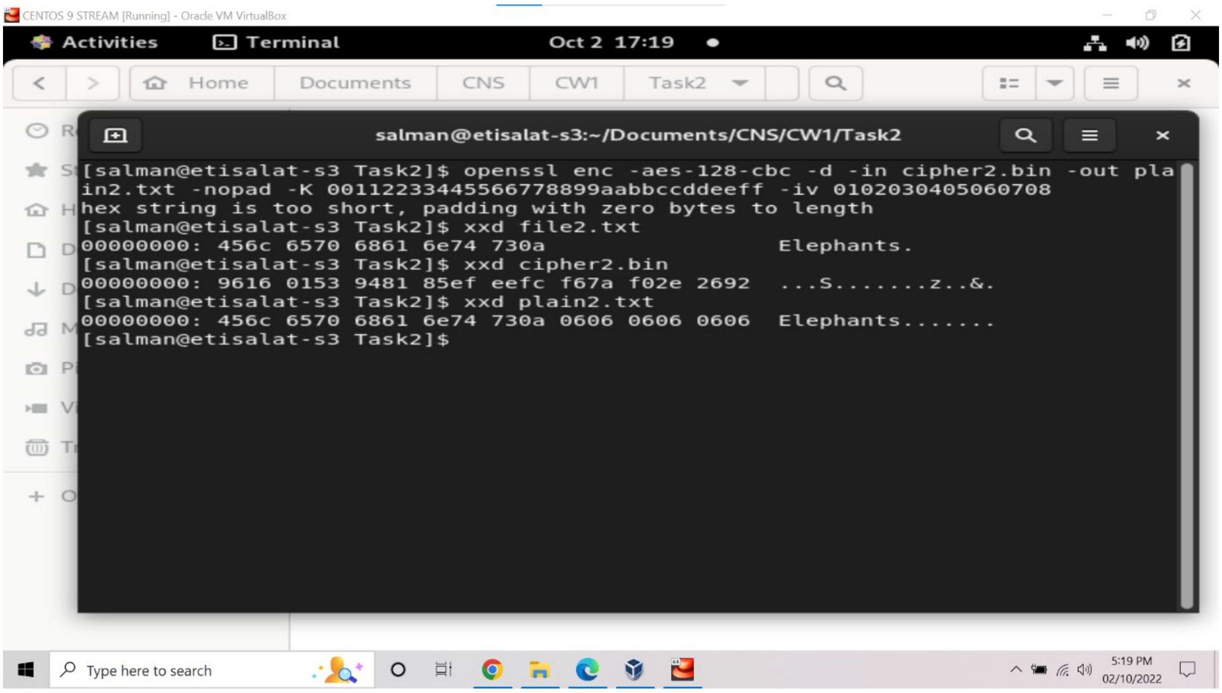
```
[salman@etisalat-s3 Task2]$ ls -l
total 12
-rw-rw-r--. 1 salman salman  5 Oct  1 21:56 file1.txt
-rw-rw-r--. 1 salman salman 10 Oct  1 21:56 file2.txt
-rw-rw-r--. 1 salman salman 16 Oct  1 21:57 file3.txt
[salman@etisalat-s3 Task2]$
```


CENTOS 9 STREAM [Running] - Oracle VM VirtualBox
Activities
Terminal
Oct 2 16:56
Home
Documents
CNS
CW1
Task2
salman@etisalat-s3:~/Documents/CNS/CW1/Task2
Type here to search
4:56 PM
02/10/2022

```
[salman@etisalat-s3 Task2]$ openssl enc -aes-128-cbc -e -in file1.txt -out ciphe
r1.bin \
> -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task2]$ openssl enc -aes-128-cbc -e -in file2.txt -out ciphe
r2.bin -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task2]$ openssl enc -aes-128-cbc -e -in file3.txt -out ciphe
r3.bin -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task2]$ ls -l
total 24
-rw-rw-r--. 1 salman salman 16 Oct  2 16:50 cipher1.bin
-rw-rw-r--. 1 salman salman 16 Oct  2 16:51 cipher2.bin
-rw-rw-r--. 1 salman salman 32 Oct  2 16:51 cipher3.bin
-rw-rw-r--. 1 salman salman  5 Oct  1 21:56 file1.txt
-rw-rw-r--. 1 salman salman 10 Oct  1 21:56 file2.txt
-rw-rw-r--. 1 salman salman 16 Oct  1 21:57 file3.txt
[salman@etisalat-s3 Task2]$ 
```

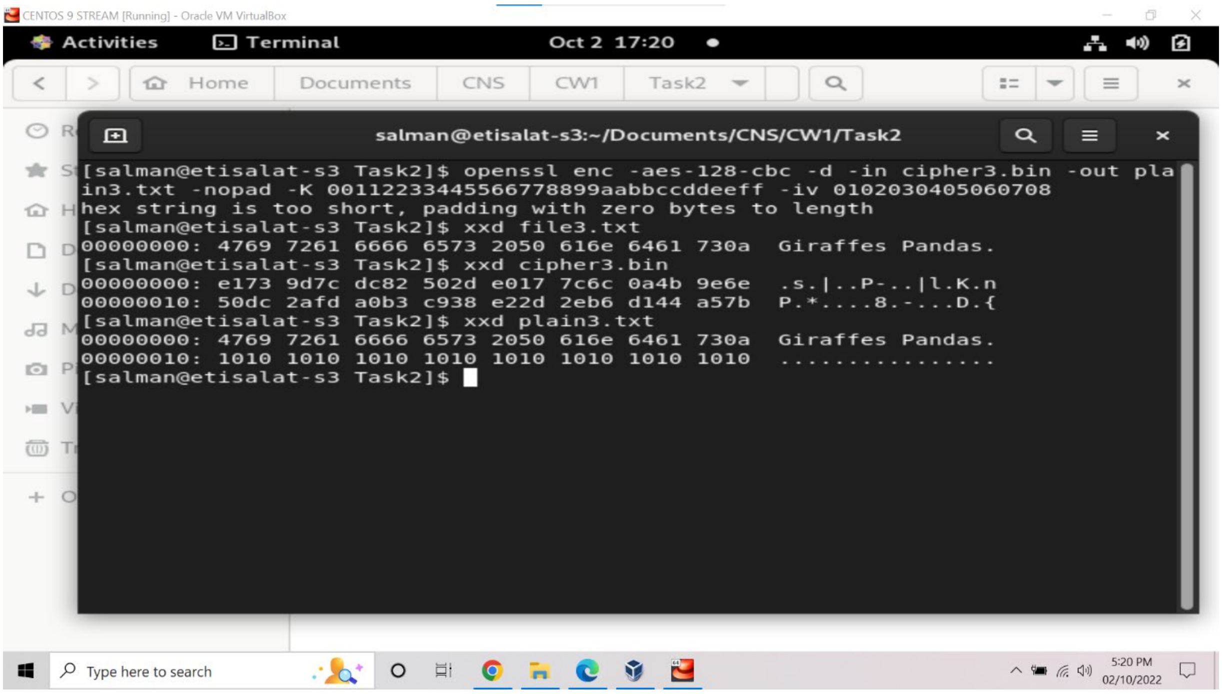

CENTOS 9 STREAM [Running] - Oracle VM VirtualBox
Activities
Terminal
Oct 2 17:18
Home
Documents
CNS
CW1
Task2
salman@etisalat-s3:~/Documents/CNS/CW1/Task2
Type here to search
5:18 PM
02/10/2022

```
[salman@etisalat-s3 Task2]$ openssl enc -aes-128-cbc -d -in cipher1.bin -out pla
in1.txt -nopad -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task2]$ xxd file1.txt
00000000: 4465 6572 0a                             Deer.
[salman@etisalat-s3 Task2]$ xxd cipher1.bin
00000000: 87c0 f068 d38b 30f9 c00f ad42 4bf2 f033  ...h..0....BK..3
[salman@etisalat-s3 Task2]$ xxd plain1.txt
00000000: 4465 6572 0a0b 0b0b 0b0b 0b0b 0b0b 0b0b  Deer............
[salman@etisalat-s3 Task2]$
```



