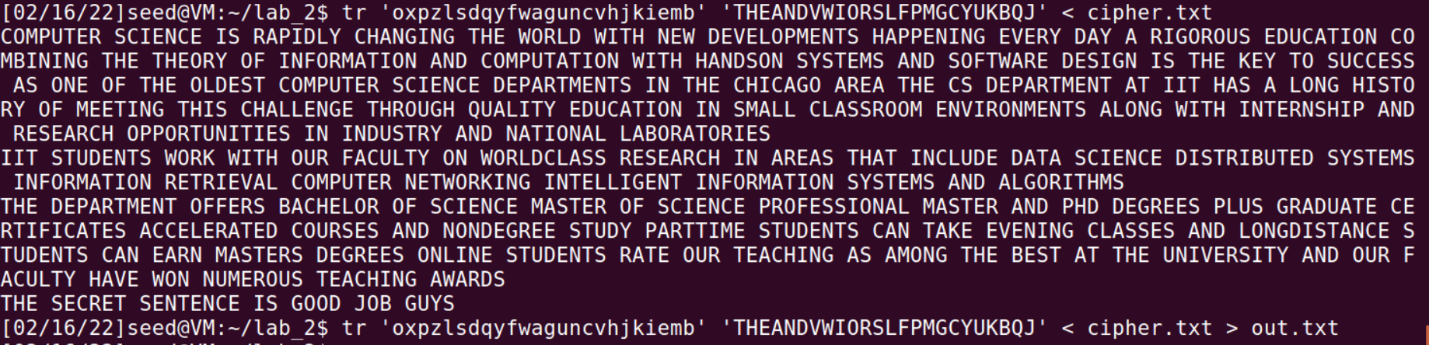
**Introduction to Information Security**

**LAB 2**

**Contents:**

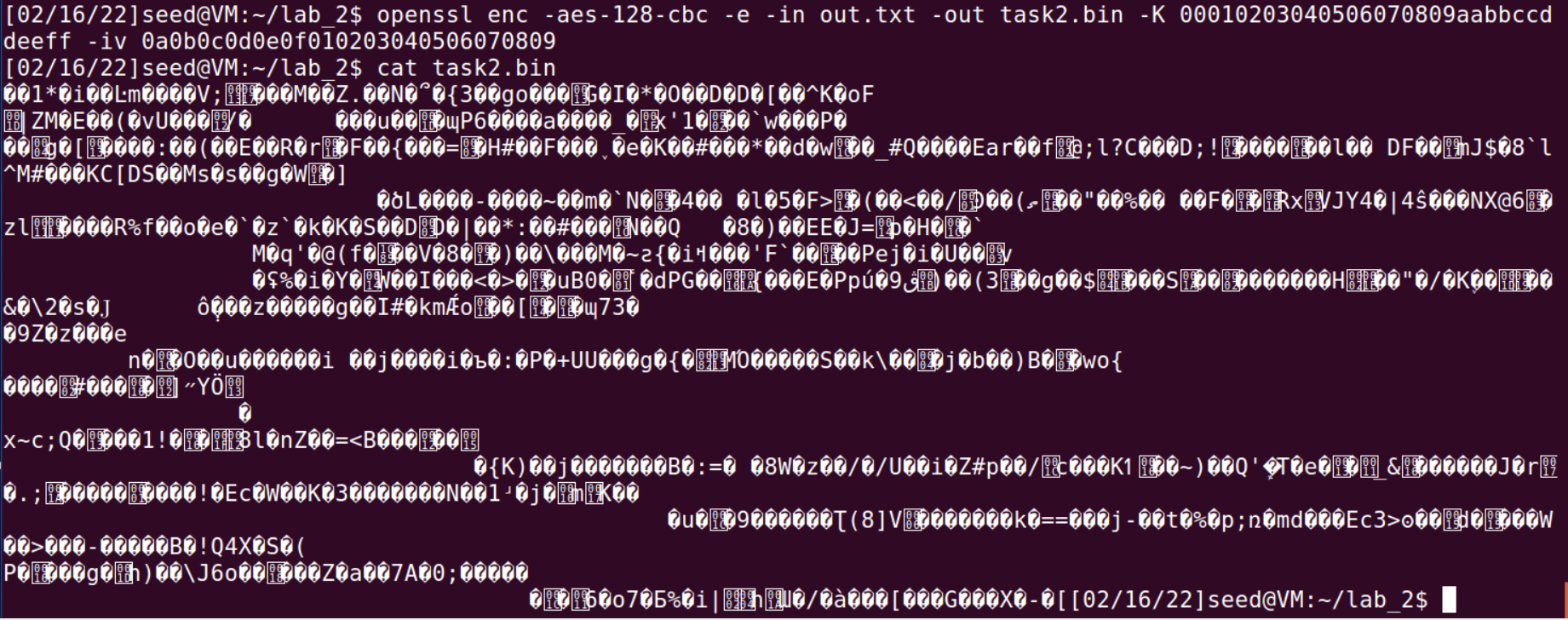
|  |  |  |
| --- | --- | --- |
| S.No. | Title | Page. No |
| 1 | Task 1: Frequency Analysis | 3 |
| 2 | Task 2: Encryption using Different Ciphers and Modes | 3 |
| 3 | Task 3: Encryption Mode – ECB vs. CBC | 5 |
| 4 | Task 4: Padding | 6 |
| 5 | Task 5: Error Propagation – Corrupted Cipher Text | 7 |
| 6 | Task 6.1: Uniqueness of the IV | 8 |
| 7 | Task 6.2: Common Mistake: Use the Same IV | 9 |
| 8 | Task 6.3: Common Mistake: Use a Predictable IV | 10 |

