Symmetric Key Encryption Lab

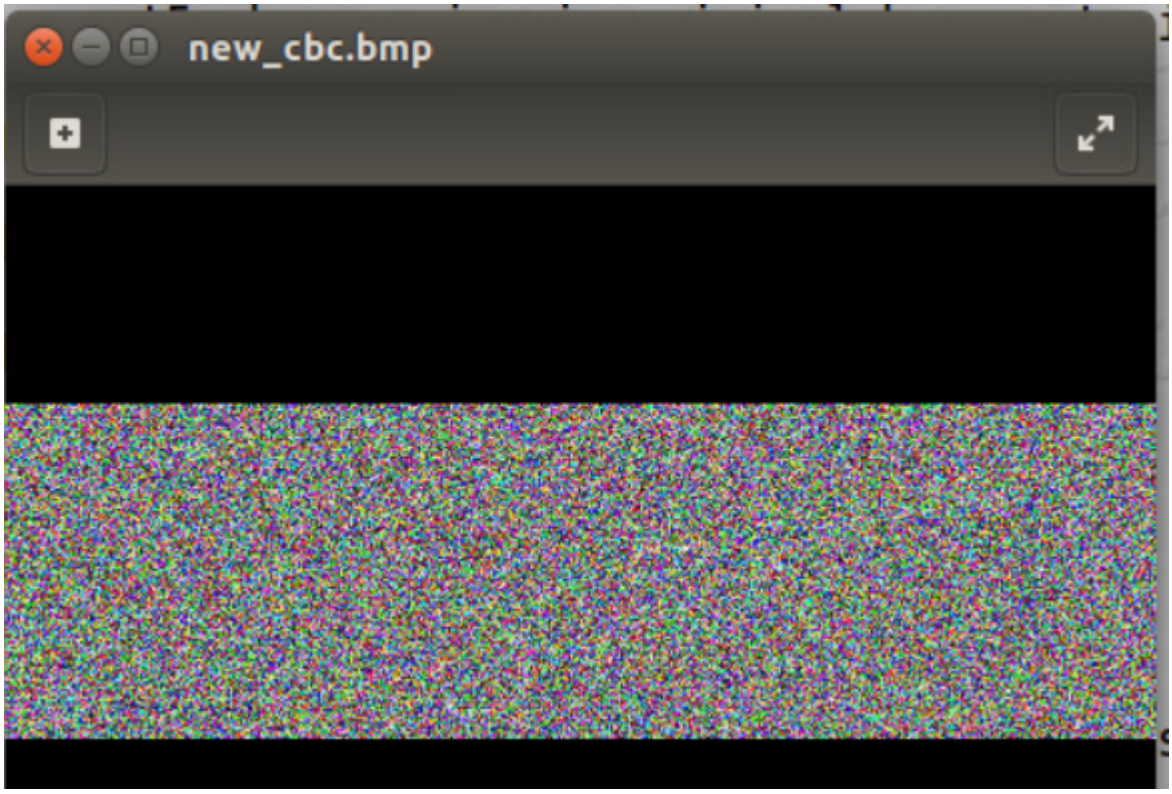
4.2 Task 1.1: Encryption Mode – ECB vs. CBC

Now we are encrypting a picture with two different ciphers.

1) ECB
2) CBC

Original picture:

