**ITSEC**

**LAB REPORT: 1**



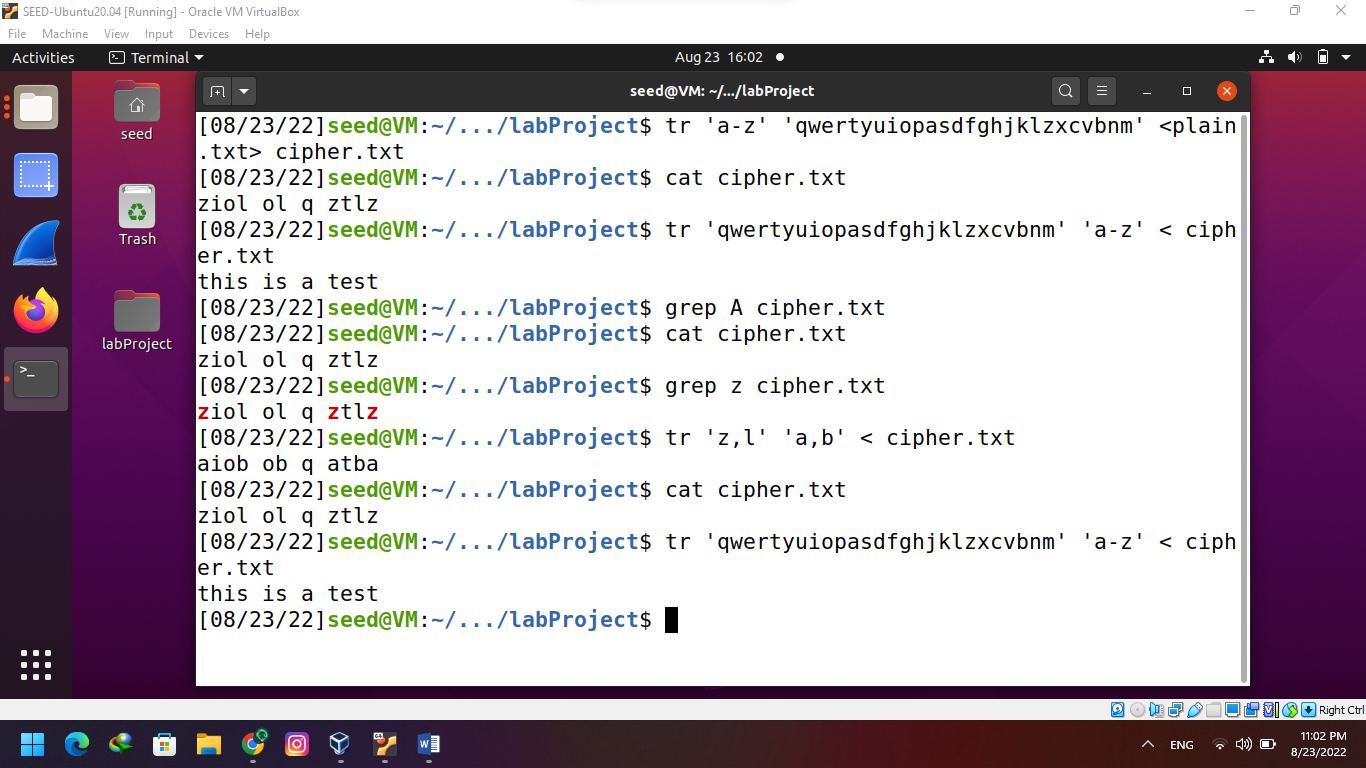
**BY – AMANUEL LEGESSE SOFTWARE ENG. EXT**

**ID – ATE/3628/1**

Secret-Key Encryption Lab

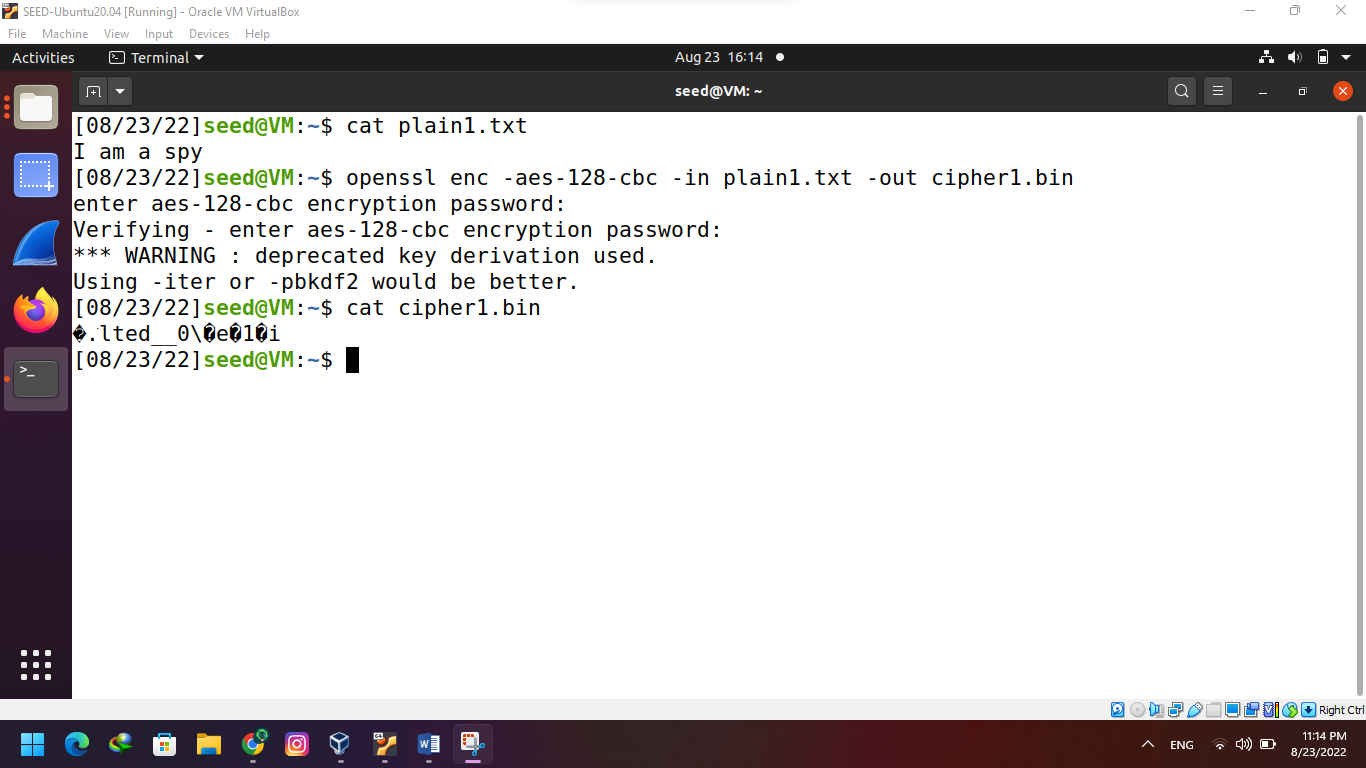
**TASK 1: Frequency analysis**

* In the first task lab exercise I used monolithic ciphering which encrypts every letter with a given one. As seen in the figure below I used frequency analysis to find the original text