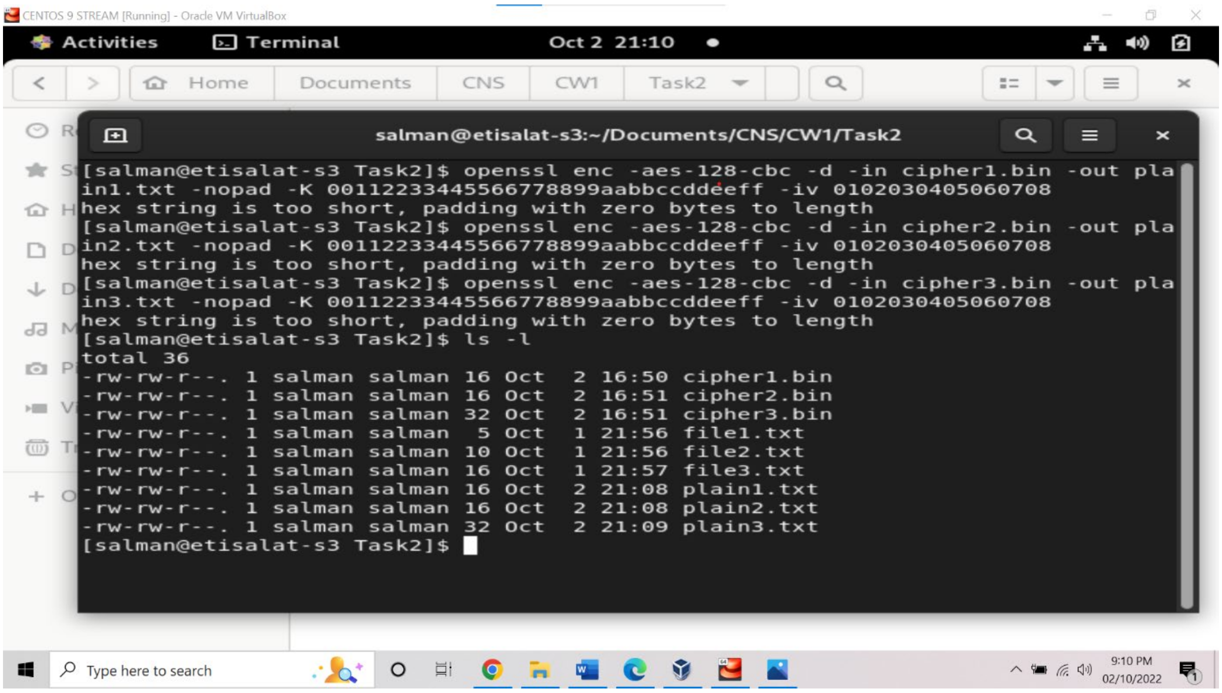
CENTOS 9 STREAM [Running] - Oracle VM VirtualBox
Activities
Terminal
Oct 2 17:19
Home
Documents
CNS
CW1
Task2
salman@etisalat-s3:~/Documents/CNS/CW1/Task2
Type here to search
5:19 PM
02/10/2022

```
[salman@etisalat-s3 Task2]$ openssl enc -aes-128-cbc -d -in cipher2.bin -out pla
in2.txt -nopad -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task2]$ xxd file2.txt
00000000: 456c 6570 6861 6e74 730a                 Elephants.
[salman@etisalat-s3 Task2]$ xxd cipher2.bin
00000000: 9616 0153 9481 85ef eefc f67a f02e 2692  ...S.......z..&.
[salman@etisalat-s3 Task2]$ xxd plain2.txt
00000000: 456c 6570 6861 6e74 730a 0606 0606 0606  Elephants.......
[salman@etisalat-s3 Task2]$
```

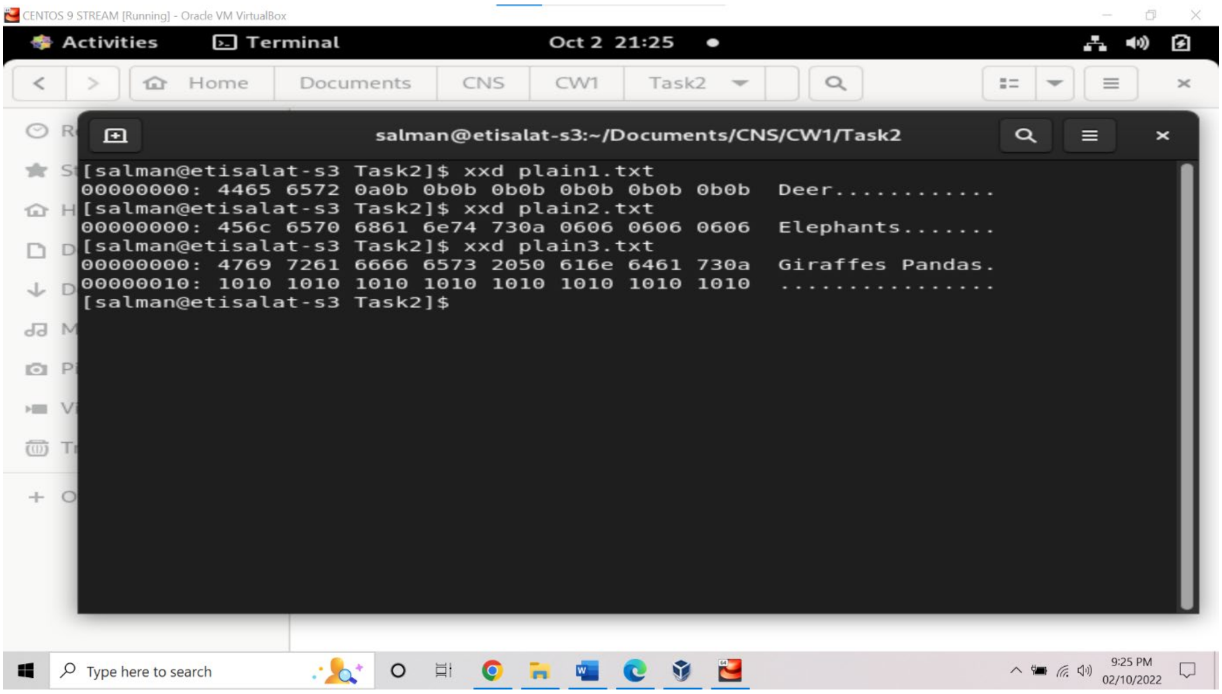


CENTOS 9 STREAM [Running] - Oracle VM VirtualBox
Activities
Terminal
Oct 2 17:20
Home
Documents
CNS
CW1
Task2
salman@etisalat-s3:~/Documents/CNS/CW1/Task2
Type here to search
5:20 PM
02/10/2022

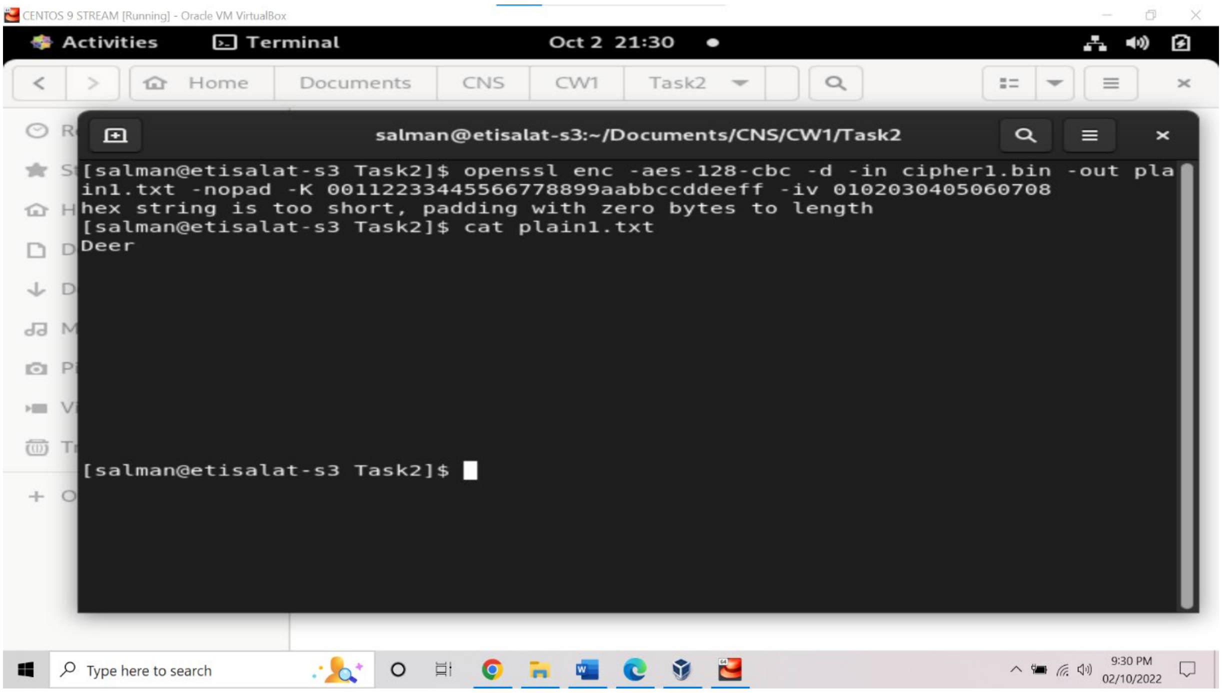
```
[salman@etisalat-s3 Task2]$ openssl enc -aes-128-cbc -d -in cipher3.bin -out pla
in3.txt -nopad -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task2]$ xxd file3.txt
00000000: 4769 7261 6666 6573 2050 616e 6461 730a  Giraffes Pandas.
[salman@etisalat-s3 Task2]$ xxd cipher3.bin
00000000: e173 9d7c dc82 502d e017 7c6c 0a4b 9e6e  .s.|..P-..|l.K.n
00000010: 50dc 2afd a0b3 c938 e22d 2eb6 d144 a57b  P.*....8.-...D.{
[salman@etisalat-s3 Task2]$ xxd plain3.txt
00000000: 4769 7261 6666 6573 2050 616e 6461 730a  Giraffes Pandas.
00000010: 1010 1010 1010 1010 1010 1010 1010 1010  ................
[salman@etisalat-s3 Task2]$
```