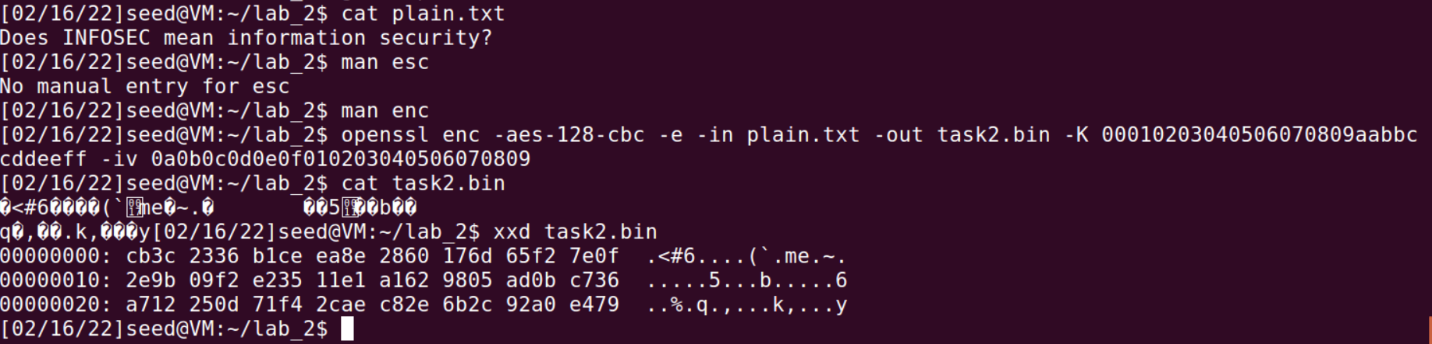
**Task 1: Frequency Analysis**

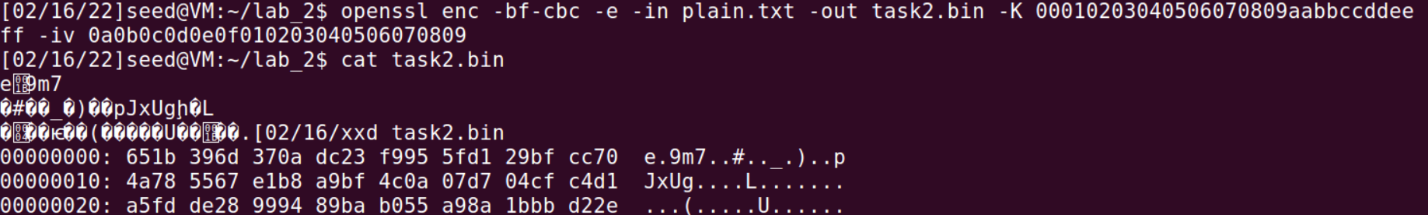
****

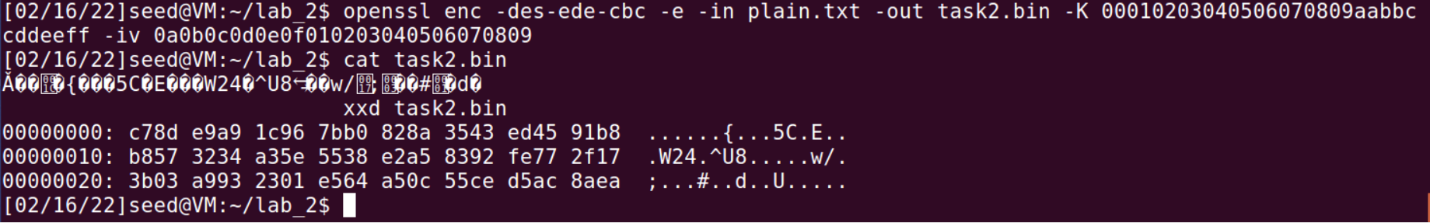
I first checked for maximum occurring three letter words and substituted them for ‘The’ & ‘And’ and went on filling for rest of them. I also noticed that it was easy to predict words if at least two or three letters were known.

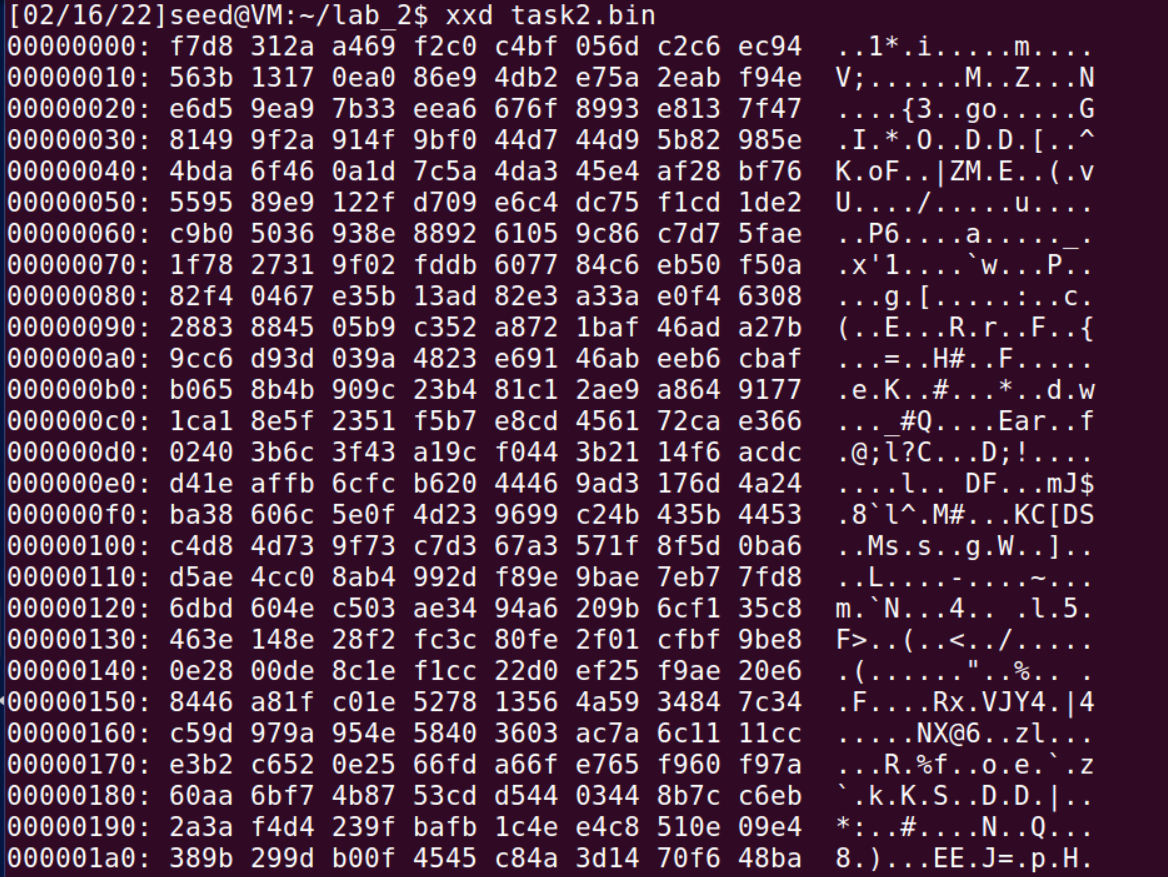
**Task 2: Encryption using Different Ciphers and Modes**

