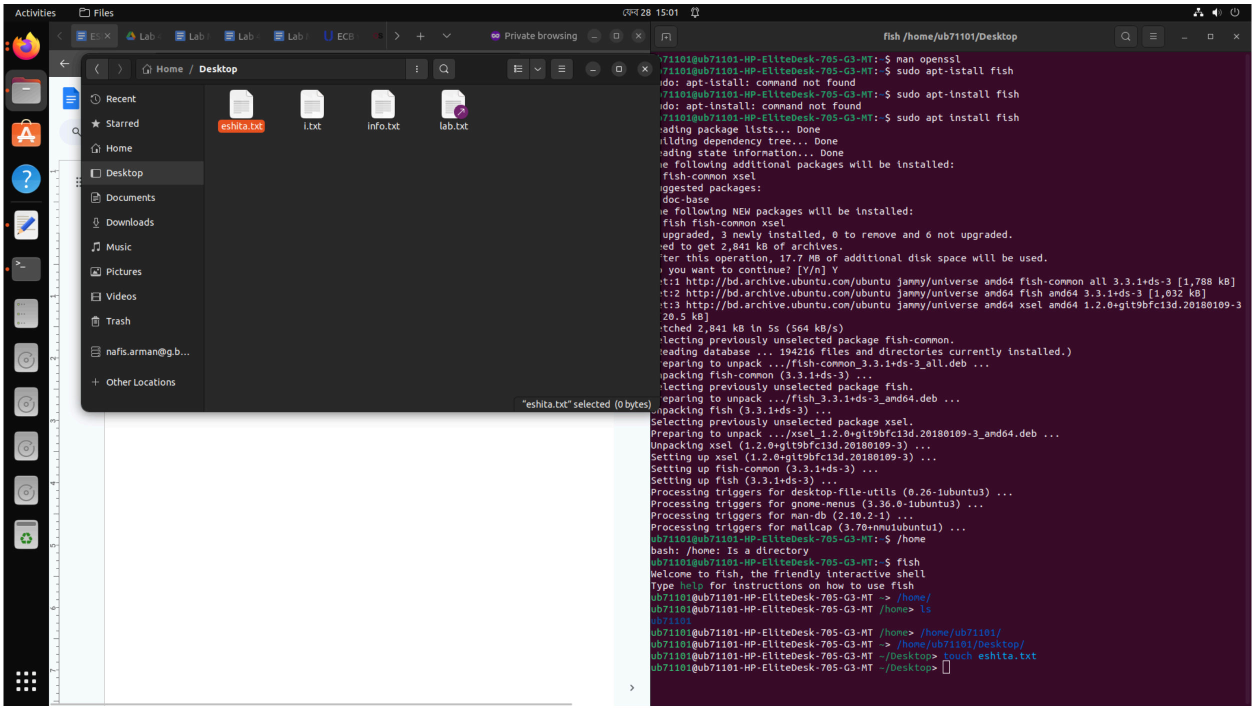
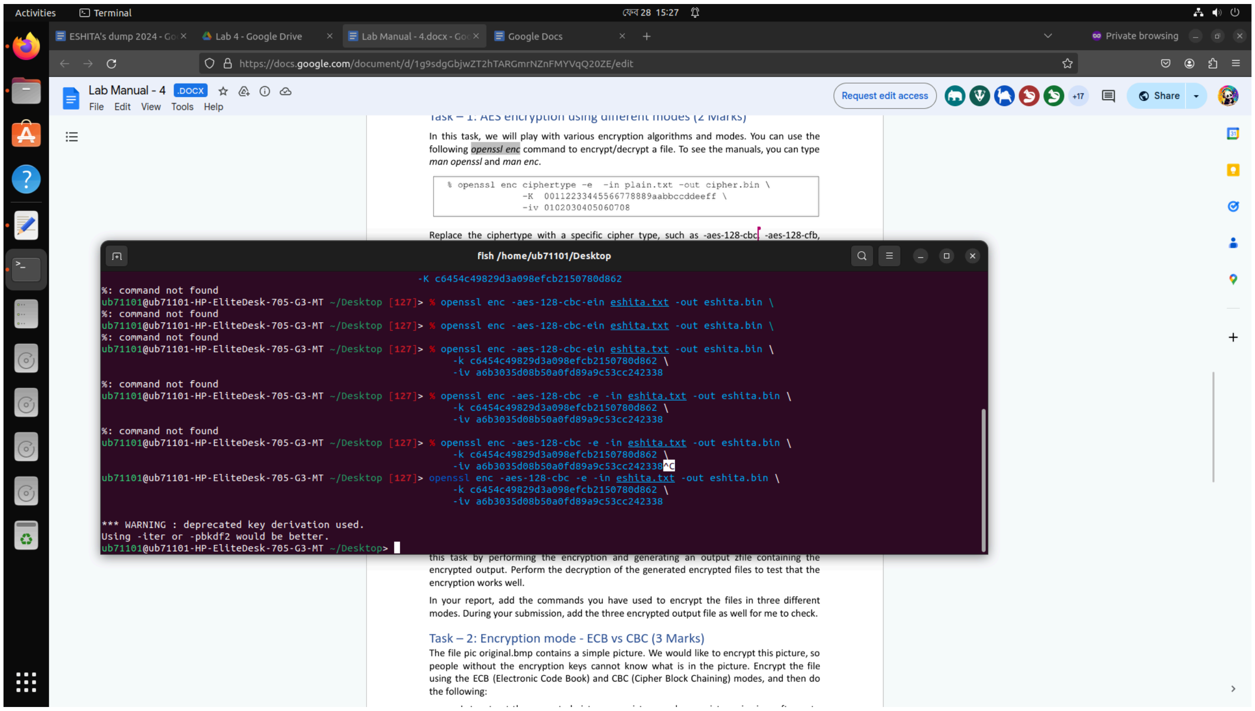


```
)71101@ub71101-HP-EliteDesk-705-G3-MT:~$ man openssl
)71101@ub71101-HP-EliteDesk-705-G3-MT:~$ sudo apt-istall fish
ido: apt-istall: command not found
)71101@ub71101-HP-EliteDesk-705-G3-MT:~$ sudo apt-install fish
ido: apt-install: command not found
)71101@ub71101-HP-EliteDesk-705-G3-MT:~$ sudo apt install fish
eading package lists... Done
iilding dependency tree... Done
eading state information... Done
ie following additional packages will be installed:
 fish-common xsel
iggested packages:
 doc-base
ie following NEW packages will be installed:
 fish fish-common xsel
 upgraded, 3 newly installed, 0 to remove and 6 not upgraded.
eed to get 2,841 kB of archives.
fter this operation, 17.7 MB of additional disk space will be used.
) you want to continue? [Y/n] Y
et:1 http://bd.archive.ubuntu.com/ubuntu jammy/universe amd64 fish-common all 3.3.1+ds-3 [1,788 kB]
et:2 http://bd.archive.ubuntu.com/ubuntu jammy/universe amd64 fish amd64 3.3.1+ds-3 [1,032 kB]
et:3 http://bd.archive.ubuntu.com/ubuntu jammy/universe amd64 xsel amd64 1.2.0+git9bfc13d.20180109-3
[20.5 kB]
etched 2,841 kB in 5s (564 kB/s)
electing previously unselected package fish-common.
Reading database ... 194216 files and directories currently installed.)
reparing to unpack .../fish-common_3.3.1+ds-3_all.deb ...
npacking fish-common (3.3.1+ds-3) ...
electing previously unselected package fish.
reparing to unpack .../fish_3.3.1+ds-3_amd64.deb ...
Unpacking fish (3.3.1+ds-3) ...
Selecting previously unselected package xsel.
Preparing to unpack .../xsel_1.2.0+git9bfc13d.20180109-3_amd64.deb ...
Unpacking xsel (1.2.0+git9bfc13d.20180109-3) ...