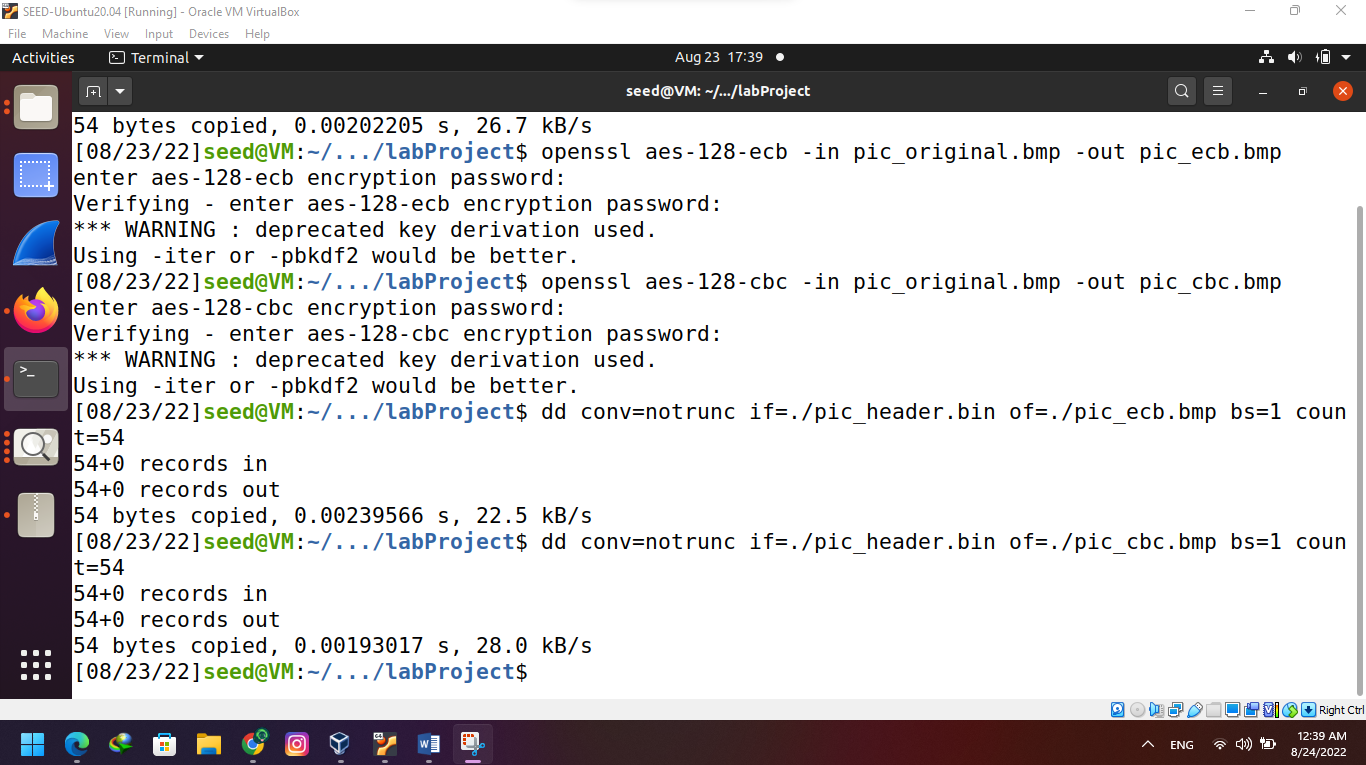
**Task 2: Encryption using Different Ciphers and Modes**

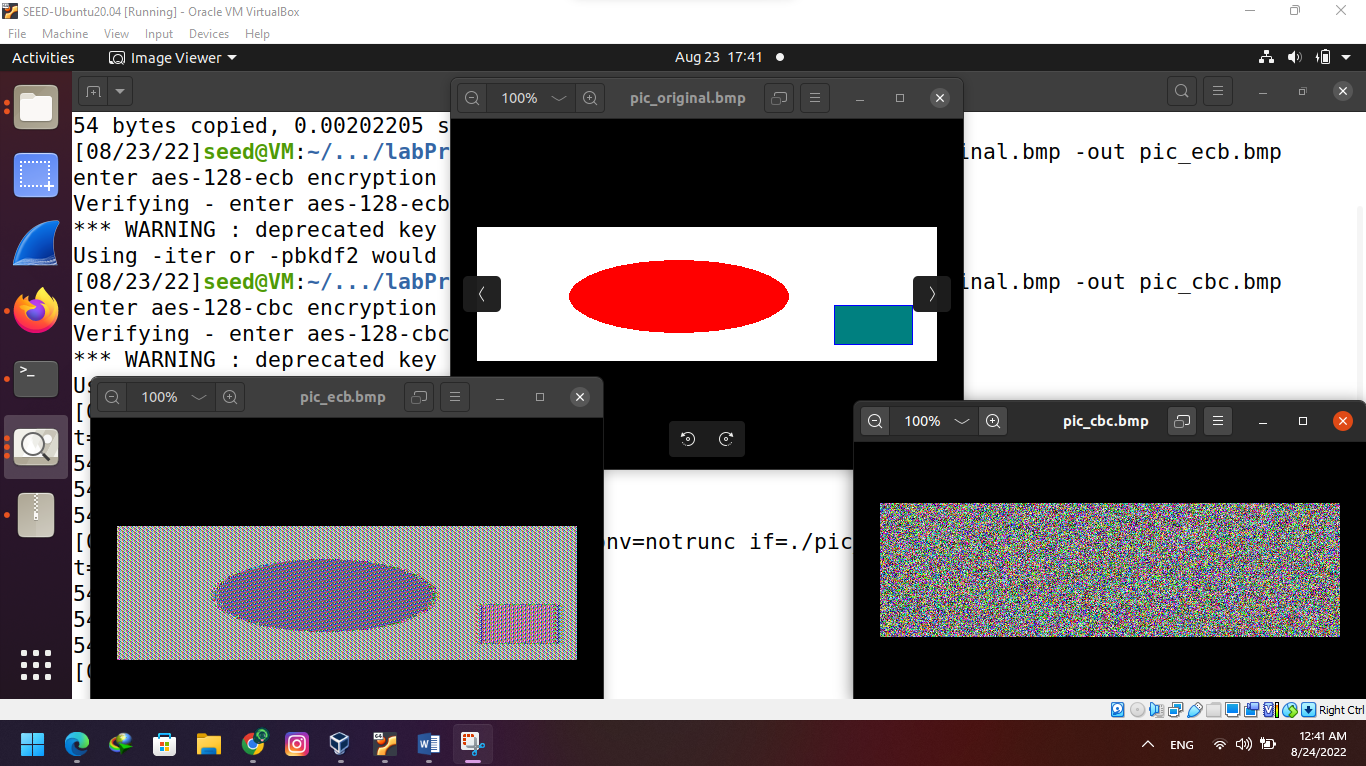
* I created a plain1.txt file to encrypt using the command ‘openssl enc’ command and –aes-128-cbc for size of the key and encryption mode. I put the output in a binary file.
* The system uses an encryption password after it verifies it will encrypt the letters. By using the ‘xxd’ command I was able to see the hexa decimal encryption.