Output with CBC****

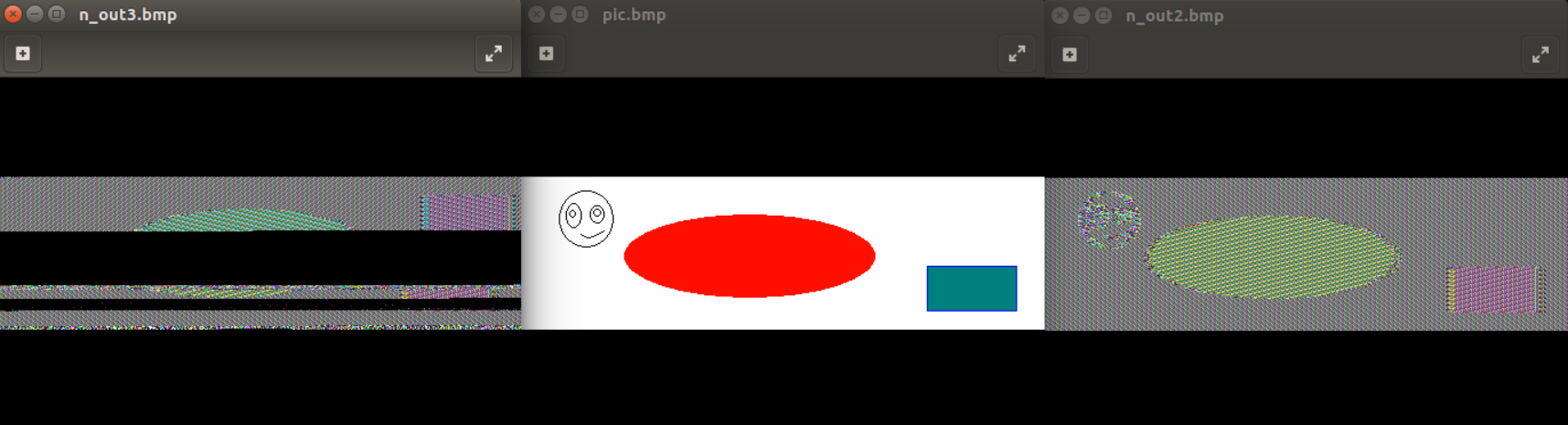
I used the sentence “Does INFOSEC mean infromation security?” encoded it using the given key and iv 