Setting up xsel (1.2.0+git9bfc13d.20180109-3) ...
Setting up fish-common (3.3.1+ds-3) ...
Setting up fish (3.3.1+ds-3) ...
Processing triggers for desktop-file-utils (0.26-1ubuntu3) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu3) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for mailcap (3.70+nmu1ubuntu1) ...
ub71101@ub71101-HP-EliteDesk-705-G3-MT:~$ /home
bash: /home: Is a directory
ub71101@ub71101-HP-EliteDesk-705-G3-MT:~$ fish
Welcome to fish, the friendly interactive shell
Type help for instructions on how to use fish
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~> /home/
ub71101@ub71101-HP-EliteDesk-705-G3-MT /home> ls
ub71101
ub71101@ub71101-HP-EliteDesk-705-G3-MT /home> /home/ub71101/
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~> /home/ub71101/Desktop/
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> touch eshita.txt
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> 
```



Task – 1: AES encryption using different modes (2 Marks)

In this task, we will play with various encryption algorithms and modes. You can use the following *openssl enc* command to encrypt/decrypt a file. To see the manuals, you can type *man openssl* and *man enc*.

```
% openssl enc ciphertype -e  -in plain.txt -out cipher.bin \
          -K  00112233445566778889aabbccddeeff \
          -iv 0102030405060708
```

Replace the ciphertype with a specific cipher type, such as -aes-128-cbc, -aes-128-cfb,

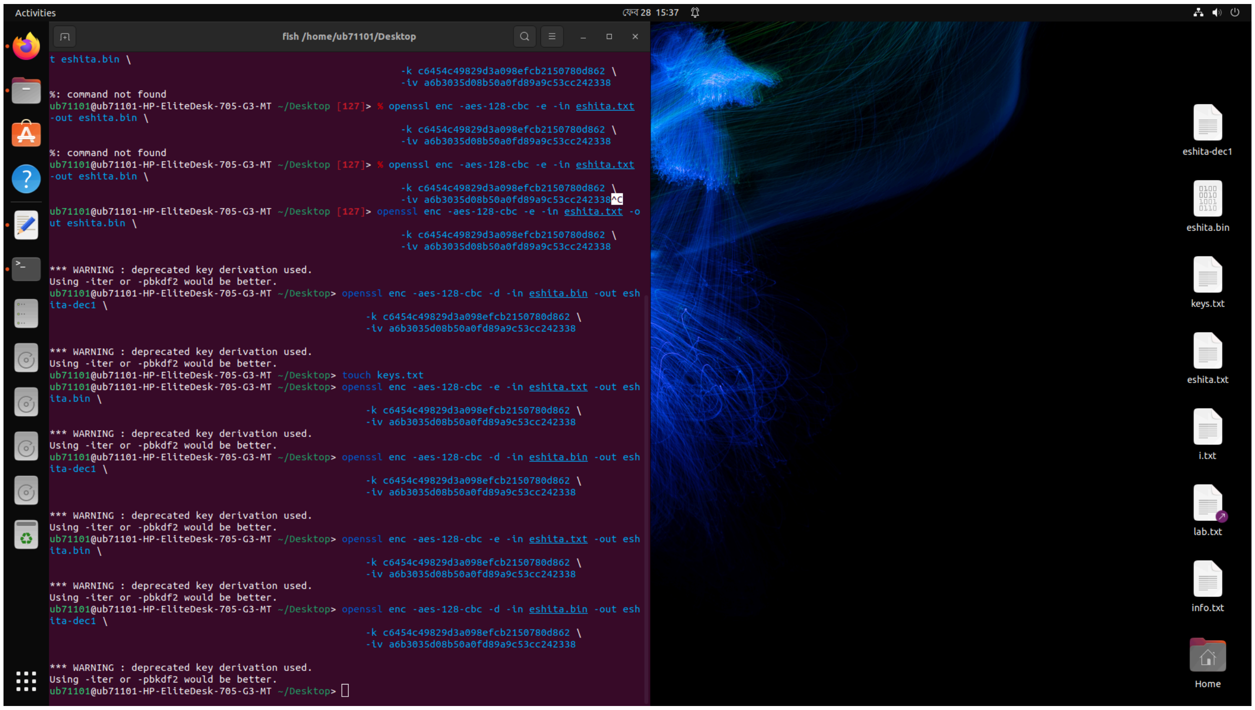
```
                                    -K c6454c49829d3a098efcb2150780d862
%: command not found
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop [127]> % openssl enc -aes-128-cbc-ein eshita.txt -out eshita.bin \
%: command not found
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop [127]> % openssl enc -aes-128-cbc-ein eshita.txt -out eshita.bin \