CENTOS 9 STREAM [Running] - Oracle VM VirtualBox
Activities
Terminal
Oct 2 21:10
Home
Documents
CNS
CW1
Task2
salman@etisalat-s3:~/Documents/CNS/CW1/Task2
Type here to search
9:10 PM
02/10/2022

```
[salman@etisalat-s3 Task2]$ openssl enc -aes-128-cbc -d -in cipher1.bin -out pla
in1.txt -nopad -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task2]$ openssl enc -aes-128-cbc -d -in cipher2.bin -out pla
in2.txt -nopad -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task2]$ openssl enc -aes-128-cbc -d -in cipher3.bin -out pla
in3.txt -nopad -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task2]$ ls -l
total 36
-rw-rw-r--. 1 salman salman 16 Oct  2 16:50 cipher1.bin
-rw-rw-r--. 1 salman salman 16 Oct  2 16:51 cipher2.bin
-rw-rw-r--. 1 salman salman 32 Oct  2 16:51 cipher3.bin
-rw-rw-r--. 1 salman salman  5 Oct  1 21:56 file1.txt
-rw-rw-r--. 1 salman salman 10 Oct  1 21:56 file2.txt
-rw-rw-r--. 1 salman salman 16 Oct  1 21:57 file3.txt
-rw-rw-r--. 1 salman salman 16 Oct  2 21:08 plain1.txt
-rw-rw-r--. 1 salman salman 16 Oct  2 21:08 plain2.txt
-rw-rw-r--. 1 salman salman 32 Oct  2 21:09 plain3.txt
[salman@etisalat-s3 Task2]$ 
```

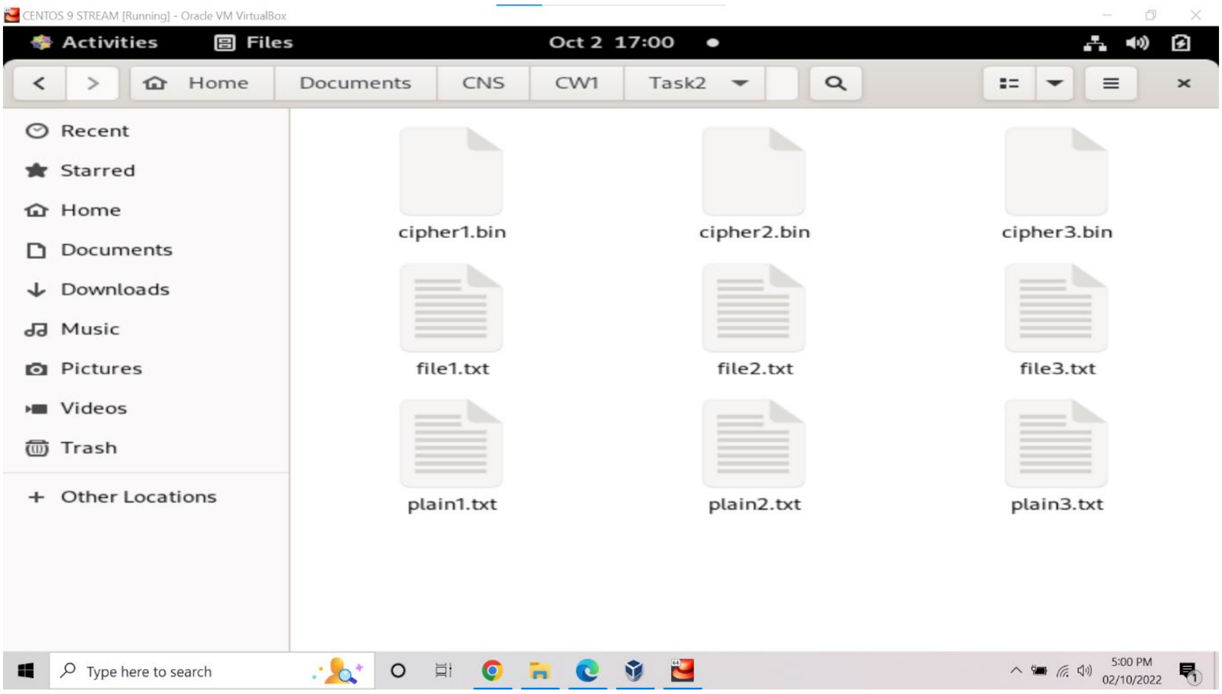

CENTOS 9 STREAM [Running] - Oracle VM VirtualBox
Activities
Terminal
Oct 2 21:25
Home
Documents
CNS
CW1
Task2
salman@etisalat-s3:~/Documents/CNS/CW1/Task2
Type here to search
9:25 PM
02/10/2022

```
[salman@etisalat-s3 Task2]$ xxd plain1.txt
00000000: 4465 6572 0a0b 0b0b 0b0b 0b0b 0b0b 0b0b  Deer............
[salman@etisalat-s3 Task2]$ xxd plain2.txt
00000000: 456c 6570 6861 6e74 730a 0606 0606 0606  Elephants.......
[salman@etisalat-s3 Task2]$ xxd plain3.txt
00000000: 4769 7261 6666 6573 2050 616e 6461 730a  Giraffes Pandas.
00000010: 1010 1010 1010 1010 1010 1010 1010 1010  ................
[salman@etisalat-s3 Task2]$
```

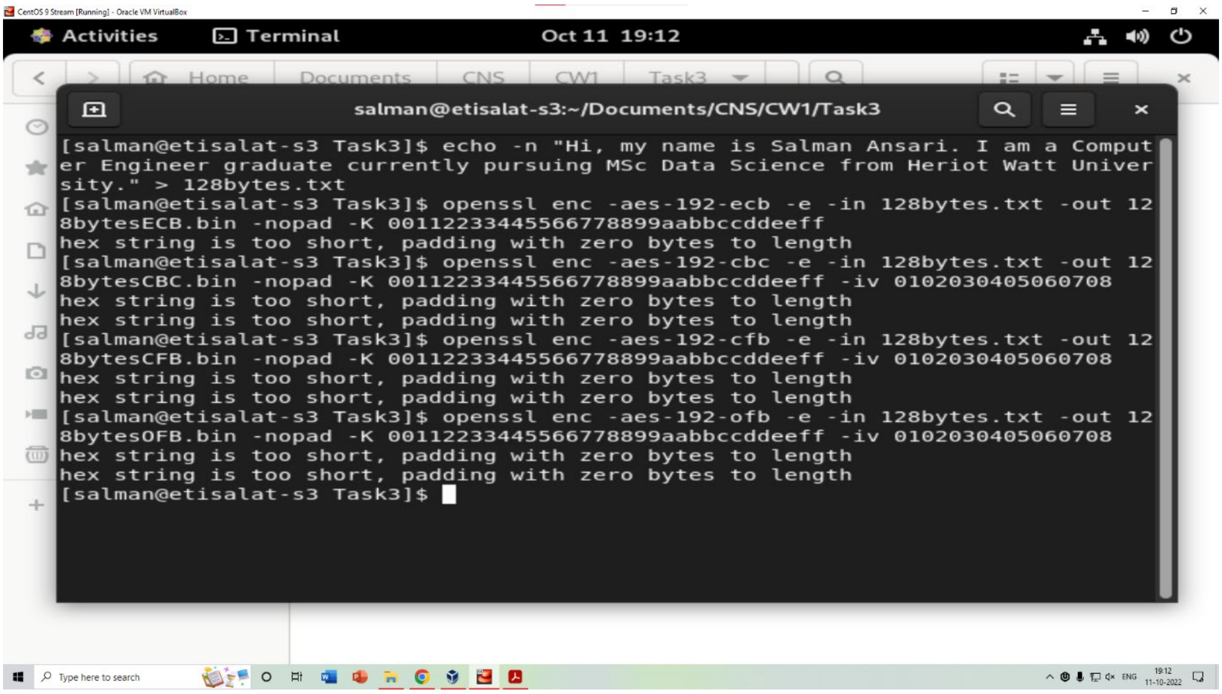


```
[salman@etisalat-s3 Task2]$ openssl enc -aes-128-cbc -d -in cipher1.bin -out plain1.txt -nopad -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task2]$ cat plain1.txt
Deer



[salman@etisalat-s3 Task2]$
```