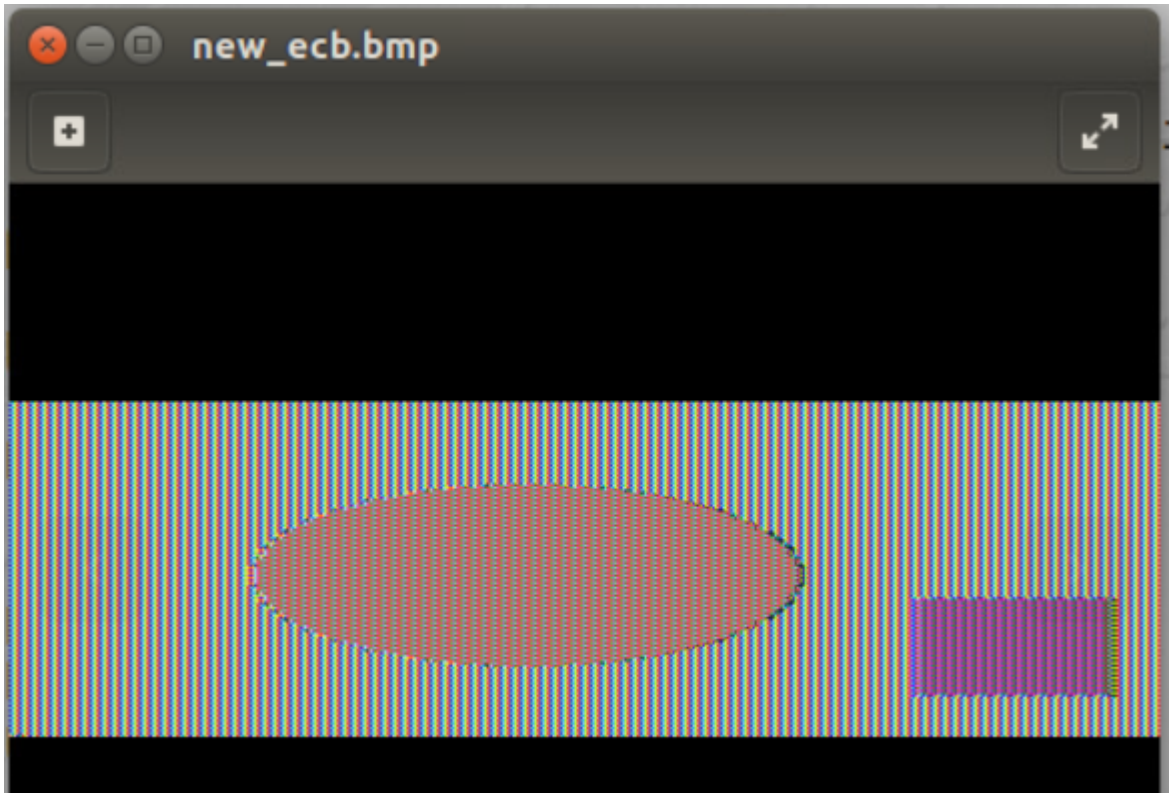
Encryption mode :- CBC:



The CBC encryption algorithm has completely changes the original file.

In this algorithm we cant derive any use full information. Because it encrypts all the byte in the picture

Encryption mode:-ECB:



In ECB the picture is similar to original picture.

We can guess this simple what the picture it was.

Yes, we can see the information here. Even it is encrypted.

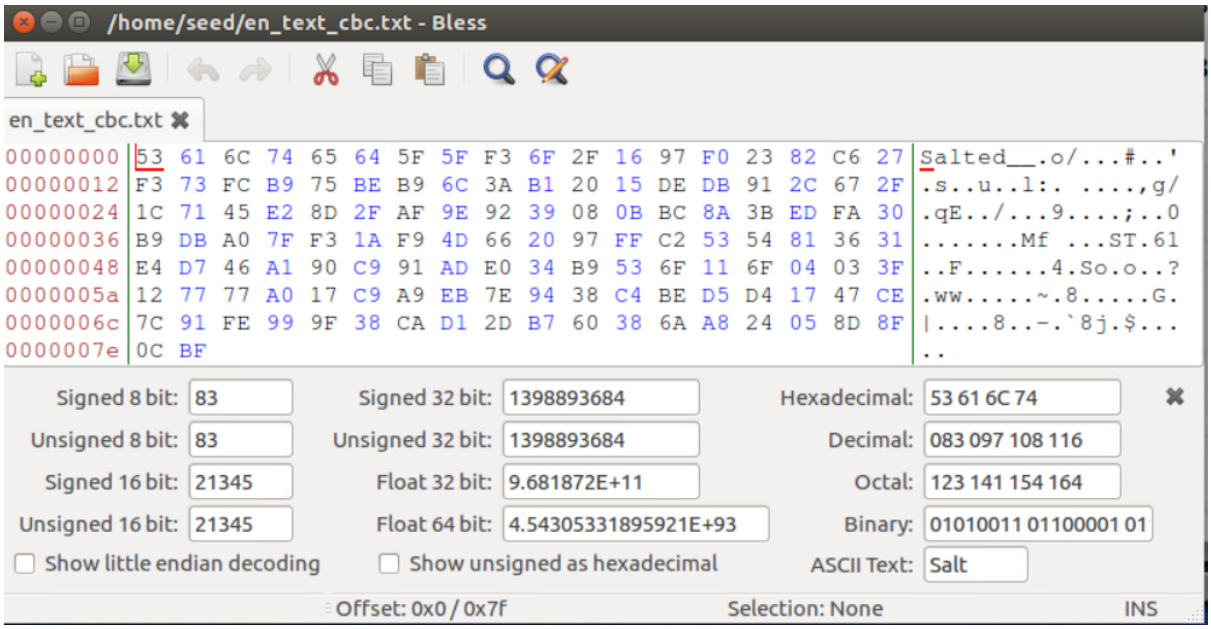
4.3 Task 2: Encryption Mode – Corrupted Cipher Text

Here first we are taking plane text file, And after encrypting the data we are in introducing an error in the 30th byte from the file in encrypted file.