%: command not found
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop [127]> % openssl enc -aes-128-cbc-ein eshita.txt -out eshita.bin \
                                                          -k c6454c49829d3a098efcb2150780d862 \
                                                          -iv a6b3035d08b50a0fd89a9c53cc242338

%: command not found
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop [127]> % openssl enc -aes-128-cbc -e -in eshita.txt -out eshita.bin \
                                                          -k c6454c49829d3a098efcb2150780d862 \
                                                          -iv a6b3035d08b50a0fd89a9c53cc242338

%: command not found
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop [127]> % openssl enc -aes-128-cbc -e -in eshita.txt -out eshita.bin \
                                                          -k c6454c49829d3a098efcb2150780d862 \
                                                          -iv a6b3035d08b50a0fd89a9c53cc242338^C
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop [127]> openssl enc -aes-128-cbc -e -in eshita.txt -out eshita.bin \
                                                          -k c6454c49829d3a098efcb2150780d862 \
                                                          -iv a6b3035d08b50a0fd89a9c53cc242338


*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> 
```

this task by performing the encryption and generating an output zfile containing the encrypted output. Perform the decryption of the generated encrypted files to test that the encryption works well.

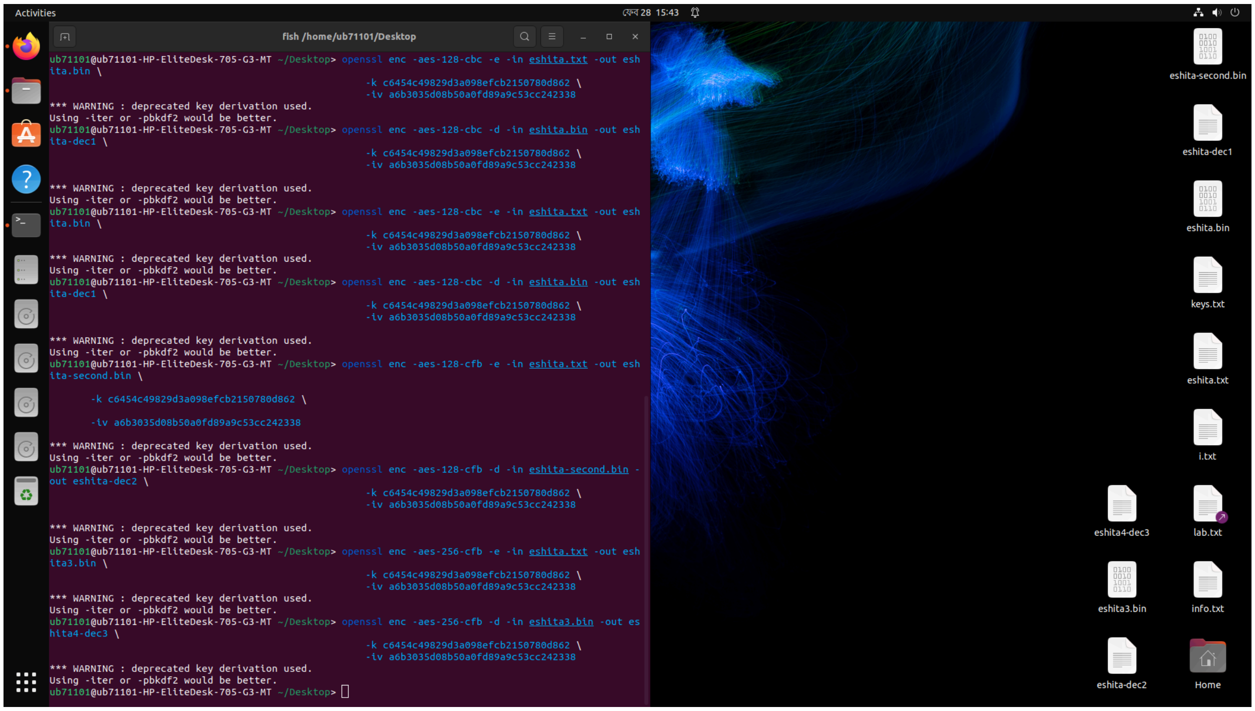
In your report, add the commands you have used to encrypt the files in three different modes. During your submission, add the three encrypted output file as well for me to check.