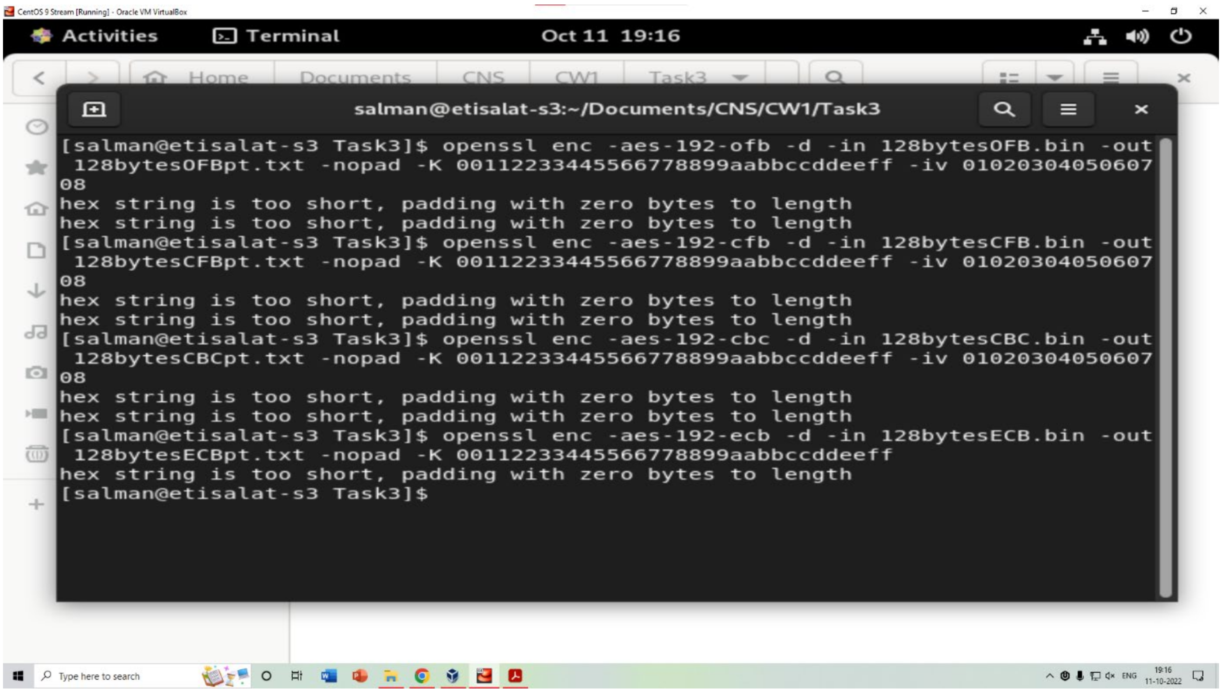
CENTOS 9 STREAM [Running] - Oracle VM VirtualBox
Activities
Terminal
Oct 2 21:30
Home
Documents
CNS
CW1
Task2
salman@etisalat-s3:~/Documents/CNS/CW1/Task2
Type here to search
9:30 PM
02/10/2022



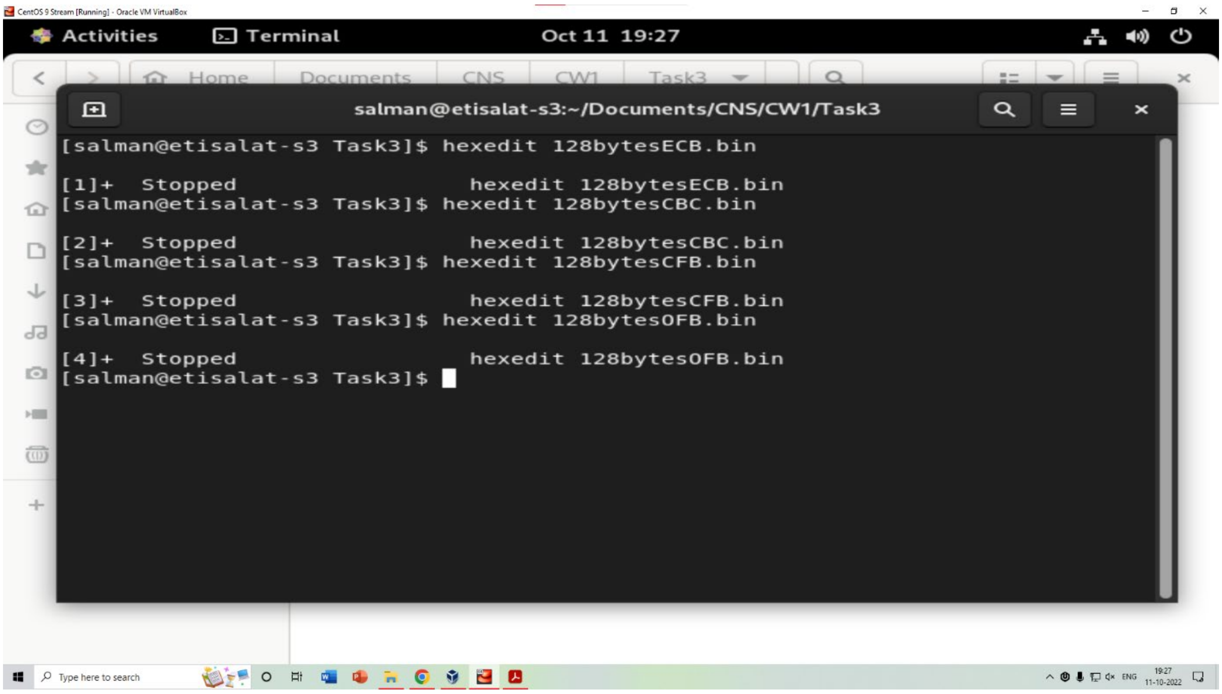
8. Appendices Task 3


CentOS 9 Stream [Running] - Oracle VM VirtualBox
Activities
Terminal
Oct 11 19:12
Home
Documents
CNS
CW1
Task3
salman@etisalat-s3:~/Documents/CNS/CW1/Task3
Type here to search
ENG
19:12
11-10-2022

```
[salman@etisalat-s3 Task3]$ echo -n "Hi, my name is Salman Ansari. I am a Comput
er Engineer graduate currently pursuing MSc Data Science from Heriot Watt Univer
sity." > 128bytes.txt
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-ecb -e -in 128bytes.txt -out 12
8bytesECB.bin -nopad -K 00112233445566778899aabbccddeeff
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-cbc -e -in 128bytes.txt -out 12
8bytesCBC.bin -nopad -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-cfb -e -in 128bytes.txt -out 12
8bytesCFB.bin -nopad -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-ofb -e -in 128bytes.txt -out 12
8bytesOFB.bin -nopad -K 00112233445566778899aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task3]$ 
```

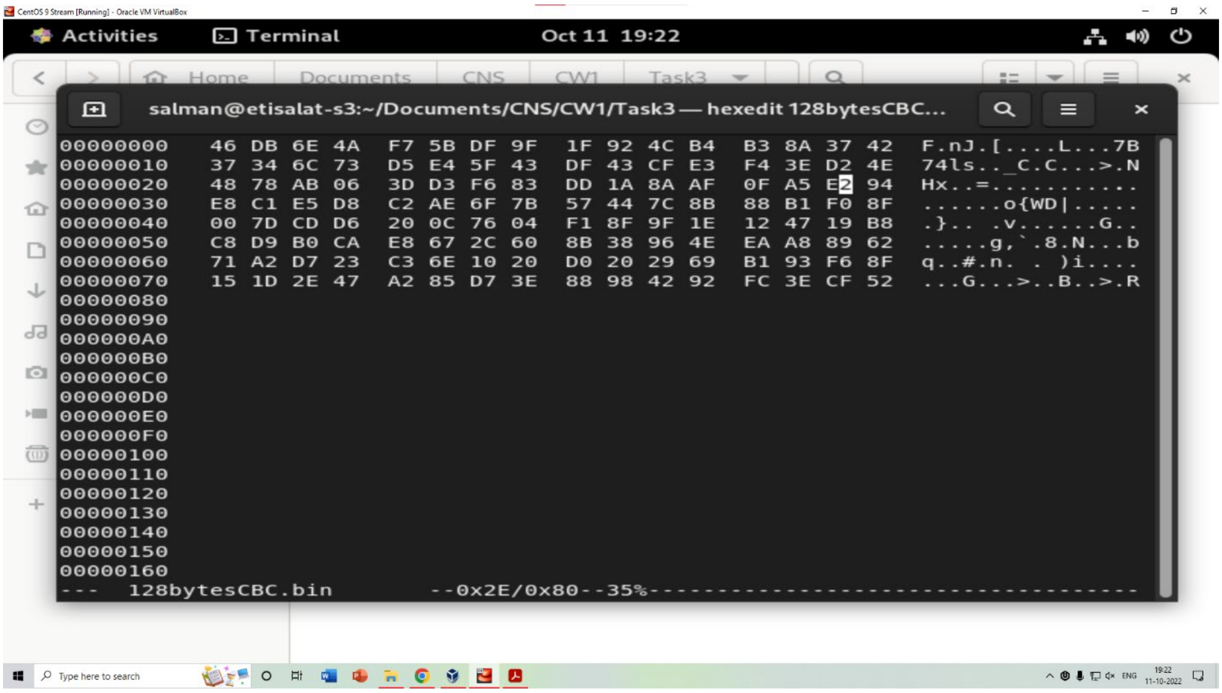

CentOS 9 Stream [Running] - Oracle VM VirtualBox
Activities
Terminal
Oct 11 19:16
Home
Documents
CNS
CW1
Task3
salman@etisalat-s3:~/Documents/CNS/CW1/Task3
Type here to search
ENG
19:16
11-10-2022

```
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-ofb -d -in 128bytesOFB.bin -out
 128bytesOFBpt.txt -nopad -K 00112233445566778899aabbccddeeff -iv 01020304050607
08
hex string is too short, padding with zero bytes to length
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-cfb -d -in 128bytesCFB.bin -out
 128bytesCFBpt.txt -nopad -K 00112233445566778899aabbccddeeff -iv 01020304050607
08
hex string is too short, padding with zero bytes to length
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-cbc -d -in 128bytesCBC.bin -out
 128bytesCBCpt.txt -nopad -K 00112233445566778899aabbccddeeff -iv 01020304050607
08
hex string is too short, padding with zero bytes to length
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-ecb -d -in 128bytesECB.bin -out
 128bytesECBpt.txt -nopad -K 00112233445566778899aabbccddeeff
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task3]$
```