Hexa devimal output with -bf-cbc

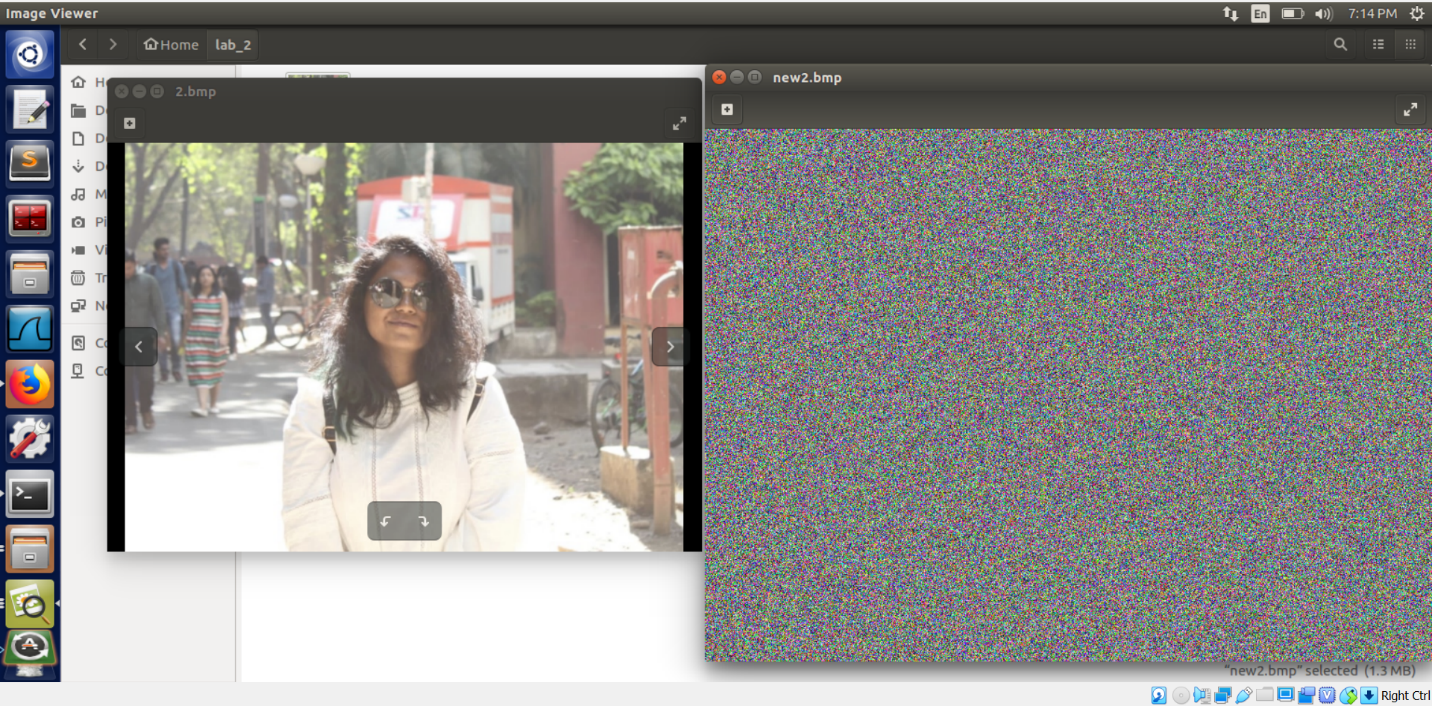
Output with des-ede-cbc

Hexadecimal output with -aes-128-cfb 

Observation: Different ciphertypes produce different cip[her text pf different lengths and characters.

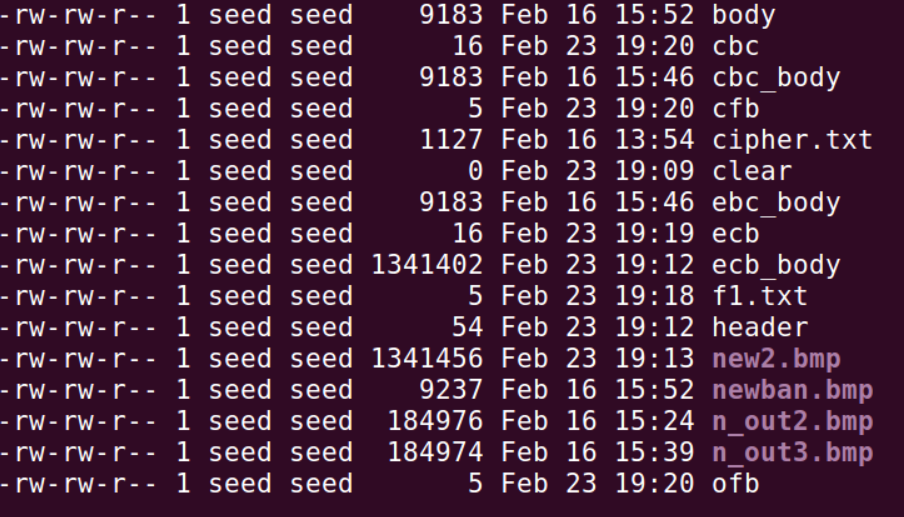
**Task 3: Encryption Mode – ECB vs. CBC**

The one on the left is output with CBC whereas the right is ECB. It can be observed that CBC is slightly better.