Task – 2: Encryption mode - ECB vs CBC (3 Marks)

The file pic original.bmp contains a simple picture. We would like to encrypt this picture, so people without the encryption keys cannot know what is in the picture. Encrypt the file using the ECB (Electronic Code Book) and CBC (Cipher Block Chaining) modes, and then do the following:

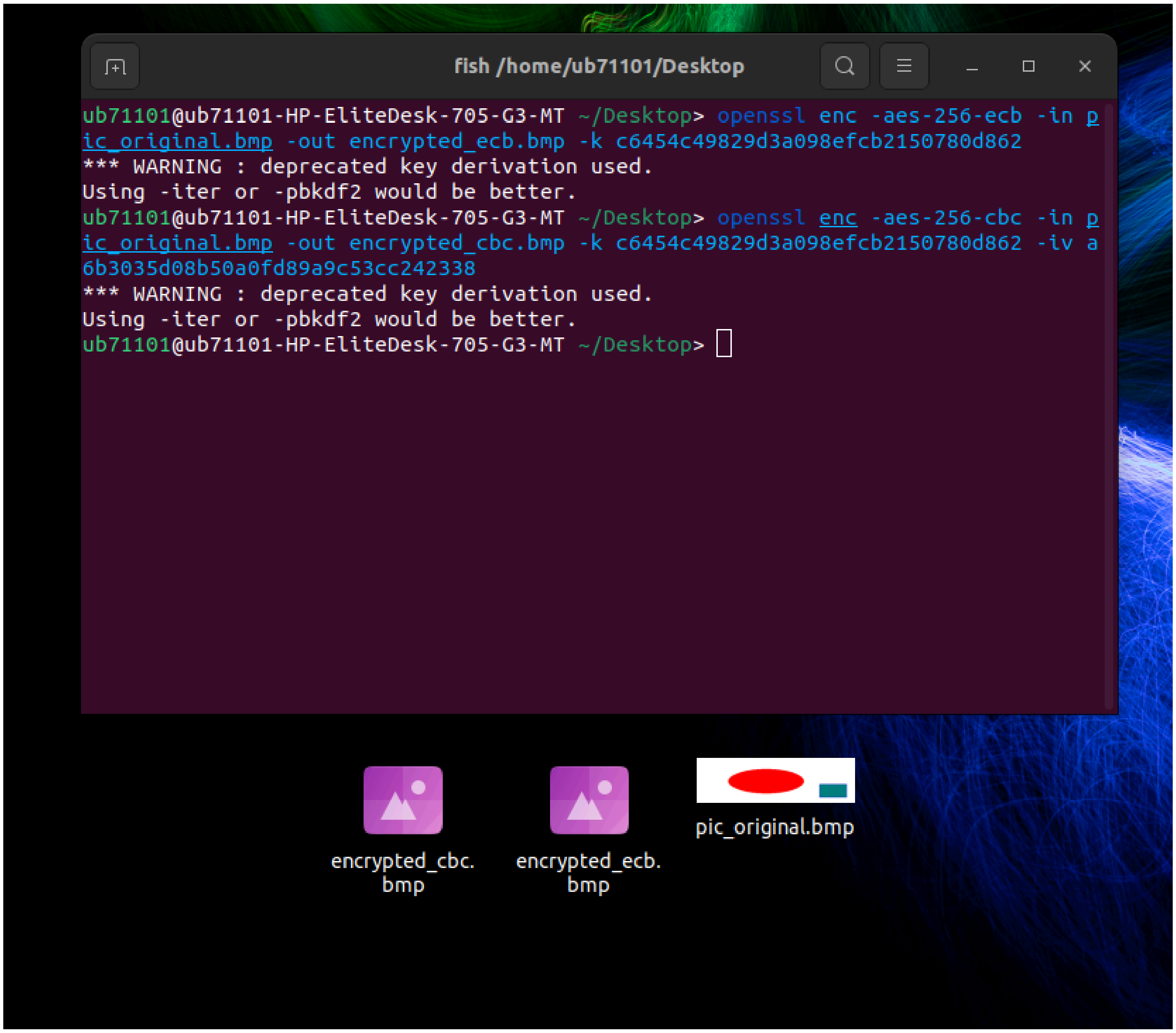


```
t eshita.bin \
                                                            -k c6454c49829d3a098efcb2150780d862 \
                                                            -iv a6b3035d08b50a0fd89a9c53cc242338
%: command not found
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop [127]> % openssl enc -aes-128-cbc -e -in eshita.txt
-out eshita.bin \
                                                            -k c6454c49829d3a098efcb2150780d862 \
                                                            -iv a6b3035d08b50a0fd89a9c53cc242338
%: command not found
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop [127]> % openssl enc -aes-128-cbc -e -in eshita.txt
-out eshita.bin \
                                                            -k c6454c49829d3a098efcb2150780d862 \
                                                            -iv a6b3035d08b50a0fd89a9c53cc242338^C
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop [127]> openssl enc -aes-128-cbc -e -in eshita.txt -o
ut eshita.bin \
                                                            -k c6454c49829d3a098efcb2150780d862 \
                                                            -iv a6b3035d08b50a0fd89a9c53cc242338

*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> openssl enc -aes-128-cbc -d -in eshita.bin -out esh
ita-dec1 \
                                                      -k c6454c49829d3a098efcb2150780d862 \
                                                      -iv a6b3035d08b50a0fd89a9c53cc242338

*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> touch keys.txt
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> openssl enc -aes-128-cbc -e -in eshita.txt -out esh