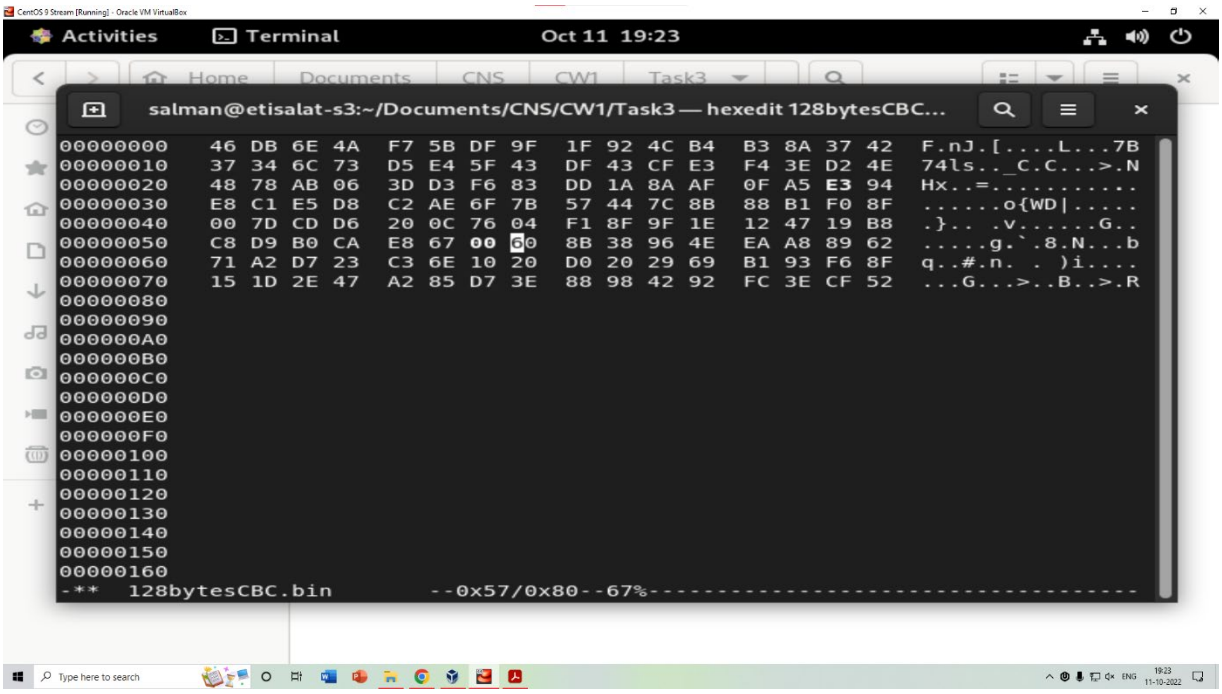
```
[salman@etisalat-s3 Task3]$ hexedit 128bytesECB.bin

[1]+  Stopped                 hexedit 128bytesECB.bin
[salman@etisalat-s3 Task3]$ hexedit 128bytesCBC.bin

[2]+  Stopped                 hexedit 128bytesCBC.bin
[salman@etisalat-s3 Task3]$ hexedit 128bytesCFB.bin

[3]+  Stopped                 hexedit 128bytesCFB.bin
[salman@etisalat-s3 Task3]$ hexedit 128bytesOFB.bin

[4]+  Stopped                 hexedit 128bytesOFB.bin
[salman@etisalat-s3 Task3]$
```

CentOS 9 Stream [Running] - Oracle VM VirtualBox
Activities
Terminal
Oct 11 19:27
salman@etisalat-s3:~/Documents/CNS/CW1/Task3
Home
Documents
CNS
CW1
Task3
Type here to search
ENG
19:27
11-10-2022

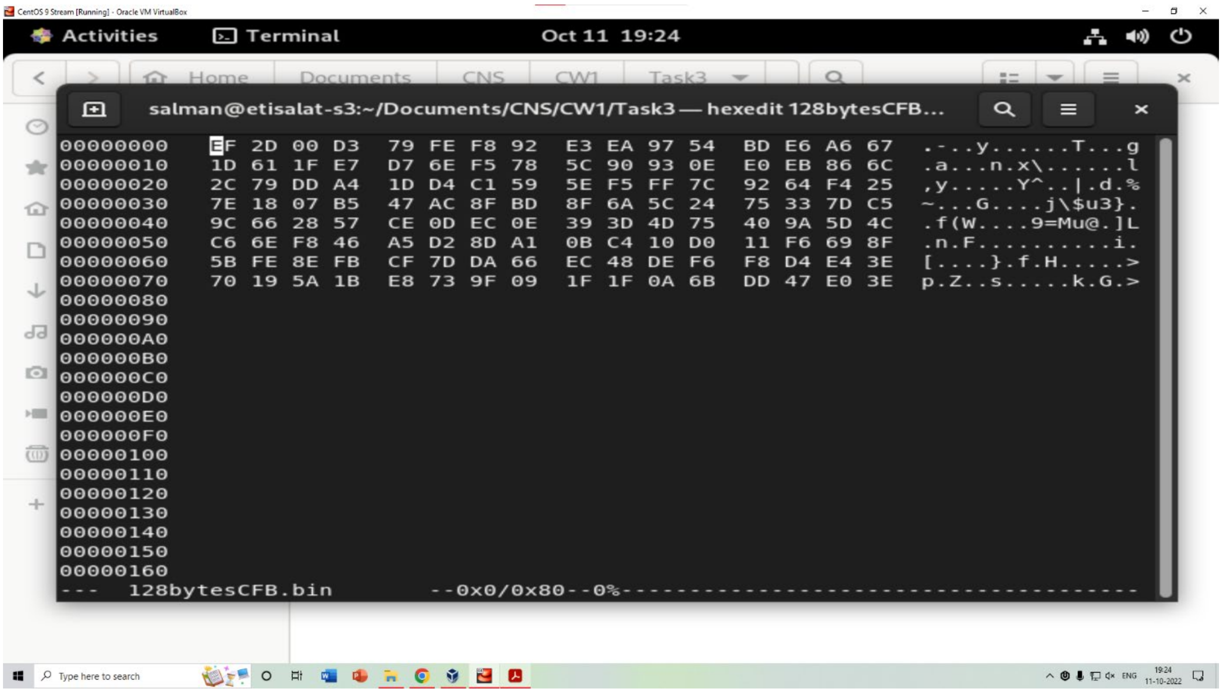


```
00000000   46 DB 6E 4A   F7 5B DF 9F   1F 92 4C B4   B3 8A 37 42   F.nJ.[....L...7B
00000010   37 34 6C 73   D5 E4 5F 43   DF 43 CF E3   F4 3E D2 4E   74ls.._C.C...>.N
00000020   48 78 AB 06   3D D3 F6 83   DD 1A 8A AF   0F A5 E2 94   Hx..=...........
00000030   E8 C1 E5 D8   C2 AE 6F 7B   57 44 7C 8B   88 B1 F0 8F   ......o{WD|.....
00000040   00 7D CD D6   20 0C 76 04   F1 8F 9F 1E   12 47 19 B8   .}.. .v......G..
00000050   C8 D9 B0 CA   E8 67 2C 60   8B 38 96 4E   EA A8 89 62   .....g,`.8.N...b
00000060   71 A2 D7 23   C3 6E 10 20   D0 20 29 69   B1 93 F6 8F   q..#.n. . )i....
00000070   15 1D 2E 47   A2 85 D7 3E   88 98 42 92   FC 3E CF 52   ...G...>..B..>.R
00000080
00000090
000000A0
000000B0
000000C0
000000D0
000000E0
000000F0
00000100
00000110
00000120
00000130
00000140
00000150
00000160
---  128bytesCBC.bin       --0x2E/0x80--35%---------------------------------
```