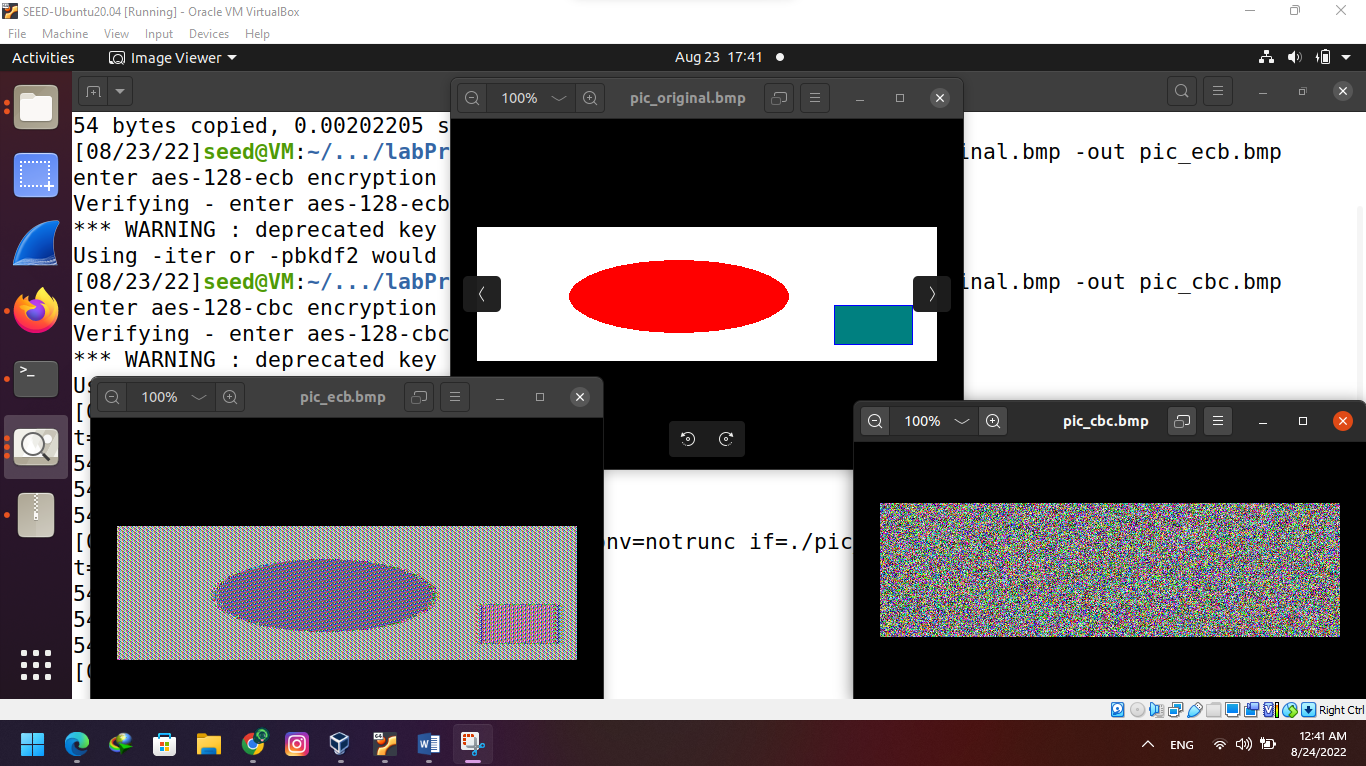


Task 3: Encryption Mode – ECB vs. CBC

* Instead of using the instructions given in the lab I decided to extract the file header first in 54 bytes from the pic\_original.bmp