This is my picture on the left and CBC encryption on the right. We can’t make out shapes or even an outline of the main image form the encrypted one.

**Task 4: Padding**

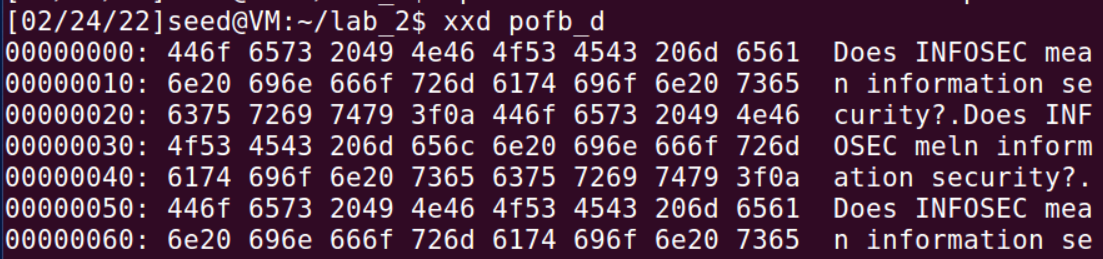
****

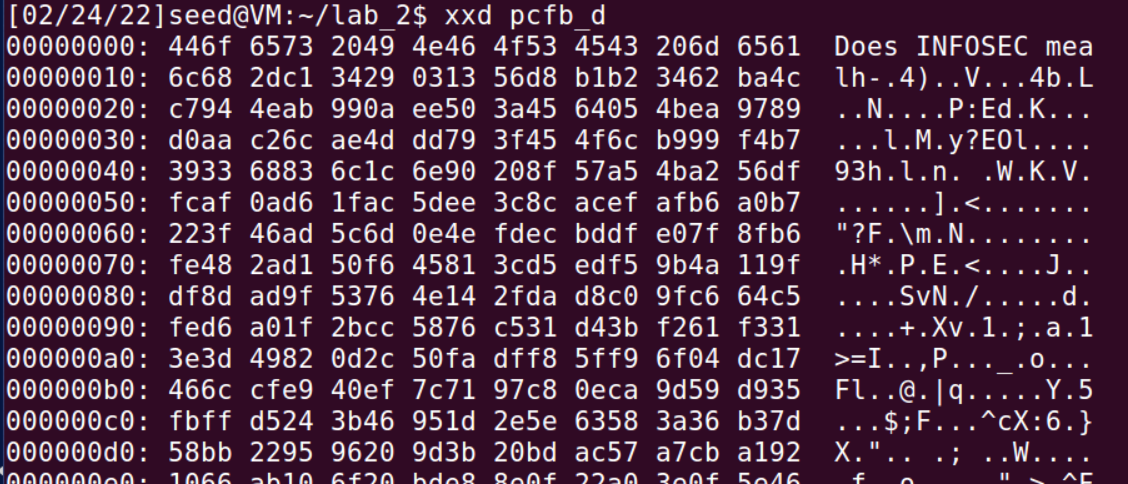
From the highlighted blue circles, we can say that both cbc and ecb has size of 16 whereas cfb and ofb has size of 5, so no padding is needed in cfb and ofb as they are stream ciphers while padding is done in cbc and ecb as they are block ciphers.