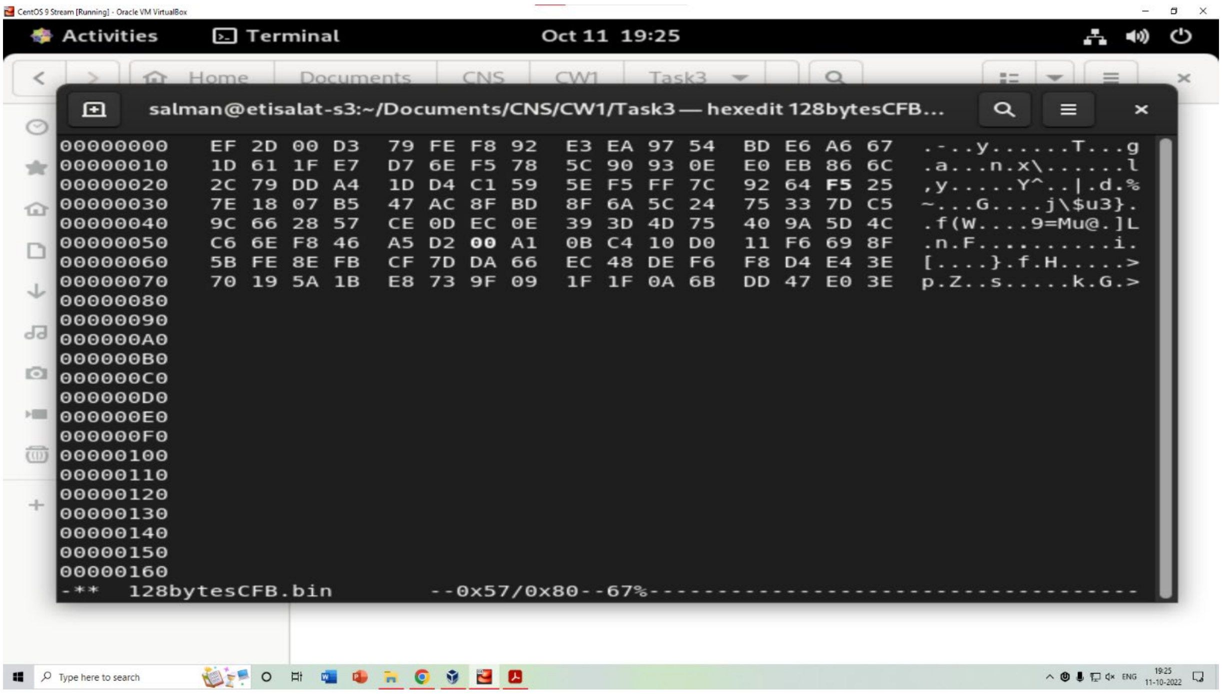
CentOS 9 Stream [Running] - Oracle VM VirtualBox
Activities
Terminal
Oct 11 19:22
salman@etisalat-s3:~/Documents/CNS/CW1/Task3 — hexedit 128bytesCBC...
Home
Documents
CNS
CW1
Task3
Type here to search
ENG
19:22
11-10-2022



```
salman@etisalat-s3:~/Documents/CNS/CW1/Task3 — hexedit 128bytesCBC...
00000000   46 DB 6E 4A  F7 5B DF 9F  1F 92 4C B4  B3 8A 37 42  F.nJ.[....L...7B
00000010   37 34 6C 73  D5 E4 5F 43  DF 43 CF E3  F4 3E D2 4E  74ls.._C.C...>.N
00000020   48 78 AB 06  3D D3 F6 83  DD 1A 8A AF  0F A5 E3 94  Hx..=...........
00000030   E8 C1 E5 D8  C2 AE 6F 7B  57 44 7C 8B  88 B1 F0 8F  ......o{WD|.....
00000040   00 7D CD D6  20 0C 76 04  F1 8F 9F 1E  12 47 19 B8  .}.. .v......G..
00000050   C8 D9 B0 CA  E8 67 00 60  8B 38 96 4E  EA A8 89 62  .....g.`.8.N...b
00000060   71 A2 D7 23  C3 6E 10 20  D0 20 29 69  B1 93 F6 8F  q..#.n. . )i....
00000070   15 1D 2E 47  A2 85 D7 3E  88 98 42 92  FC 3E CF 52  ...G...>..B..>.R
00000080
00000090
000000A0
000000B0
000000C0
000000D0
000000E0
000000F0
00000100
00000110
00000120
00000130
00000140
00000150
00000160
-**  128bytesCBC.bin       --0x57/0x80--67%-------------------------------------
```

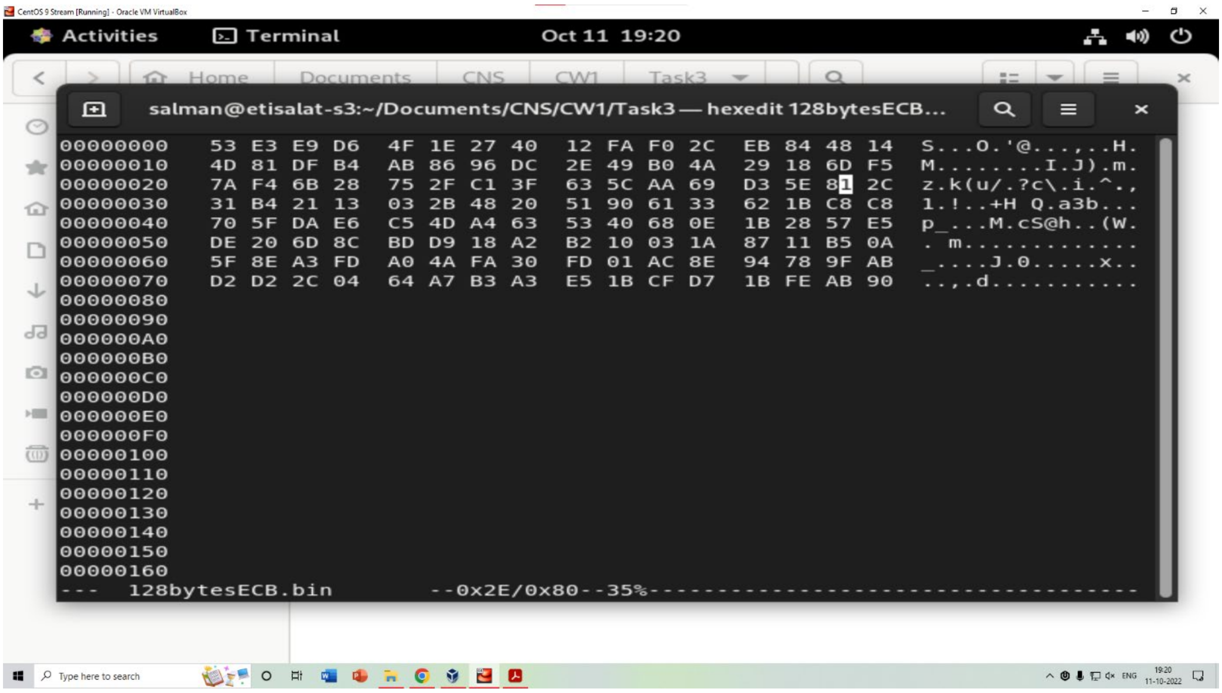


```
salman@etisalat-s3:~/Documents/CNS/CW1/Task3 — hexedit 128bytesCFB...
00000000   EF 2D 00 D3  79 FE F8 92  E3 EA 97 54  BD E6 A6 67  .-..y......T...g
00000010   1D 61 1F E7  D7 6E F5 78  5C 90 93 0E  E0 EB 86 6C  .a...n.x\......l
00000020   2C 79 DD A4  1D D4 C1 59  5E F5 FF 7C  92 64 F4 25  ,y.....Y^..|.d.%
00000030   7E 18 07 B5  47 AC 8F BD  8F 6A 5C 24  75 33 7D C5  ~...G....j\$u3}.
00000040   9C 66 28 57  CE 0D EC 0E  39 3D 4D 75  40 9A 5D 4C  .f(W....9=Mu@.]L
00000050   C6 6E F8 46  A5 D2 8D A1  0B C4 10 D0  11 F6 69 8F  .n.F..........i.
00000060   5B FE 8E FB  CF 7D DA 66  EC 48 DE F6  F8 D4 E4 3E  [....}.f.H.....>
00000070   70 19 5A 1B  E8 73 9F 09  1F 1F 0A 6B  DD 47 E0 3E  p.Z..s.....k.G.>
00000080
00000090
000000A0
000000B0
000000C0
000000D0
000000E0
000000F0
00000100
00000110
00000120
00000130
00000140
00000150
00000160
---  128bytesCFB.bin       --0x0/0x80--0%--------------------------------------
```