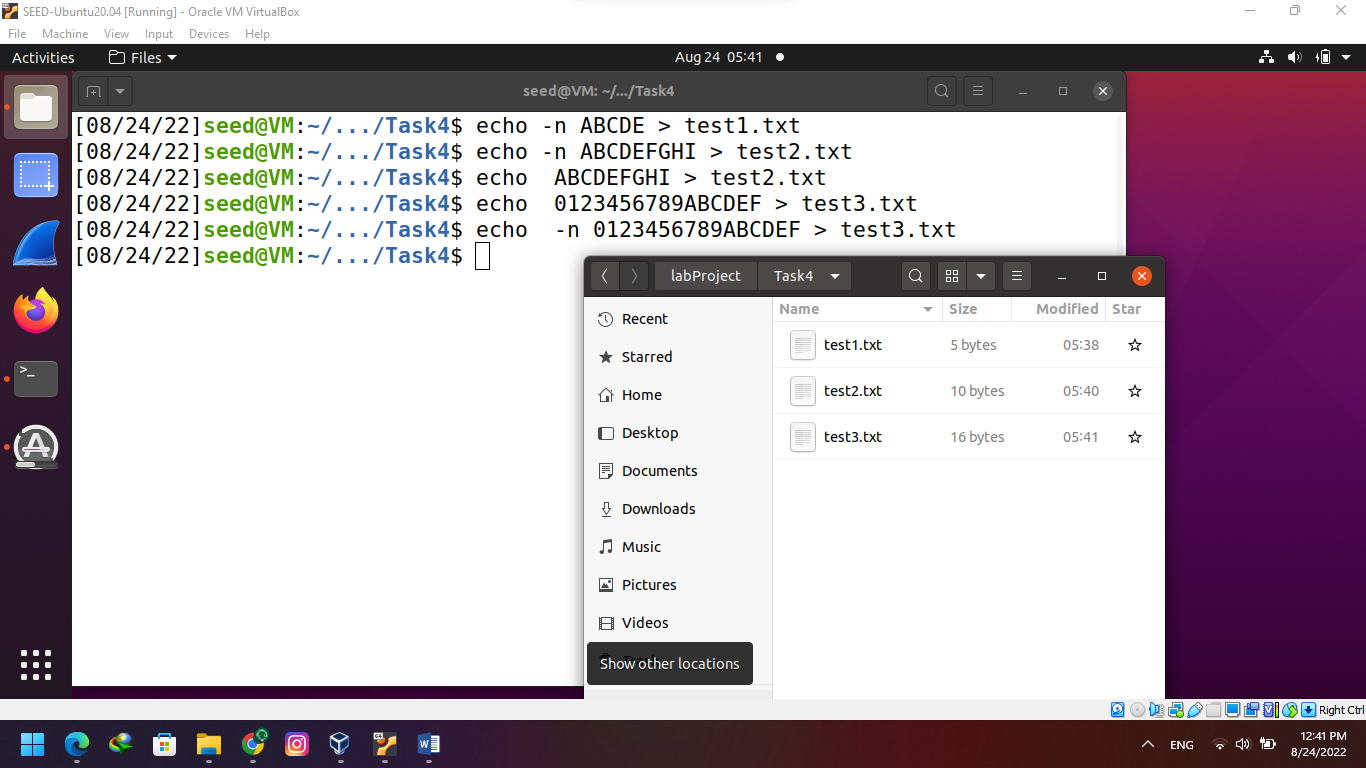




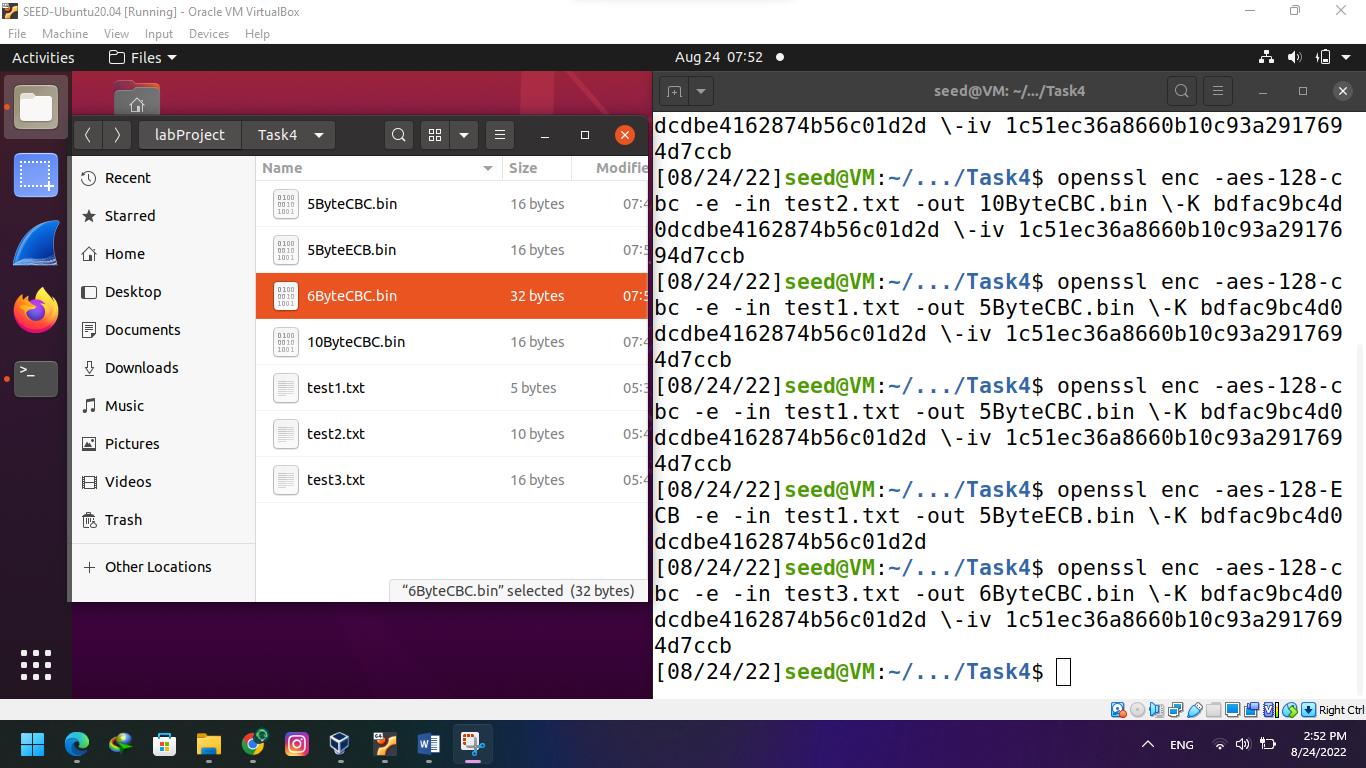
* As seen in the screen shot the encryption in CBC is better than ECB.