ita.bin \
                                                      -k c6454c49829d3a098efcb2150780d862 \
                                                      -iv a6b3035d08b50a0fd89a9c53cc242338
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> openssl enc -aes-128-cbc -d -in eshita.bin -out esh
ita-dec1 \
                                                      -k c6454c49829d3a098efcb2150780d862 \
                                                      -iv a6b3035d08b50a0fd89a9c53cc242338

*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> openssl enc -aes-128-cbc -e -in eshita.txt -out esh
ita.bin \
                                                      -k c6454c49829d3a098efcb2150780d862 \
                                                      -iv a6b3035d08b50a0fd89a9c53cc242338
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> openssl enc -aes-128-cbc -d -in eshita.bin -out esh
ita-dec1 \
                                                      -k c6454c49829d3a098efcb2150780d862 \
                                                      -iv a6b3035d08b50a0fd89a9c53cc242338

*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop>
```

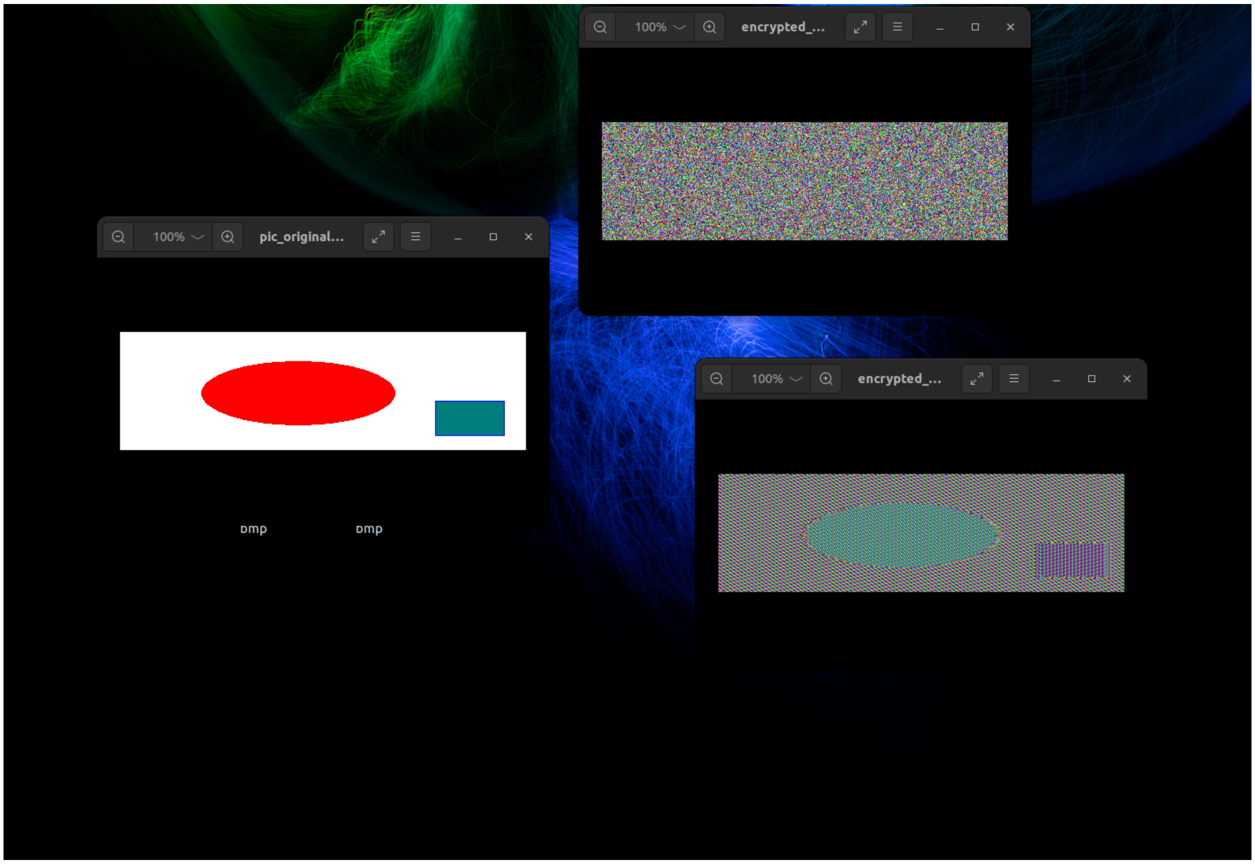


```
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> openssl enc -aes-128-cbc -e -in eshita.txt -out esh
ita.bin \
                                                      -k c6454c49829d3a098efcb2150780d862 \
                                                      -iv a6b3035d08b50a0fd89a9c53cc242338
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> openssl enc -aes-128-cbc -d -in eshita.bin -out esh
ita-dec1 \
                                                      -k c6454c49829d3a098efcb2150780d862 \
                                                      -iv a6b3035d08b50a0fd89a9c53cc242338

*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> openssl enc -aes-128-cbc -e -in eshita.txt -out esh
ita.bin \
                                                      -k c6454c49829d3a098efcb2150780d862 \