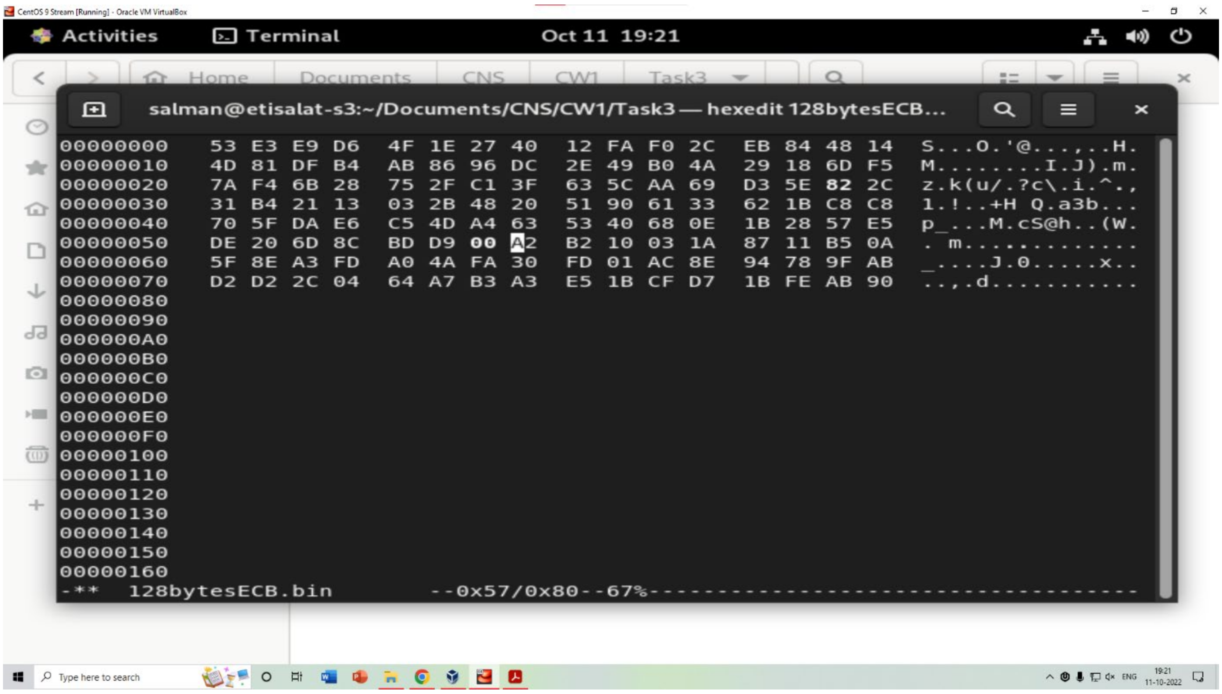
CentOS 9 Stream [Running] - Oracle VM VirtualBox
Activities
Terminal
Oct 11 19:25
Home
Documents
CNS
CW1
Task3
salman@etisalat-s3:~/Documents/CNS/CW1/Task3 — hexedit 128bytesCFB...
Type here to search

```
00000000   EF 2D 00 D3  79 FE F8 92  E3 EA 97 54  BD E6 A6 67  .-..y......T...g
00000010   1D 61 1F E7  D7 6E F5 78  5C 90 93 0E  E0 EB 86 6C  .a...n.x\......l
00000020   2C 79 DD A4  1D D4 C1 59  5E F5 FF 7C  92 64 F5 25  ,y.....Y^..|.d.%
00000030   7E 18 07 B5  47 AC 8F BD  8F 6A 5C 24  75 33 7D C5  ~...G....j\$u3}.
00000040   9C 66 28 57  CE 0D EC 0E  39 3D 4D 75  40 9A 5D 4C  .f(W....9=Mu@.]L
00000050   C6 6E F8 46  A5 D2 00 A1  0B C4 10 D0  11 F6 69 8F  .n.F..........i.
00000060   5B FE 8E FB  CF 7D DA 66  EC 48 DE F6  F8 D4 E4 3E  [....}.f.H.....>
00000070   70 19 5A 1B  E8 73 9F 09  1F 1F 0A 6B  DD 47 E0 3E  p.Z..s.....k.G.>
00000080
00000090
000000A0
000000B0
000000C0
000000D0
000000E0
000000F0
00000100
00000110
00000120
00000130
00000140
00000150
00000160
-**  128bytesCFB.bin       --0x57/0x80--67%-----------------------------------
```



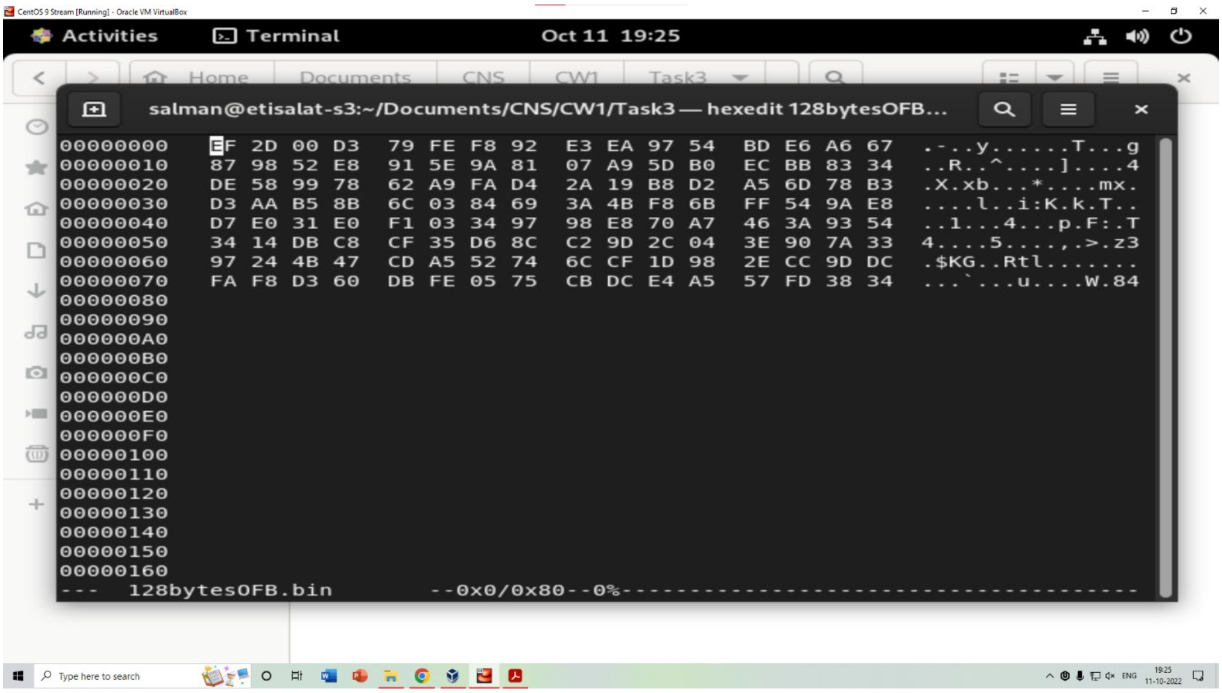
CentOS 9 Stream [Running] - Oracle VM VirtualBox
Activities
Terminal
Oct 11 19:20
Home
Documents
CNS
CW1
Task3
salman@etisalat-s3:~/Documents/CNS/CW1/Task3 — hexedit 128bytesECB...
Type here to search

```
00000000   53 E3 E9 D6  4F 1E 27 40  12 FA F0 2C  EB 84 48 14  S...O.'@...,..H.
00000010   4D 81 DF B4  AB 86 96 DC  2E 49 B0 4A  29 18 6D F5  M........I.J).m.
00000020   7A F4 6B 28  75 2F C1 3F  63 5C AA 69  D3 5E 81 2C  z.k(u/.?c\.i.^.,
00000030   31 B4 21 13  03 2B 48 20  51 90 61 33  62 1B C8 C8  1.!..+H Q.a3b...
00000040   70 5F DA E6  C5 4D A4 63  53 40 68 0E  1B 28 57 E5  p_...M.cS@h..(W.
00000050   DE 20 6D 8C  BD D9 18 A2  B2 10 03 1A  87 11 B5 0A  . m.............
00000060   5F 8E A3 FD  A0 4A FA 30  FD 01 AC 8E  94 78 9F AB  _....J.0.....x..
00000070   D2 D2 2C 04  64 A7 B3 A3  E5 1B CF D7  1B FE AB 90  ..,.d...........
00000080
00000090
000000A0
000000B0
000000C0
000000D0
000000E0
000000F0
00000100
00000110
00000120
00000130
00000140
00000150
00000160
---  128bytesECB.bin       --0x2E/0x80--35%-----------------------------------
```