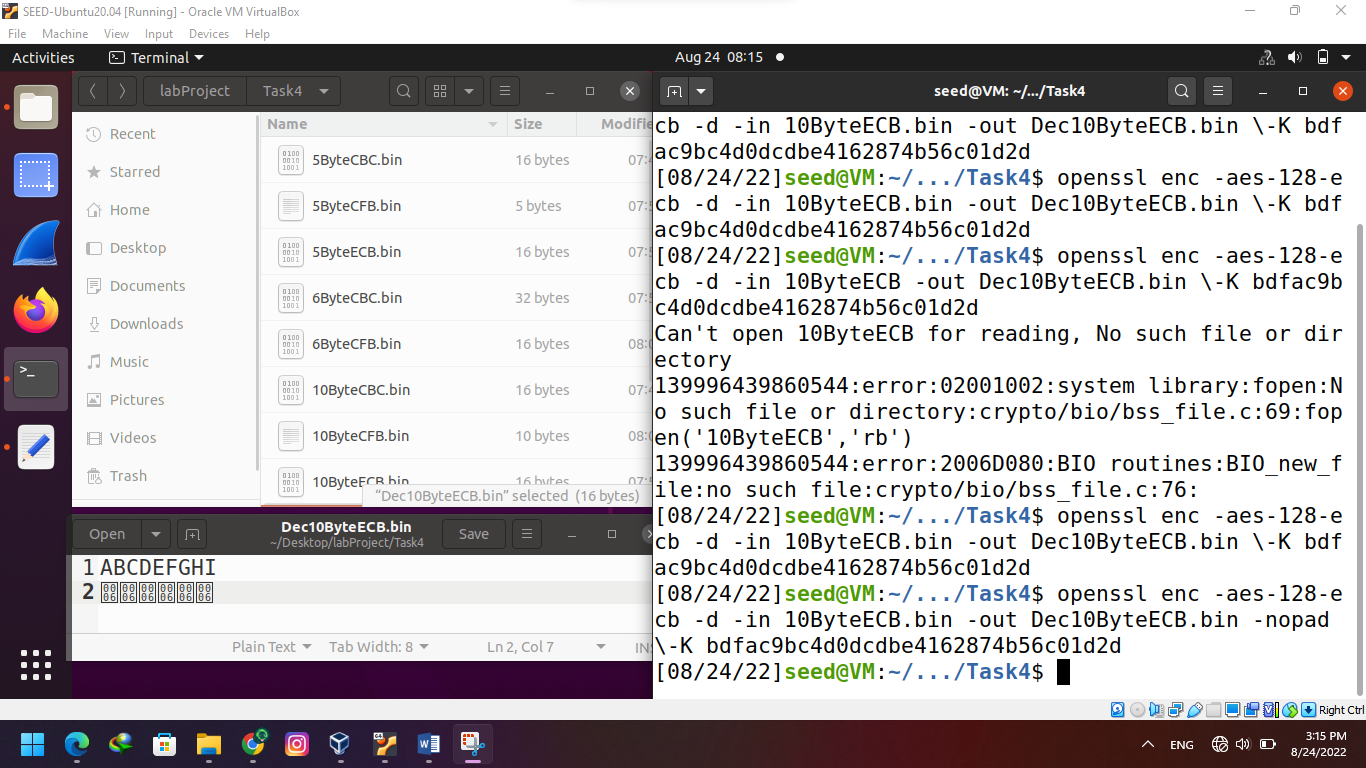
Task 4: Padding

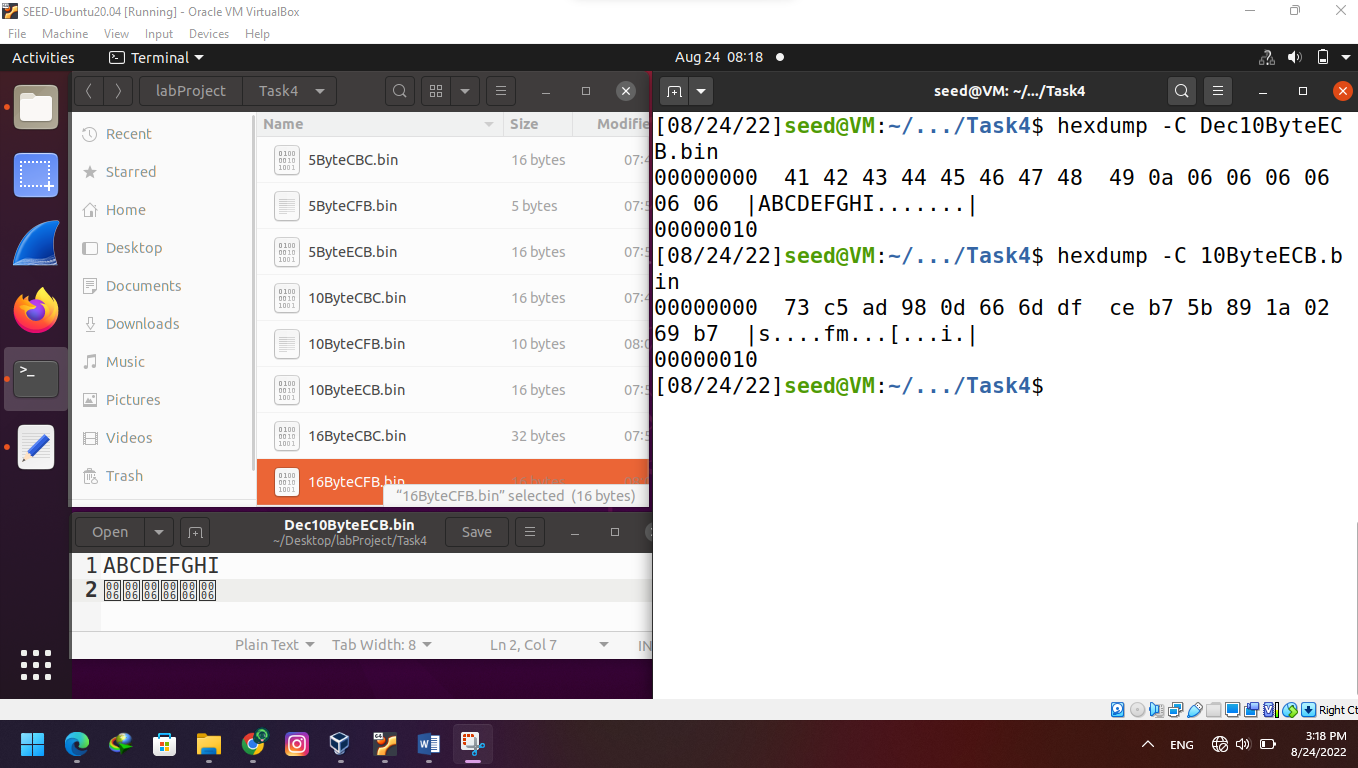
* I created a 20 and a 30 byte file then encrypted them to compare and see where padding was used