                                                      -iv a6b3035d08b50a0fd89a9c53cc242338
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> openssl enc -aes-128-cbc -d -in eshita.bin -out esh
ita-dec1 \
                                                      -k c6454c49829d3a098efcb2150780d862 \
                                                      -iv a6b3035d08b50a0fd89a9c53cc242338

*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> openssl enc -aes-128-cfb -e -in eshita.txt -out esh
ita-second.bin \

       -k c6454c49829d3a098efcb2150780d862 \

       -iv a6b3035d08b50a0fd89a9c53cc242338

*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> openssl enc -aes-128-cfb -d -in eshita-second.bin -
out eshita-dec2 \
                                                      -k c6454c49829d3a098efcb2150780d862 \
                                                      -iv a6b3035d08b50a0fd89a9c53cc242338

*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> openssl enc -aes-256-cfb -e -in eshita.txt -out esh
ita3.bin \
                                                      -k c6454c49829d3a098efcb2150780d862 \
                                                      -iv a6b3035d08b50a0fd89a9c53cc242338
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> openssl enc -aes-256-cfb -d -in eshita3.bin -out es
hita4-dec3 \
                                                      -k c6454c49829d3a098efcb2150780d862 \
                                                      -iv a6b3035d08b50a0fd89a9c53cc242338
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop>
```

## Task 2:



```
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> openssl enc -aes-256-ecb -in p
ic_original.bmp -out encrypted_ecb.bmp -k c6454c49829d3a098efcb2150780d862
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> openssl enc -aes-256-cbc -in p
ic_original.bmp -out encrypted_cbc.bmp -k c6454c49829d3a098efcb2150780d862 -iv a
6b3035d08b50a0fd89a9c53cc242338
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> 