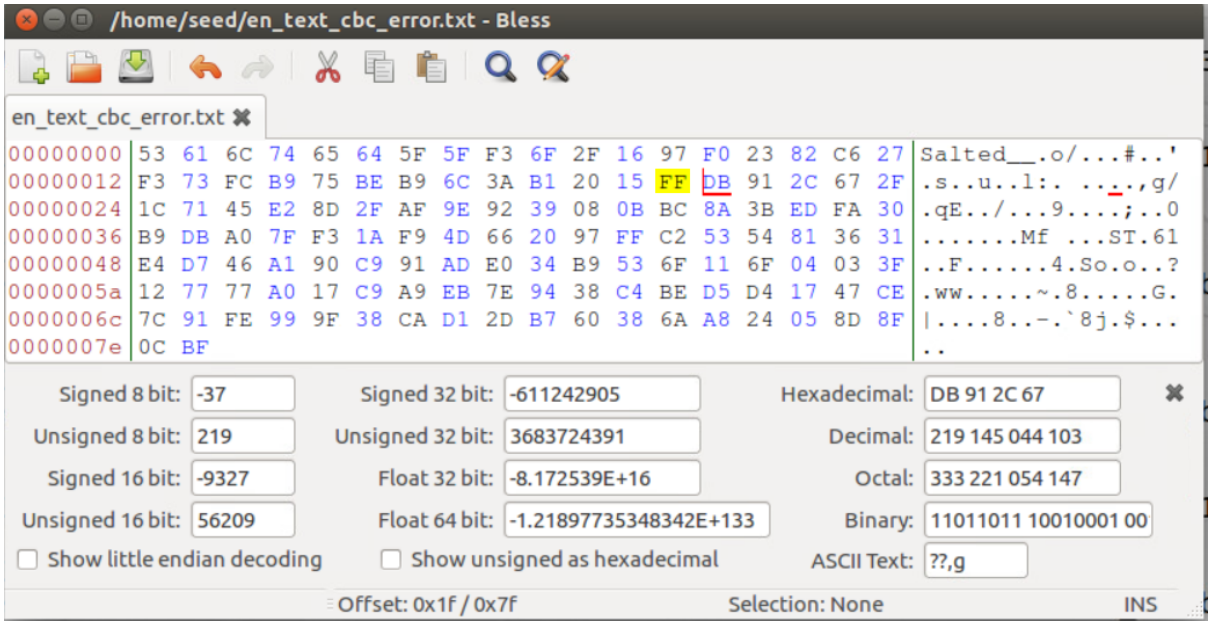
For introducing a error we are using “Bless command”

Encryption using AES-128-CBC :