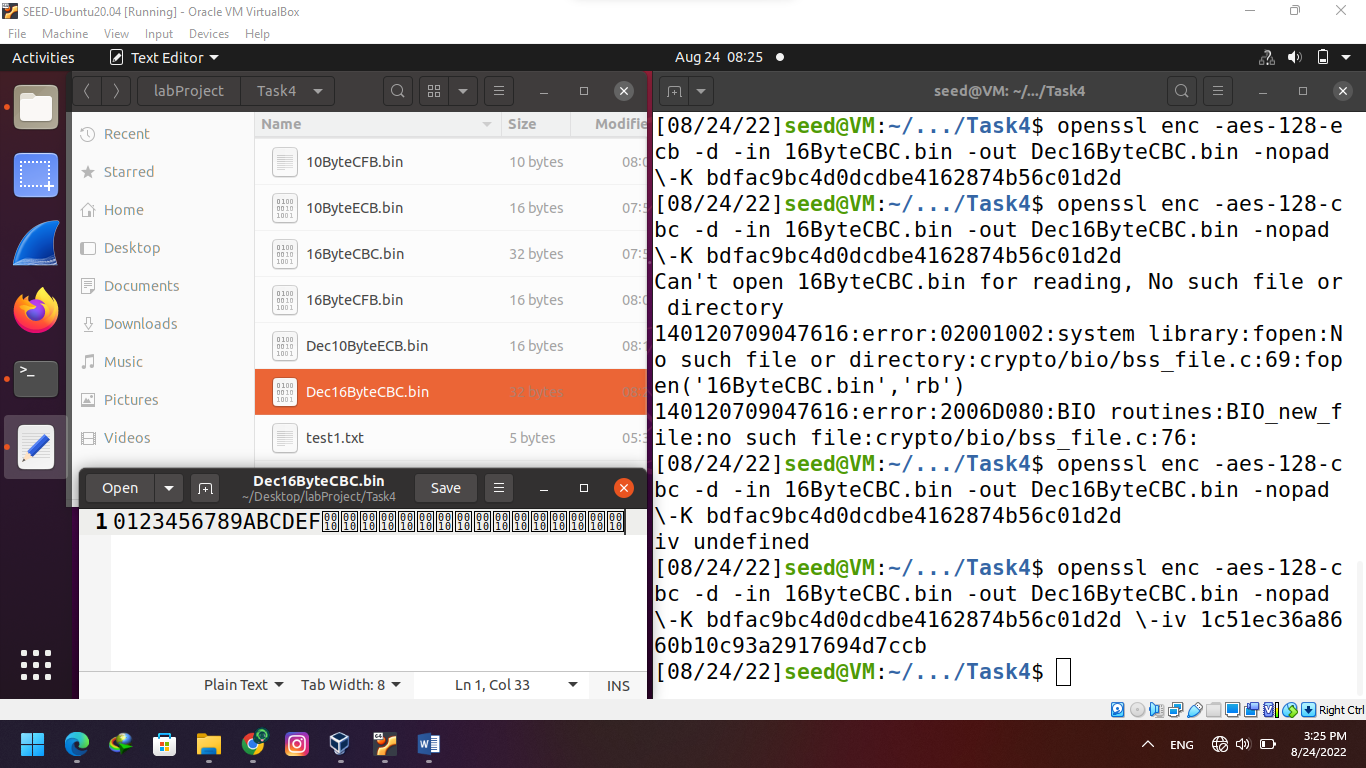


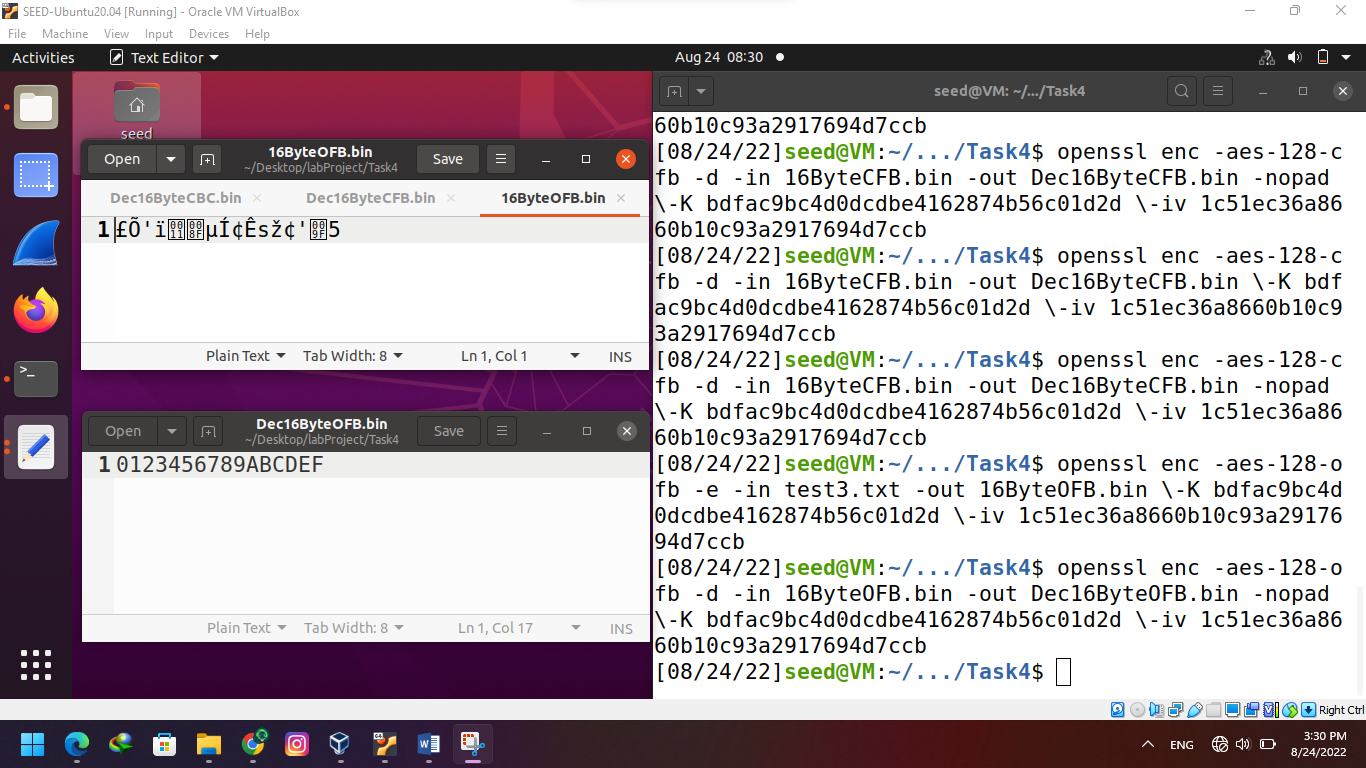
* Padding is needed for ECB and CBC encryption modes because their inputs contain number of blocks, thus padding could ensure that. Block size depends on the algorithm: AES uses 16 byte blocks while Blowfish and 3DES use 8-byte blocks.







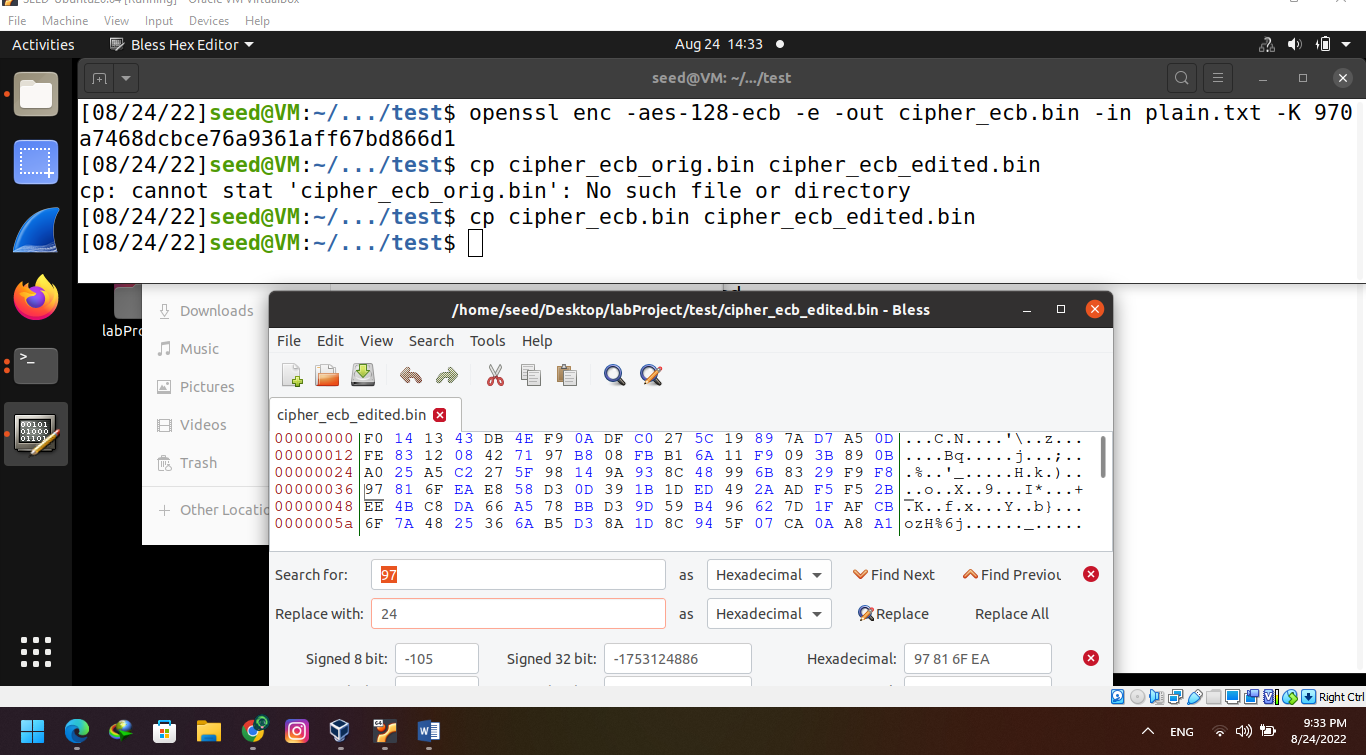


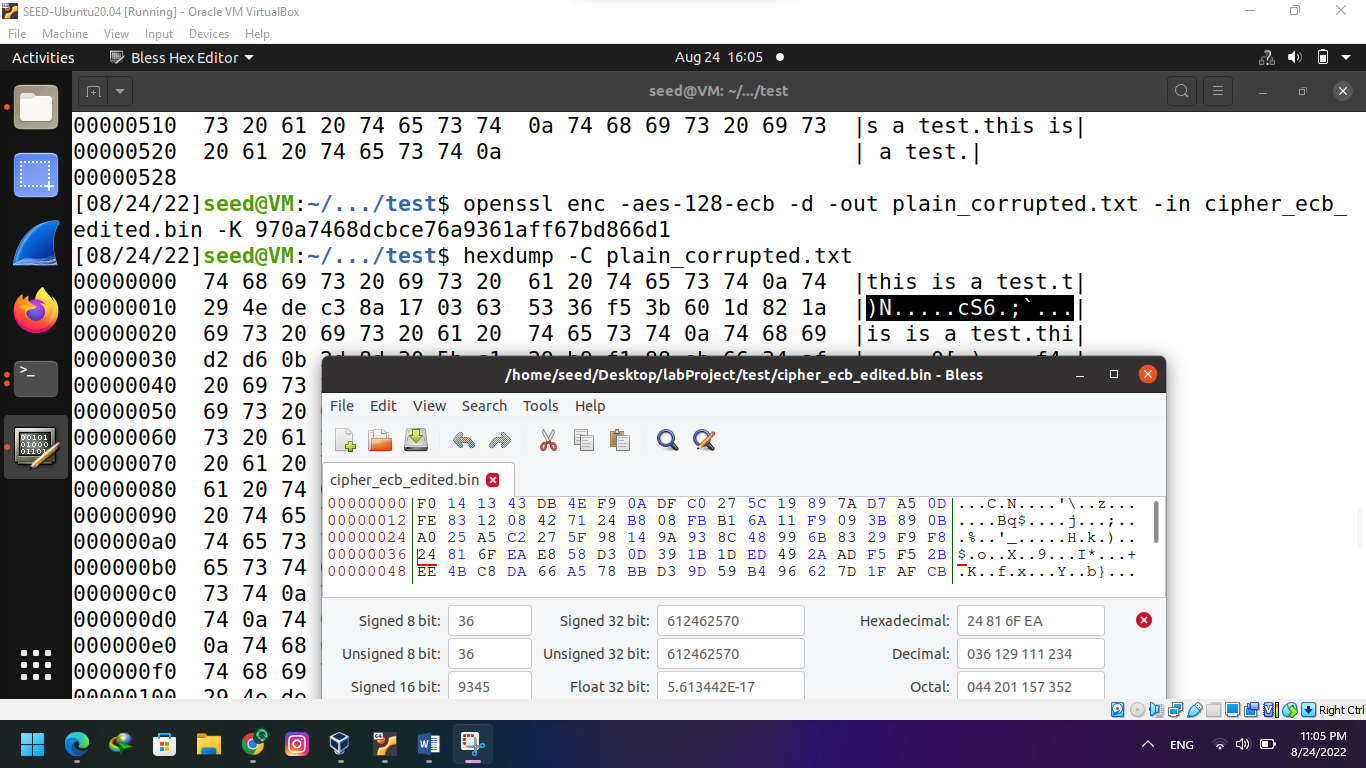


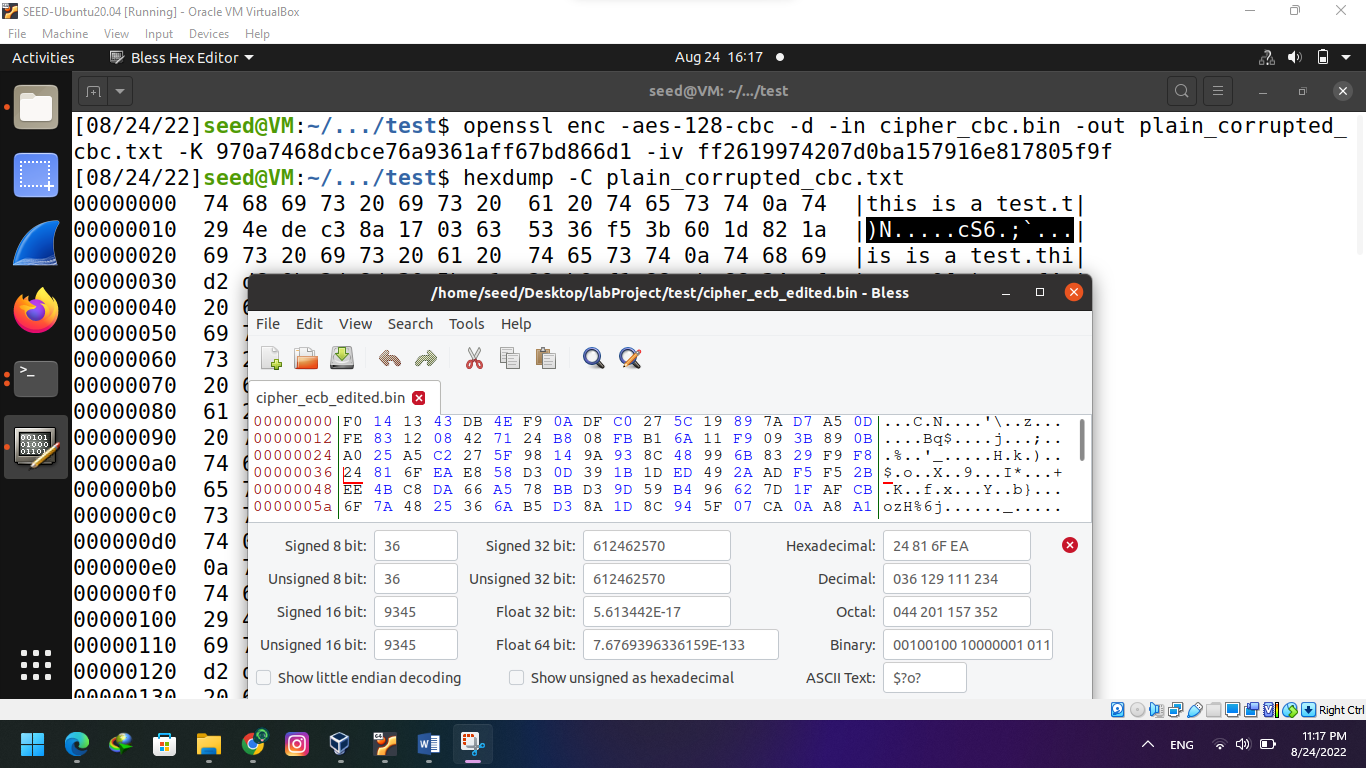
* There is no need padding for encryption mode CFB and OFB because they are stream ciphers, in which the size of the block is usually fixed (one character).

Task 5: Error Propagation – Corrupted Cipher Text

* I replaced the 55th byte in all encrypted files with “$” to corrupt the cipher. I feel that in the: ECB mode, 1 block of data would be corrupted CBC mode, 2 blocks of data would be corrupted OFB mode, 1 block of data would be corrupted CFB mode, the entire data after the corrupt block should be corrupted



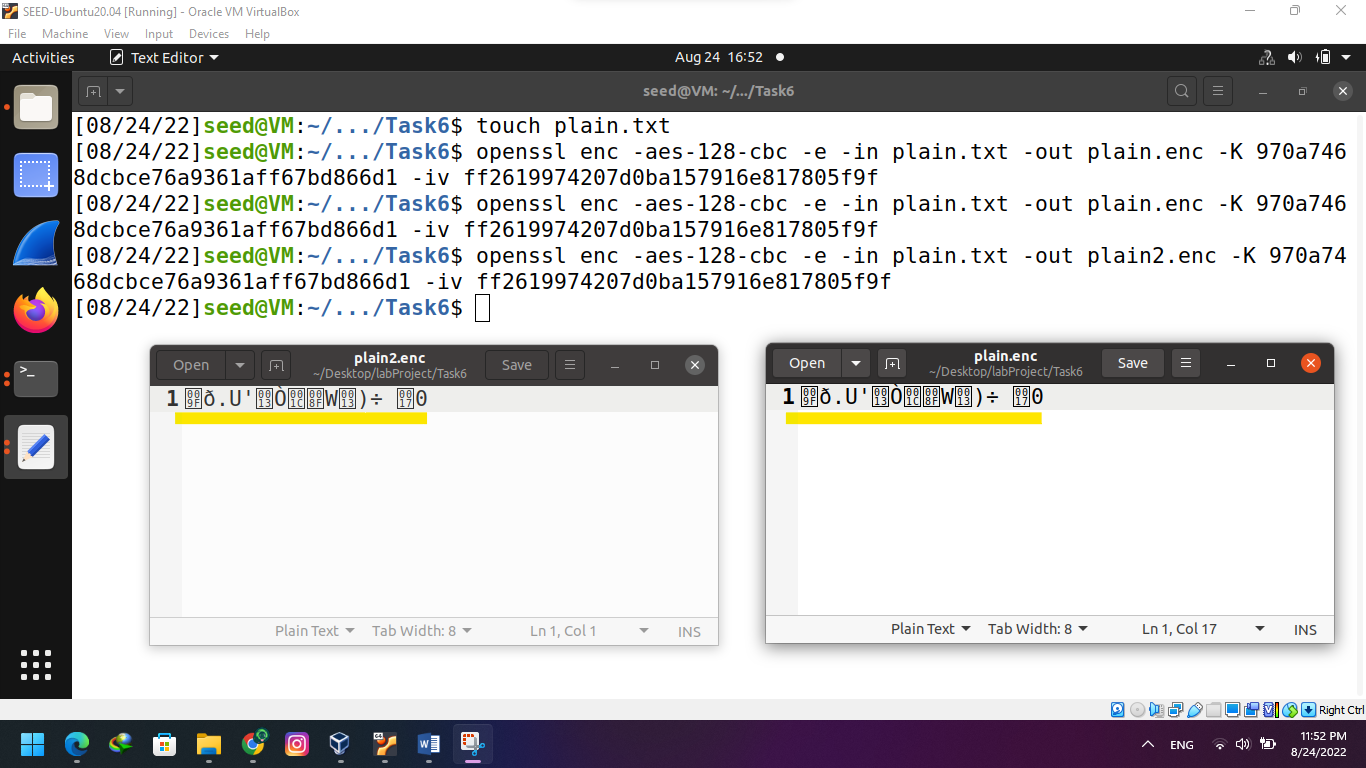




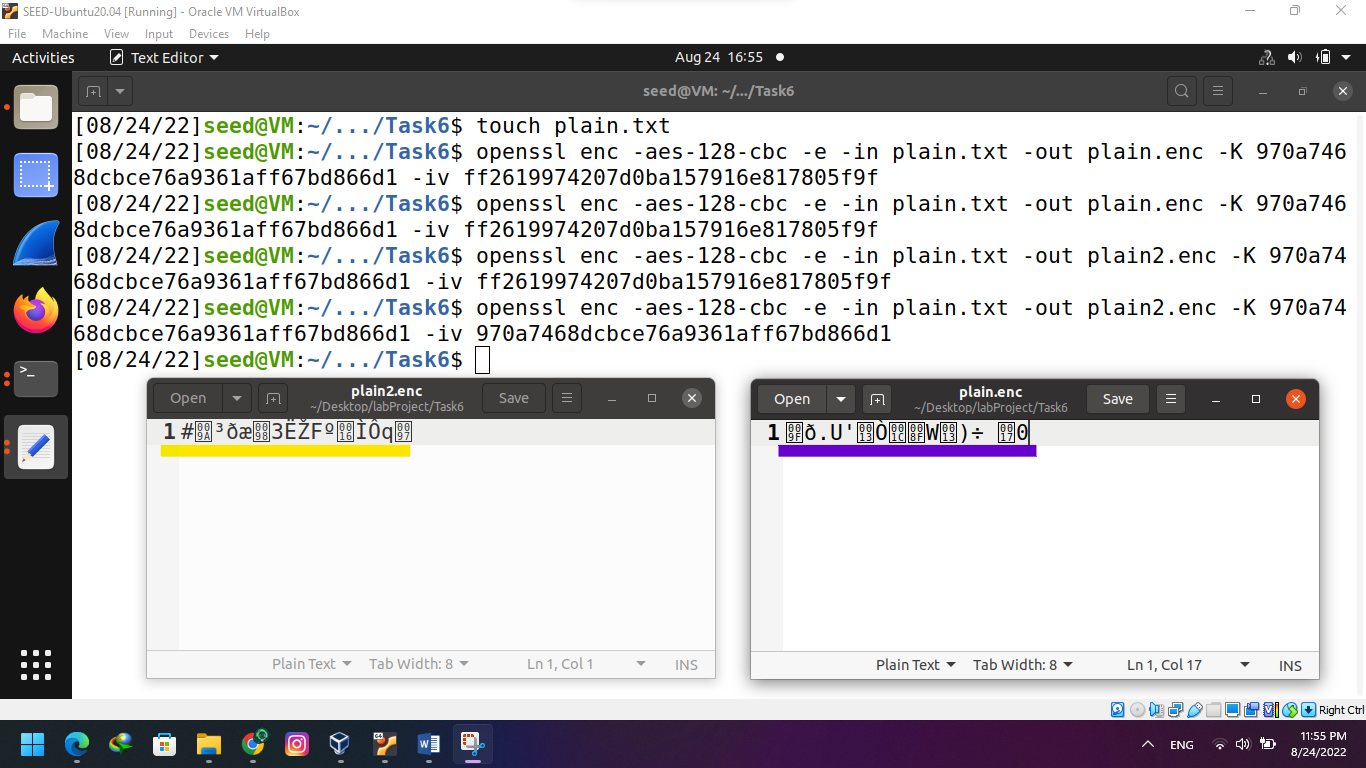
Task 6: Initial Vector (IV) and Common Mistakes

**6.1: IV Experiment:**

* Using the same IV twice on the same plaintext file resulted in and identical output for the encryption.

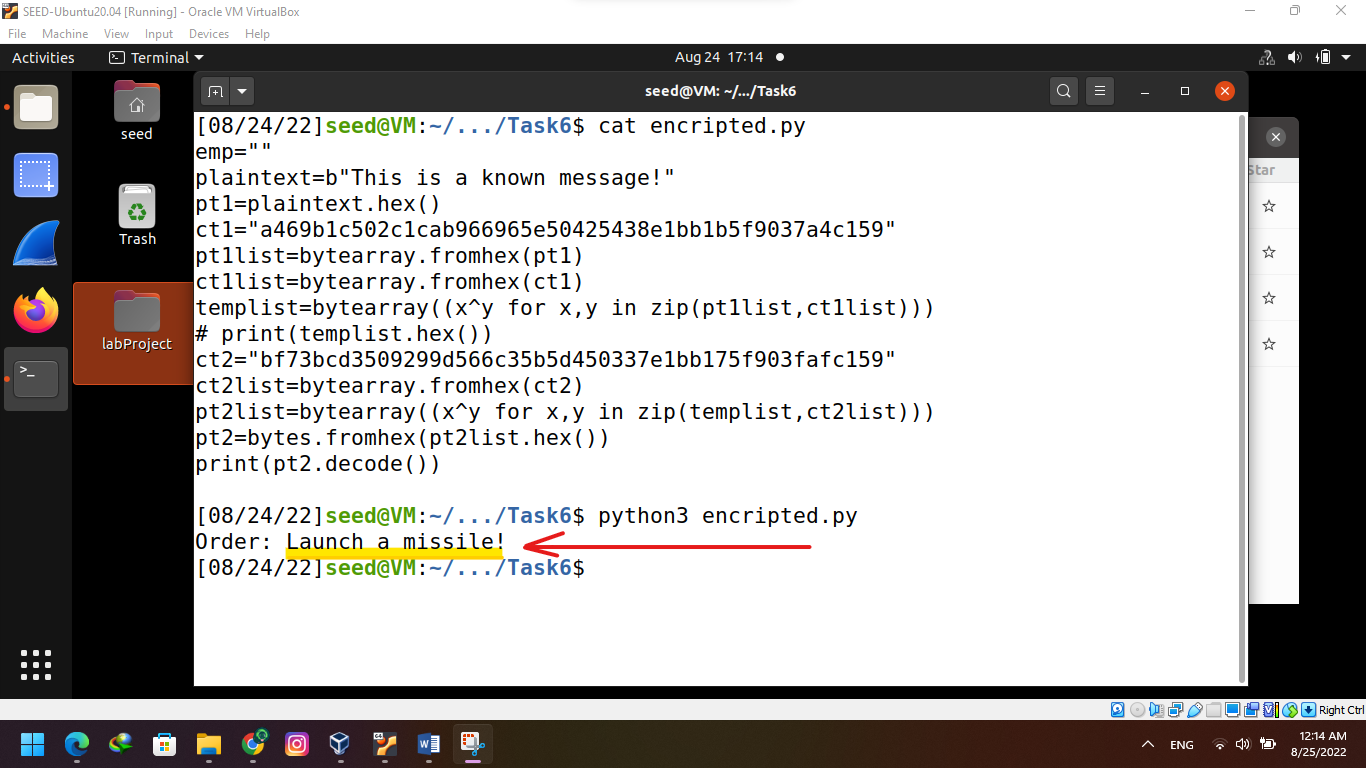


* With different IVs the encryption results were completely different



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

* Output: Order: Launch a missile! In the OFB mode, it is essential to change the IV for every plaintext. If the encryption mode was changed to CFB, only 1 block of the ciphertext would be recovered since the ciphertext would then be passed as the IV for the second block and would still require the key to actually decrypt it



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

* The generated input is passed as plaintext to the encryption. If the new ciphertext matches the old ciphertext then the old plaintext was “Yes”, if it is different then the old plaintext was “No”