**Task 5: Error Propagation – Corrupted Cipher Text**

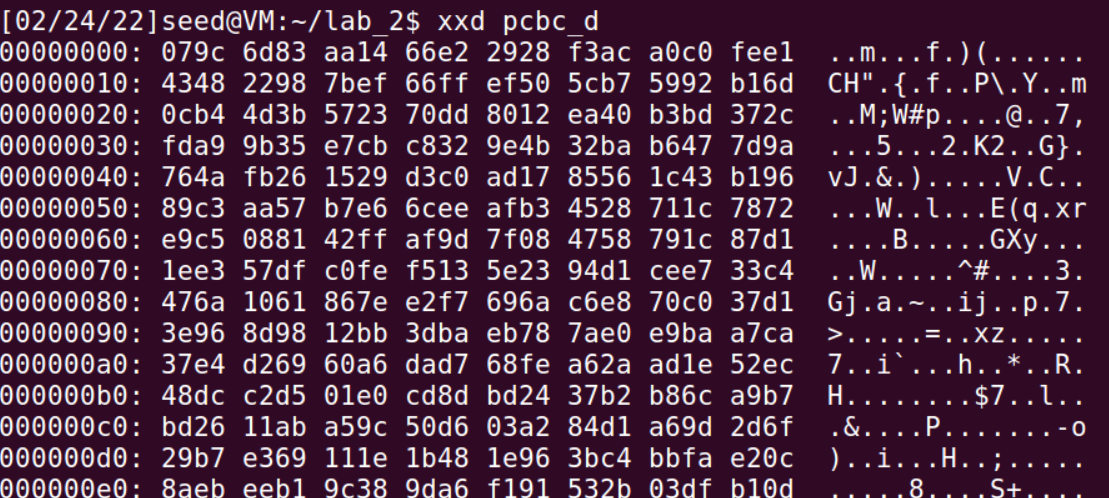
Prediction before experiment: I think after the corruption, OFC should be able to retain everything while in the other three, all information will be lost.

Information retained after ofb: Everything

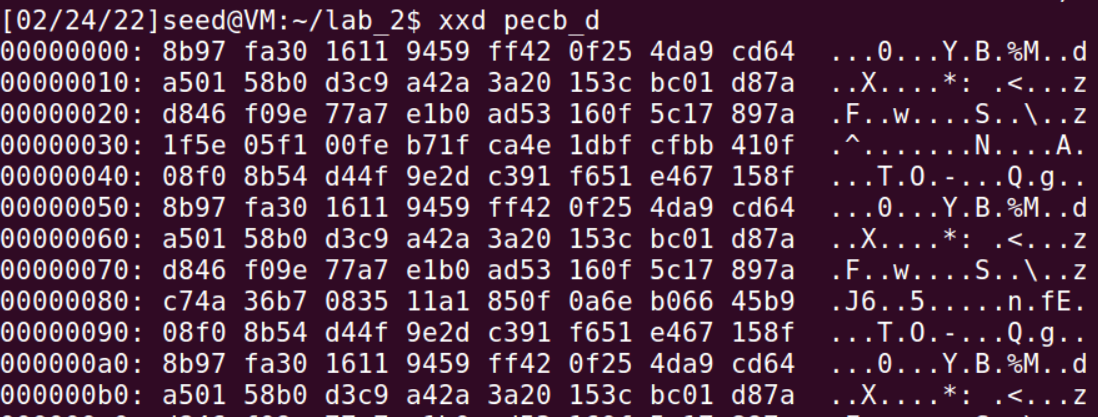


Information retained after cfb: Everything until the bit that was corrupted. ****