Original File



Error File

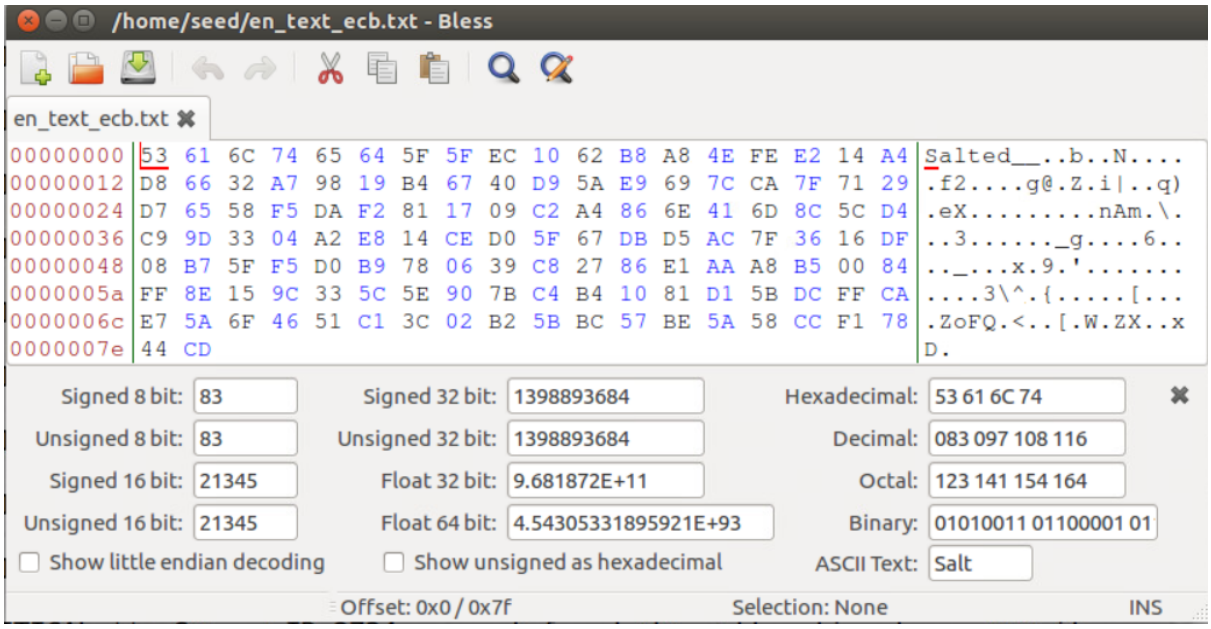


Output after corrupting 30th byte

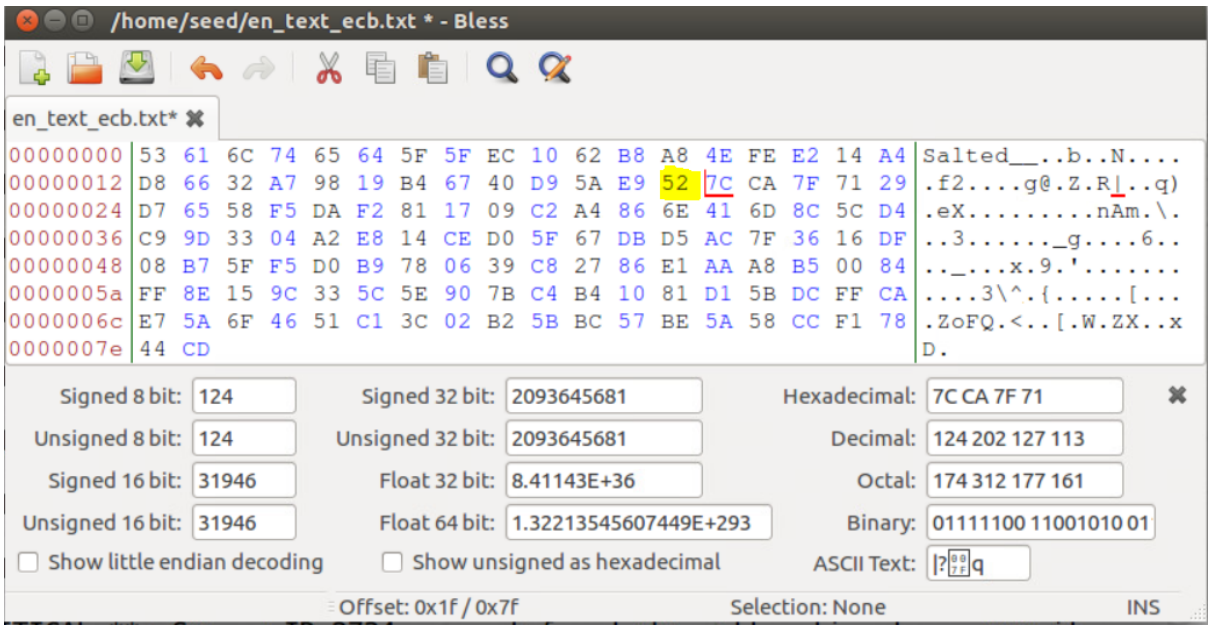
```
-@`8j@$@@[09/05/21]seed@SEED:~$ cat de_text_cbc_error.txt
@@@4`@  D@Z$@u@ ssignment and Uhis is Lakshmi Sai Tejaswi Pathuri. I'm from wichita state university.
```

Encryption using AES-128-ECB

Original File



Error File



Output after corrupting 30th byte

```
5/21]seed@SEED:~$ cat de_text_ecb_error.txt
[illegible]Gssignment and this is Lakshmi Sai Tejaswi Pathuri. I'm from wichita state university.
```

DELIVERABLES FOR “ECB “AND “CBC”

ECB

- Here in ECB, I can derive the information from 30th byte
- ECB is basic encryption, but the date can be guessed easily.
- ECB encrypt the data by byte by byte

CBC

- Here in CBC, I can derive the information from 30th byte and in the middle, there is a word corrupted
- CBC is advabce level encryption, it is very hard to guess the data
- CBC encrpt the data with reference to previous encrypted information.