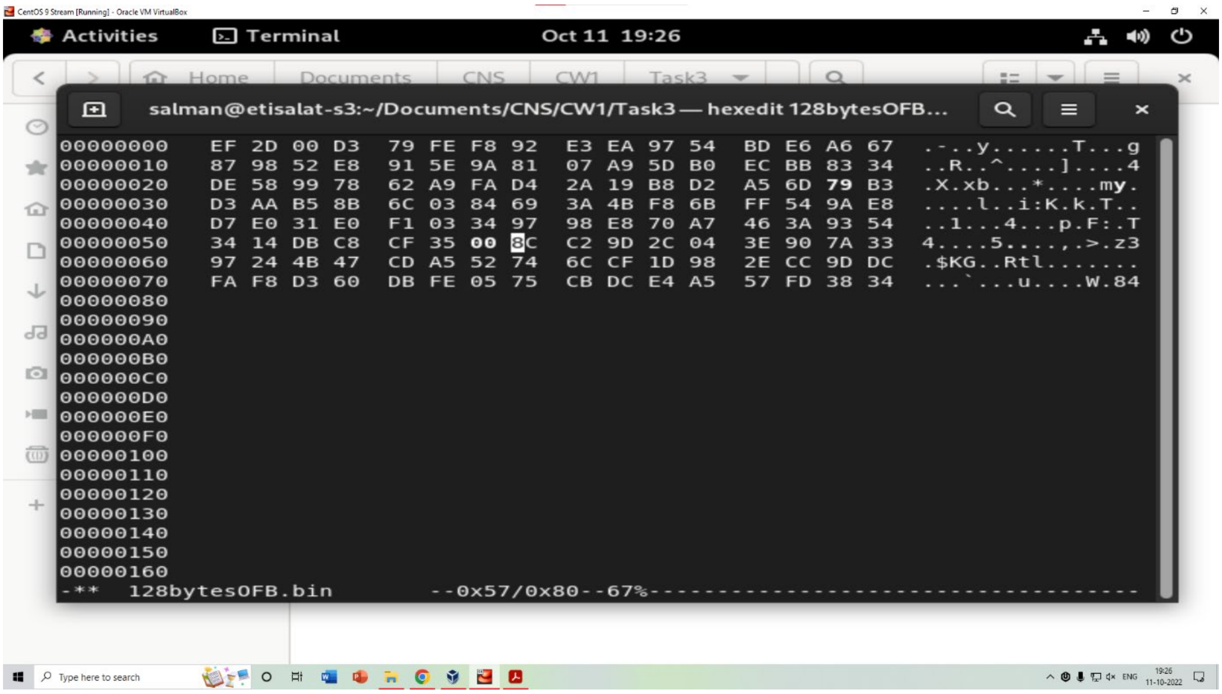
salman@etisalat-s3:~/Documents/CNS/CW1/Task3 — hexedit 128bytesECB...

```
00000000   53 E3 E9 D6  4F 1E 27 40  12 FA F0 2C  EB 84 48 14  S...O.'@...,..H.
00000010   4D 81 DF B4  AB 86 96 DC  2E 49 B0 4A  29 18 6D F5  M........I.J).m.
00000020   7A F4 6B 28  75 2F C1 3F  63 5C AA 69  D3 5E 82 2C  z.k(u/.?c\.i.^.,
00000030   31 B4 21 13  03 2B 48 20  51 90 61 33  62 1B C8 C8  1.!..+H Q.a3b...
00000040   70 5F DA E6  C5 4D A4 63  53 40 68 0E  1B 28 57 E5  p_...M.cS@h..(W.
00000050   DE 20 6D 8C  BD D9 00 A2  B2 10 03 1A  87 11 B5 0A  . m.............
00000060   5F 8E A3 FD  A0 4A FA 30  FD 01 AC 8E  94 78 9F AB  _....J.0.....x..
00000070   D2 D2 2C 04  64 A7 B3 A3  E5 1B CF D7  1B FE AB 90  ..,.d...........
00000080
00000090
000000A0
000000B0
000000C0
000000D0
000000E0
000000F0
00000100
00000110
00000120
00000130
00000140
00000150
00000160
-**  128bytesECB.bin       --0x57/0x80--67%----------------------------------------
```



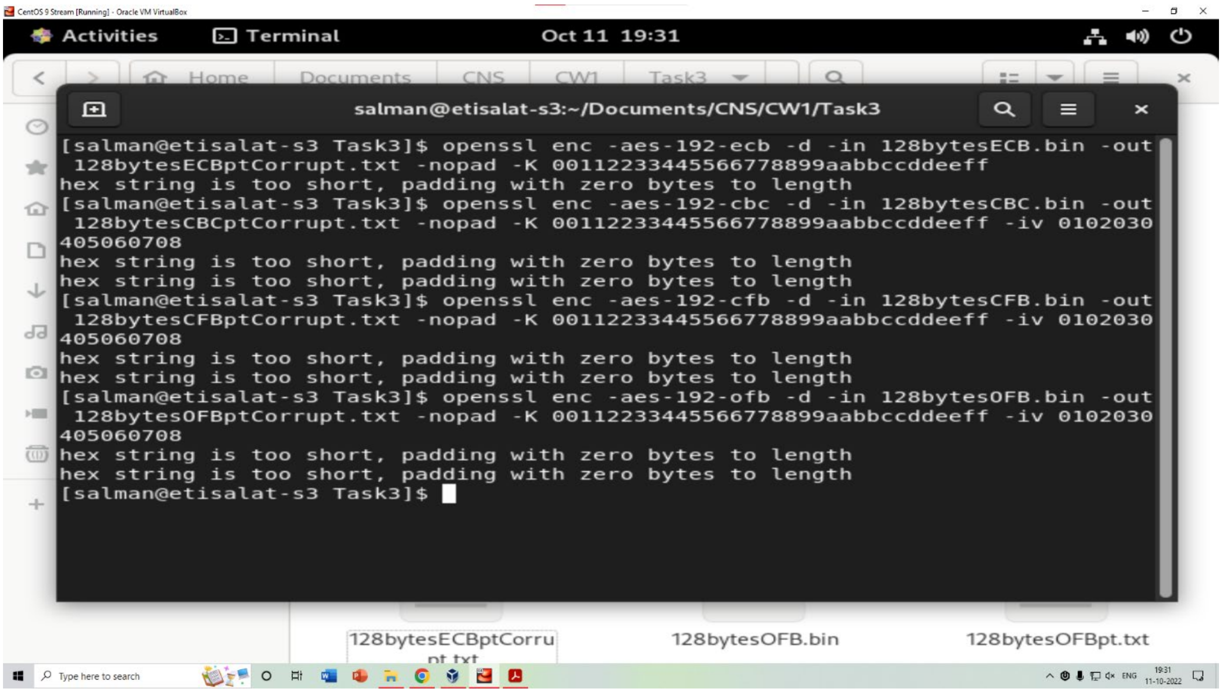
salman@etisalat-s3:~/Documents/CNS/CW1/Task3 — hexedit 128bytesOFB...

```
00000000   EF 2D 00 D3  79 FE F8 92  E3 EA 97 54  BD E6 A6 67  .-..y......T...g
00000010   87 98 52 E8  91 5E 9A 81  07 A9 5D B0  EC BB 83 34  ..R..^....]....4
00000020   DE 58 99 78  62 A9 FA D4  2A 19 B8 D2  A5 6D 78 B3  .X.xb...*....mx.
00000030   D3 AA B5 8B  6C 03 84 69  3A 4B F8 6B  FF 54 9A E8  ....l..i:K.k.T..
00000040   D7 E0 31 E0  F1 03 34 97  98 E8 70 A7  46 3A 93 54  ..1...4...p.F:.T
00000050   34 14 DB C8  CF 35 D6 8C  C2 9D 2C 04  3E 90 7A 33  4....5....,.>.z3
00000060   97 24 4B 47  CD A5 52 74  6C CF 1D 98  2E CC 9D DC  .$KG..Rtl.......
00000070   FA F8 D3 60  DB FE 05 75  CB DC E4 A5  57 FD 38 34  ...`...u....W.84
00000080
00000090
000000A0
000000B0
000000C0
000000D0
000000E0
000000F0
00000100
00000110
00000120
00000130
00000140
00000150
00000160
---  128bytesOFB.bin       --0x0/0x80--0%----------------------------------------
```



salman@etisalat-s3:~/Documents/CNS/CW1/Task3 — hexedit 128bytesOFB...

```
00000000   EF 2D 00 D3  79 FE F8 92  E3 EA 97 54  BD E6 A6 67  .-..y......T...g
00000010   87 98 52 E8  91 5E 9A 81  07 A9 5D B0  EC BB 83 34  ..R..^....]....4
00000020   DE 58 99 78  62 A9 FA D4  2A 19 B8 D2  A5 6D 79 B3  .X.xb...*....my.
00000030   D3 AA B5 8B  6C 03 84 69  3A 4B F8 6B  FF 54 9A E8  ....l..i:K.k.T..
00000040   D7 E0 31 E0  F1 03 34 97  98 E8 70 A7  46 3A 93 54  ..1...4...p.F:.T
00000050   34 14 DB C8  CF 35 00 8C  C2 9D 2C 04  3E 90 7A 33  4....5....,.>.z3
00000060   97 24 4B 47  CD A5 52 74  6C CF 1D 98  2E CC 9D DC  .$KG..Rtl.......
00000070   FA F8 D3 60  DB FE 05 75  CB DC E4 A5  57 FD 38 34  ...`...u....W.84
00000080
00000090
000000A0
000000B0
000000C0
000000D0
000000E0
000000F0
00000100
00000110
00000120
00000130
00000140
00000150
00000160
-**  128bytesOFB.bin       --0x57/0x80--67%--------------------------------------
```



salman@etisalat-s3:~/Documents/CNS/CW1/Task3

```
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-ecb -d -in 128bytesECB.bin -out
 128bytesECBptCorrupt.txt -nopad -K 00112233445566778899aabbccddeeff
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-cbc -d -in 128bytesCBC.bin -out
 128bytesCBCptCorrupt.txt -nopad -K 00112233445566778899aabbccddeeff -iv 0102030
405060708
hex string is too short, padding with zero bytes to length
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-cfb -d -in 128bytesCFB.bin -out
 128bytesCFBptCorrupt.txt -nopad -K 00112233445566778899aabbccddeeff -iv 0102030
405060708
hex string is too short, padding with zero bytes to length
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task3]$ openssl enc -aes-192-ofb -d -in 128bytesOFB.bin -out
 128bytesOFBptCorrupt.txt -nopad -K 00112233445566778899aabbccddeeff -iv 0102030
405060708
hex string is too short, padding with zero bytes to length
hex string is too short, padding with zero bytes to length
[salman@etisalat-s3 Task3]$ 
```