Information retained after cbc: None

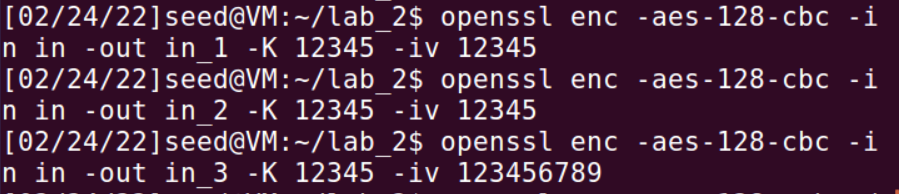


Information retained after ecb: None

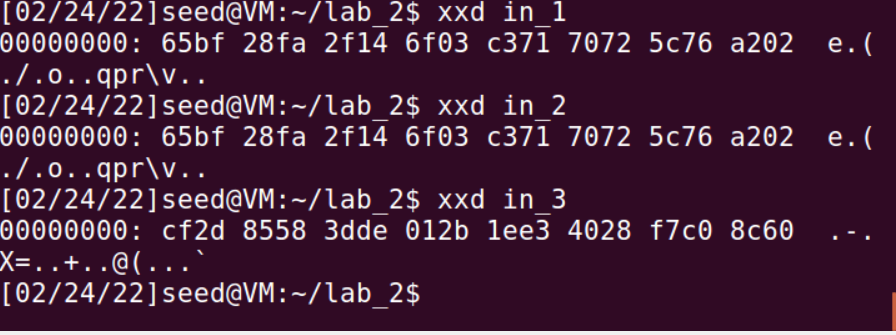


**Task 6.1. Uniqueness of the IV**

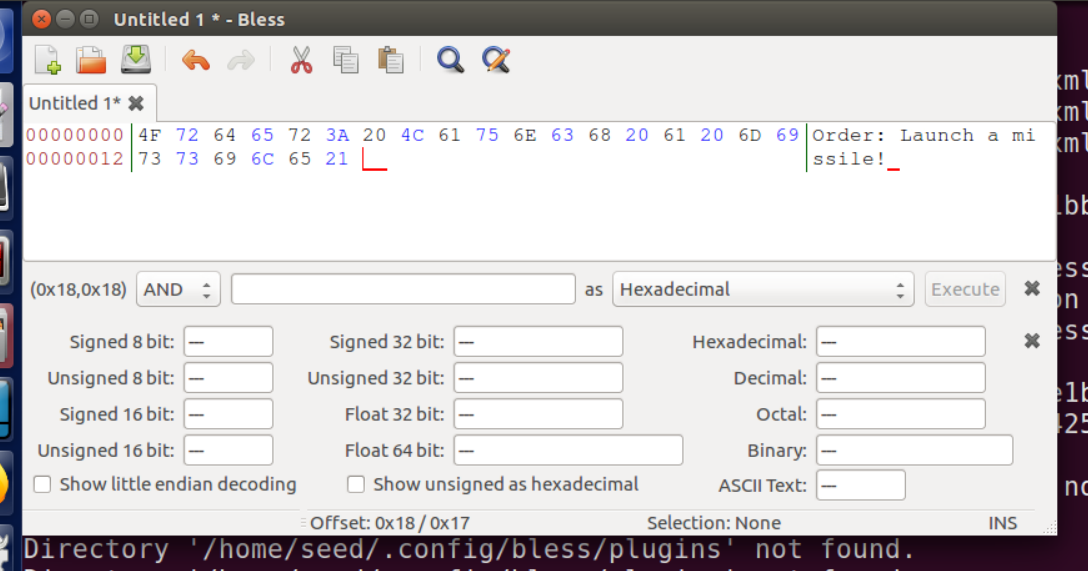
Encrypting 2 files with the same Key and IV and changing the third IV



Observation: Same IVs produce same encryption. Hence IVs should be changed and shouldn’t be predictable.



**Task 6.2. Common Mistake: Use the Same IV**

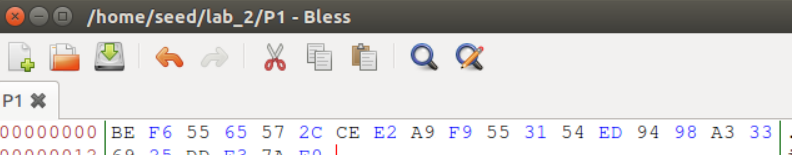
****

P2 can be completely revealed with the given information.

**Task 6.3. Common Mistake: Use a Predictable IV**

I started out with the assumption that the message is ‘yes’ then I did XOR of all the known Hex values. If the resultant is the same then the message was yes. If it doesn’t match, then it’s no,

Luckily, it was yes and it worked.



The first few bits match exactly to the cipher text of P1, which confirms that the message was yes.