```



Used commands task 1:

```
touch eshita.txt
/home/ub71101/Desktop/
ub71101@ub71101-HP-EliteDesk-705-G3-MT ~/Desktop> touch eshita.txt
openssl rand -hex 16
openssl enc -aes-128-cbc -e -in eshita.txt -out eshita.bin \
                                             -k c6454c49829d3a098efcb2150780d862 \
                                             -iv a6b3035d08b50a0fd89a9c53cc242338




openssl enc -aes-128-cbc -d -in eshita.bin -out eshita-dec1 \
                                             -k c6454c49829d3a098efcb2150780d862 \
                                             -iv a6b3035d08b50a0fd89a9c53cc242338
openssl enc -aes-128-cfb -e -in eshita.txt -out eshita-second.bin \

         -k c6454c49829d3a098efcb2150780d862 \

         -iv a6b3035d08b50a0fd89a9c53cc242338

openssl enc -aes-128-cfb -d -in eshita-second.bin -out eshita-dec2 \
                                             -k c6454c49829d3a098efcb2150780d862 \
                                     -iv a6b3035d08b50a0fd89a9c53cc242338
```

```
openssl enc -aes-256-cfb -e -in eshita.txt -out eshita3.bin \
                                     -k c6454c49829d3a098efcb2150780d862 \
                                     -iv a6b3035d08b50a0fd89a9c53cc242338
```

```
openssl enc -aes-256-cfb -d -in eshita3.bin -out eshita4-dec3 \
                                     -k c6454c49829d3a098efcb2150780d862 \
                                     -iv a6b3035d08b50a0fd89a9c53cc242338
```

Task2:

```
openssl enc -aes-256-ecb -in pic_original.bmp -out encrypted_ecb.bmp -k
c6454c49829d3a098efcb2150780d862
openssl enc -aes-256-cbc -in pic_original.bmp -out encrypted_cbc.bmp -k
c6454c49829d3a098efcb2150780d862 -iv a6b3035d08b50a0fd89a9c53cc242338
dd bs=1 count=54 if=pic_original.bmp of=encrypted_ecb.bmp conv=notrunc
dd bs=1 count=54 if=pic_original.bmp of=encrypted_ecb.bmp conv=notrunc
openssl enc -aes-256-cbc -in pic_original.bmp -out encrypted_cb1c.bmp -k
c6454c49829d3a098efcb2150780d862 -iv a6b3035d08b50a0fd89a9c53cc242338
```

Task3: