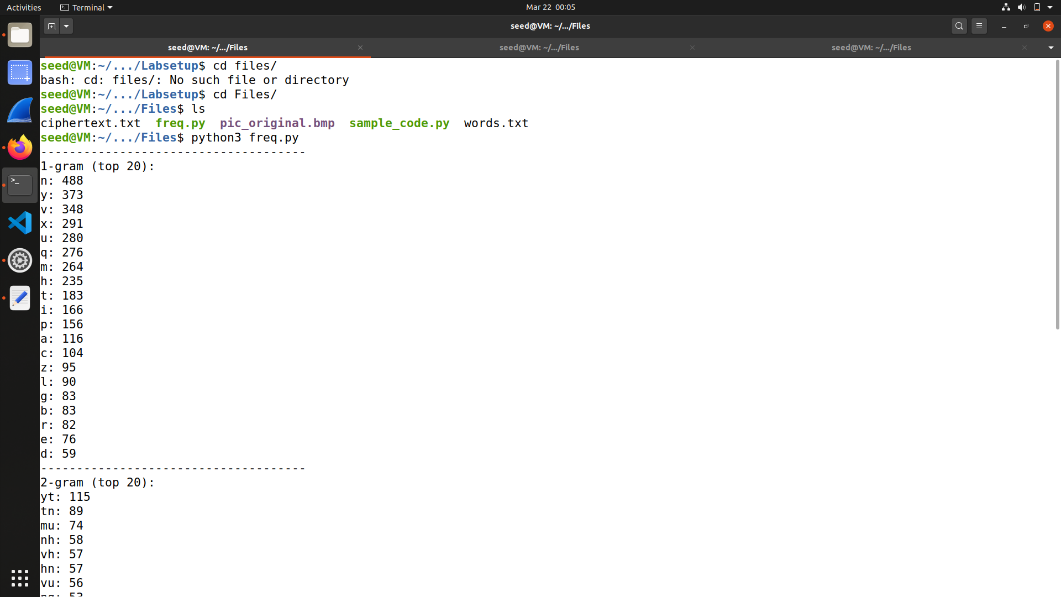
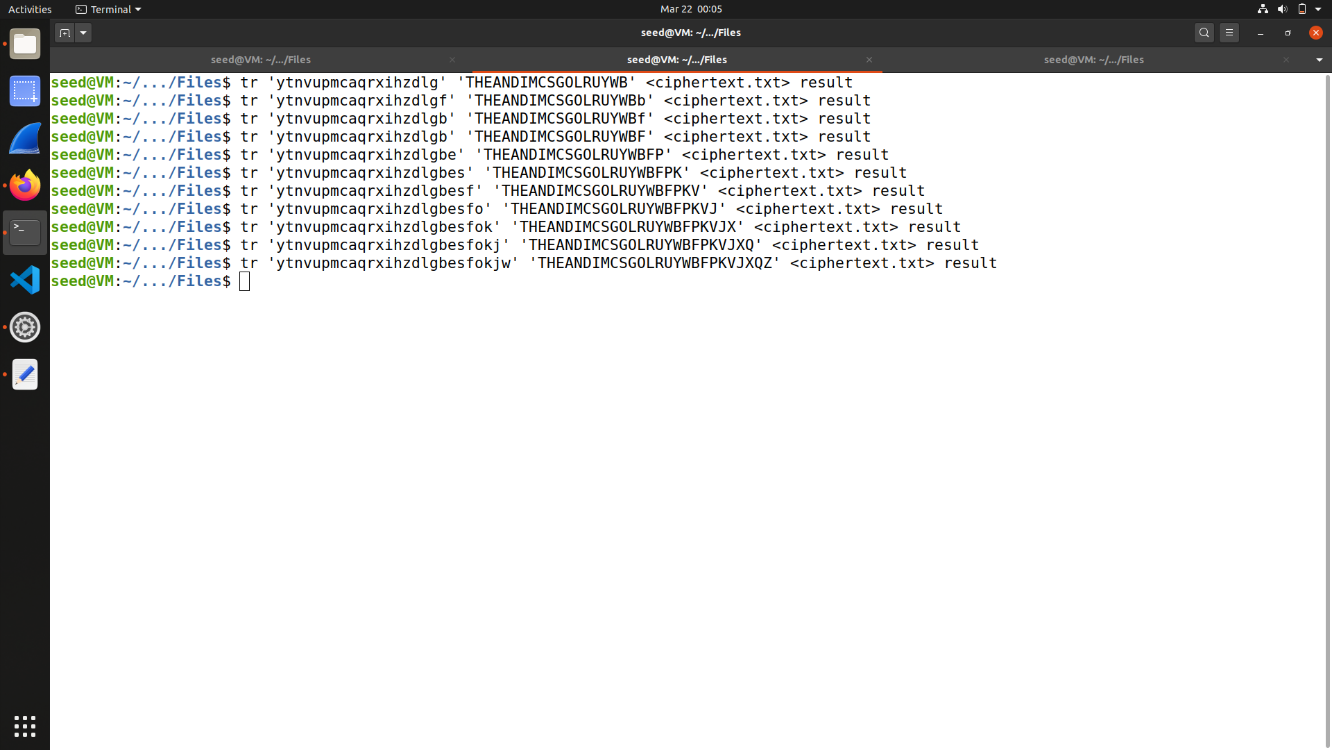
**ACS 54500 Cryptography and Network Security**

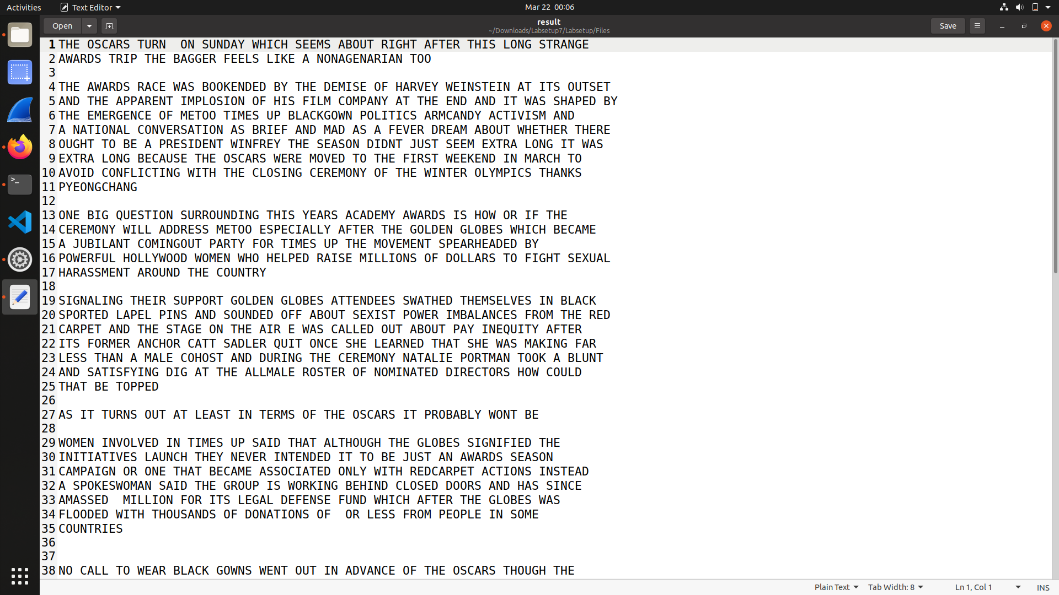
**Lab 7: Crypto Lab: Secret-Key Encryption**

Task 1: Frequency Analysis

Opening the freq.py file.

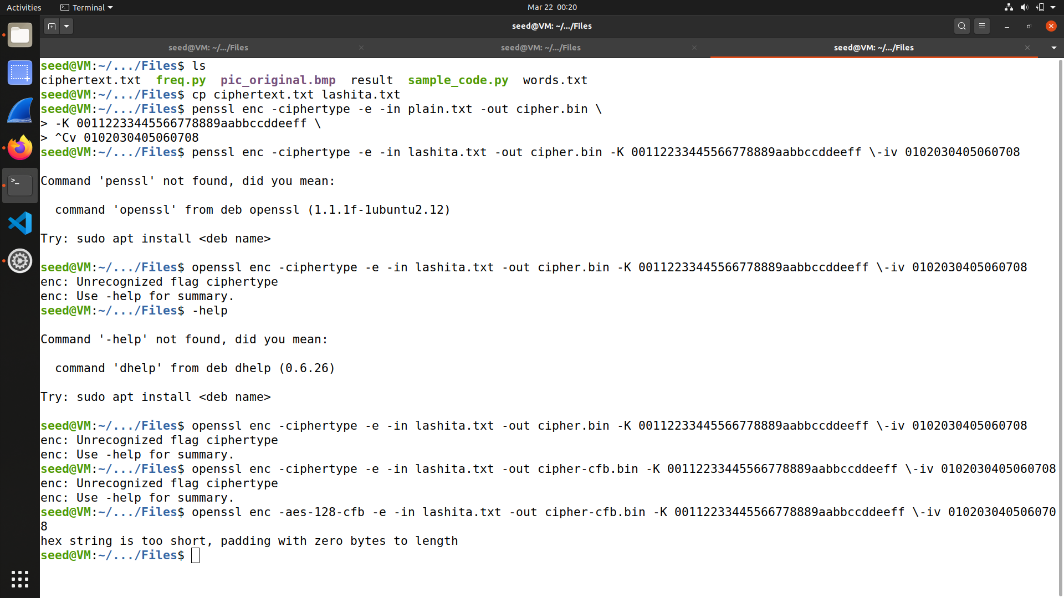


Cipher text:



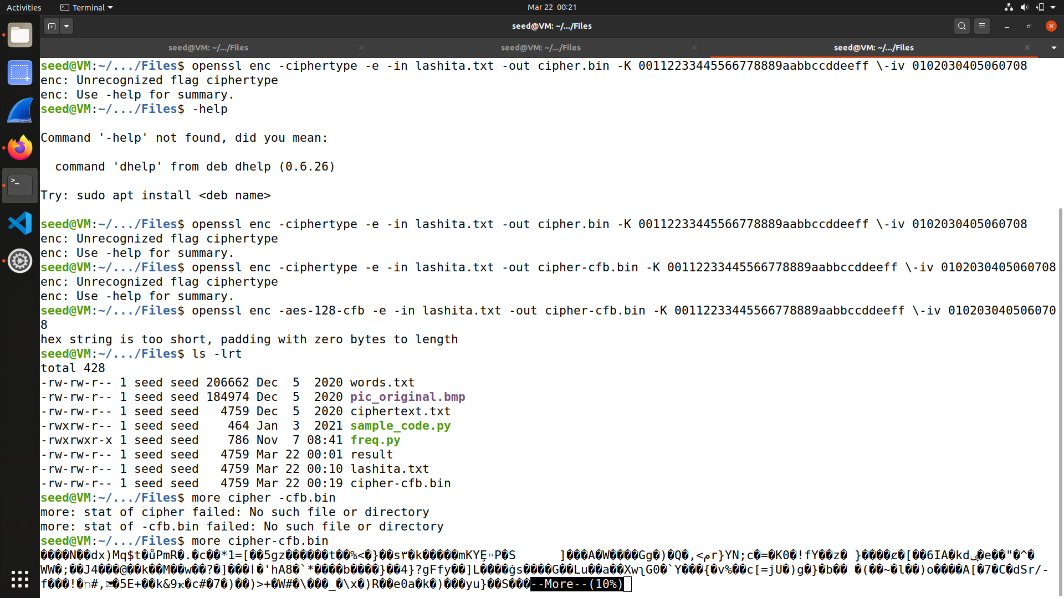
Output:

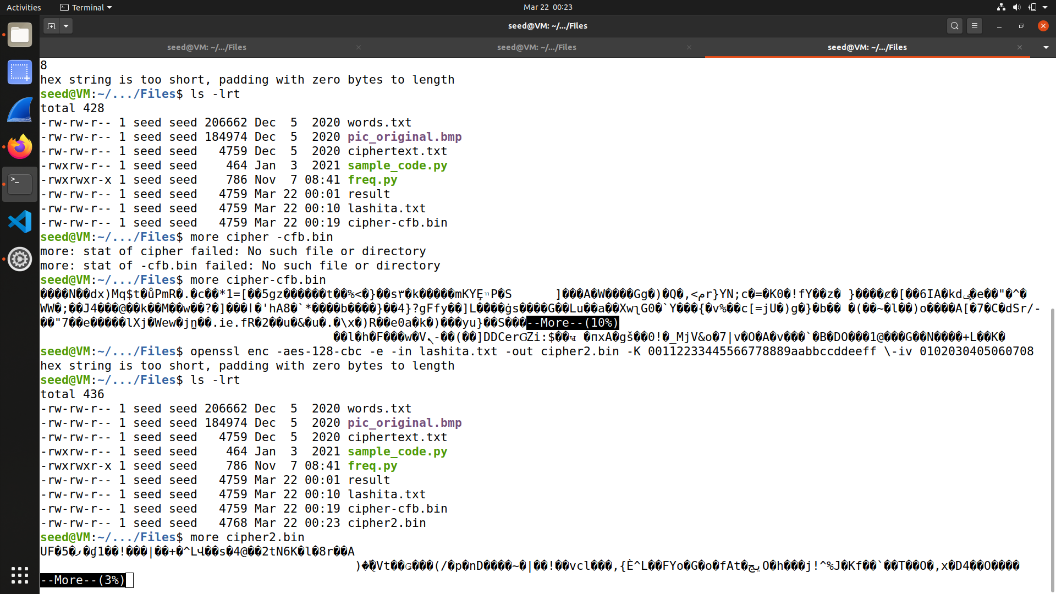
Task 2: Encryption using Different Ciphers and Modes



openssl enc command to encrypt/decrypt a file.

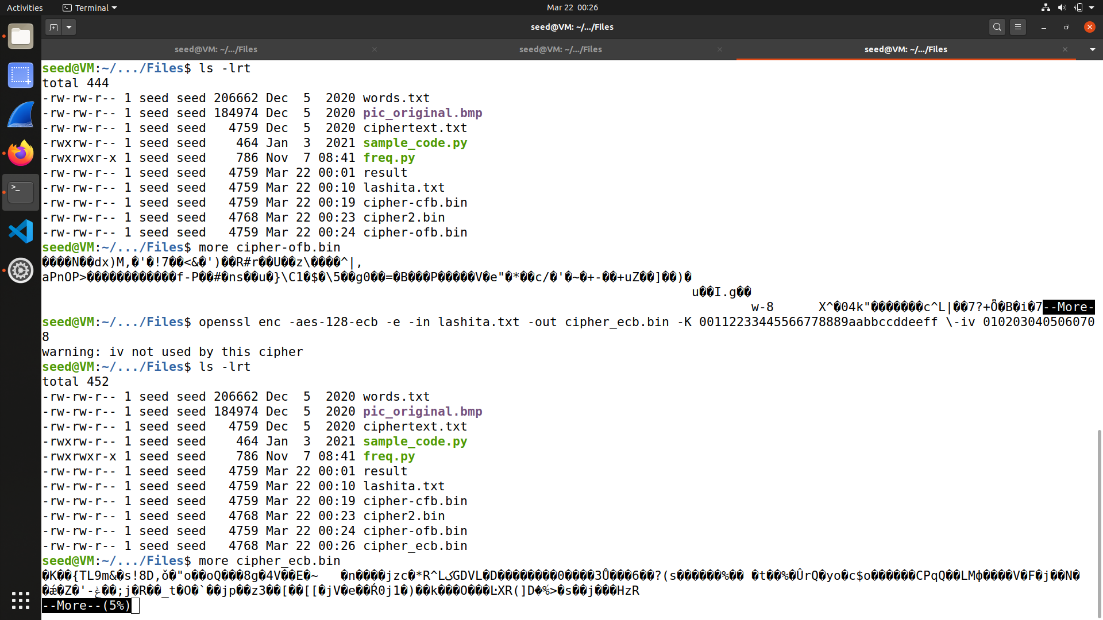
Task 3: Encryption Mode – ECB vs. CBC

Encryption with CBF



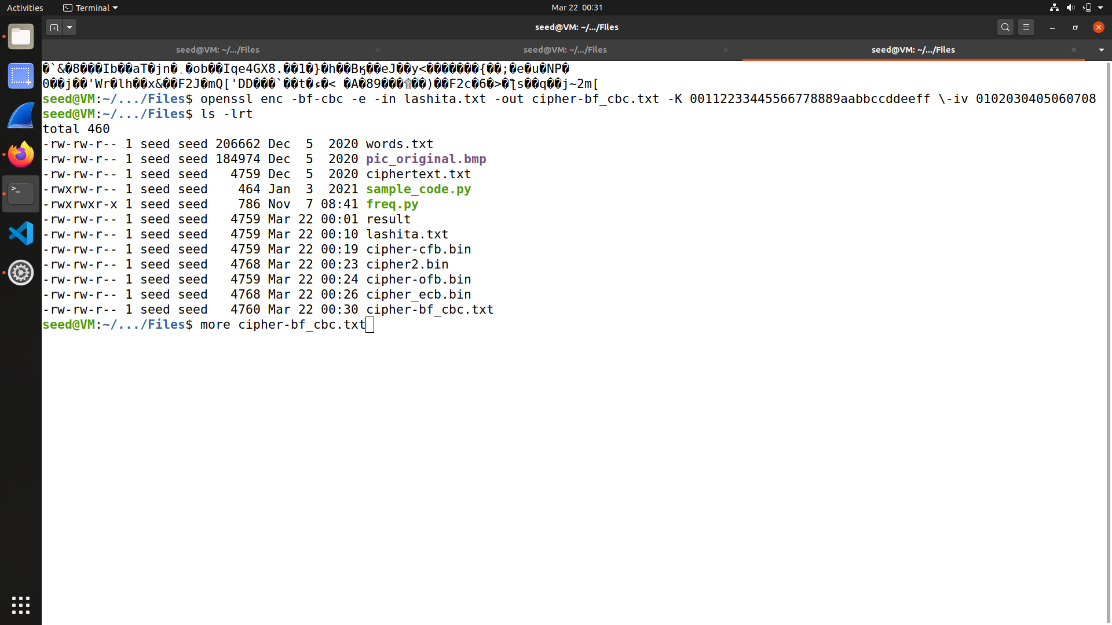
Encryption with CBC

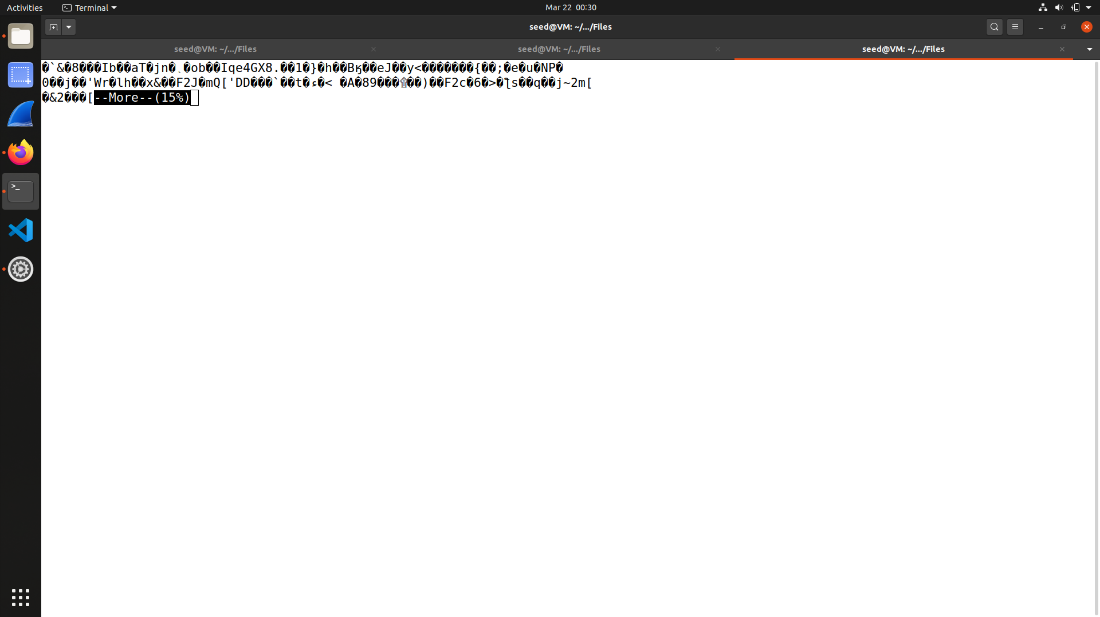
Task 4: Padding  
Encryption with OFB



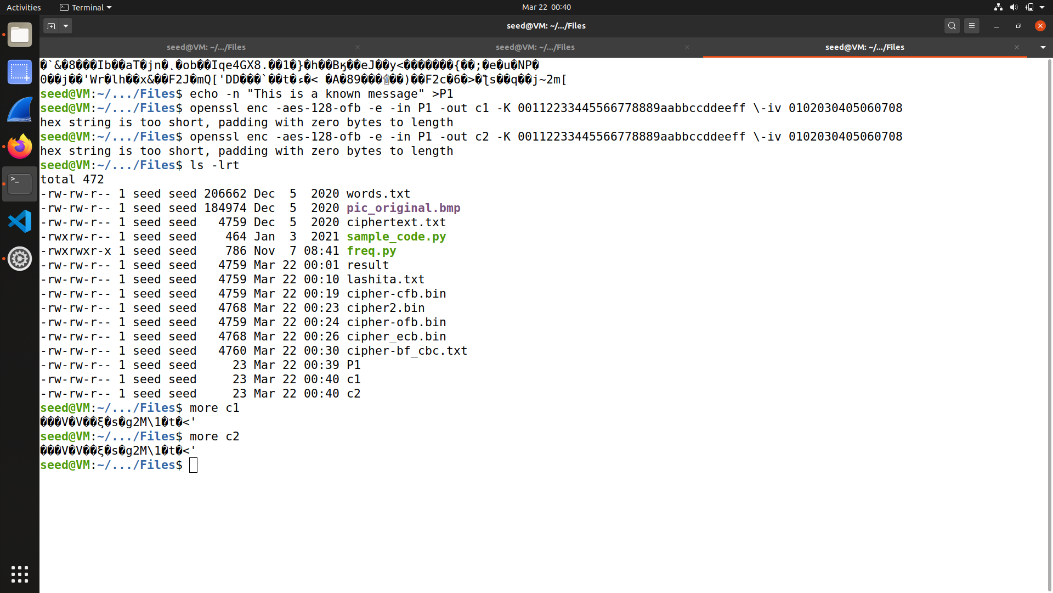
Encryption with ECB

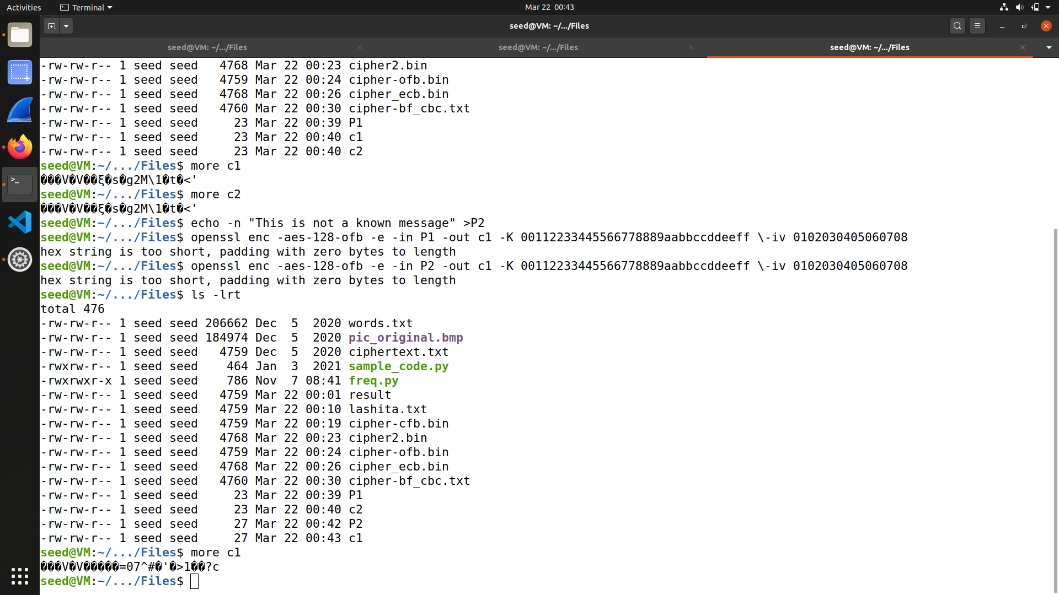
Task 5: Error Propagation – Corrupted Cipher Text

Encryption with Blowfish

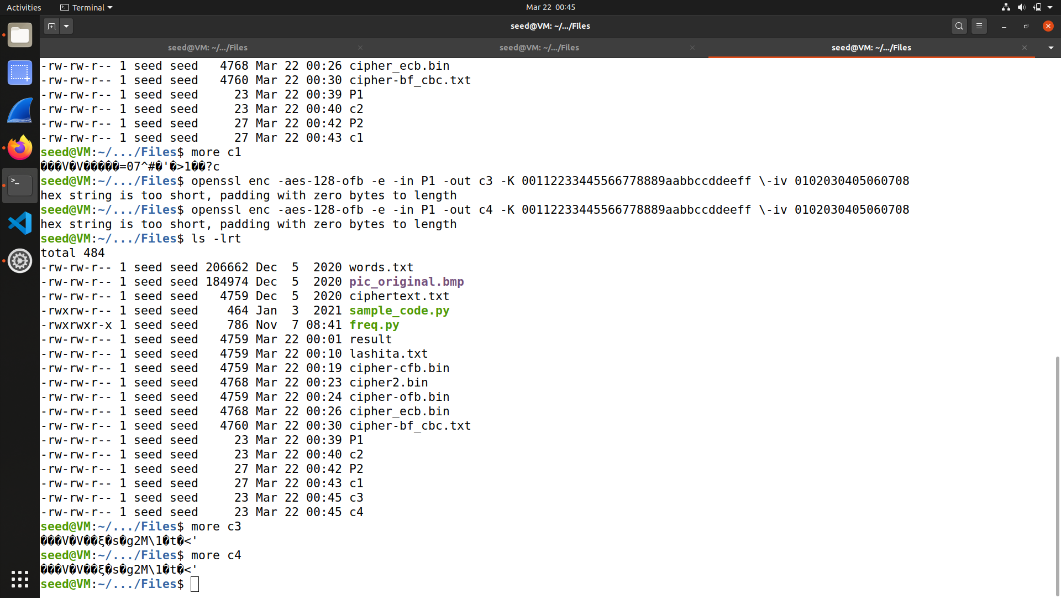


Task 6: Initial Vector (IV) and Common Mistakes

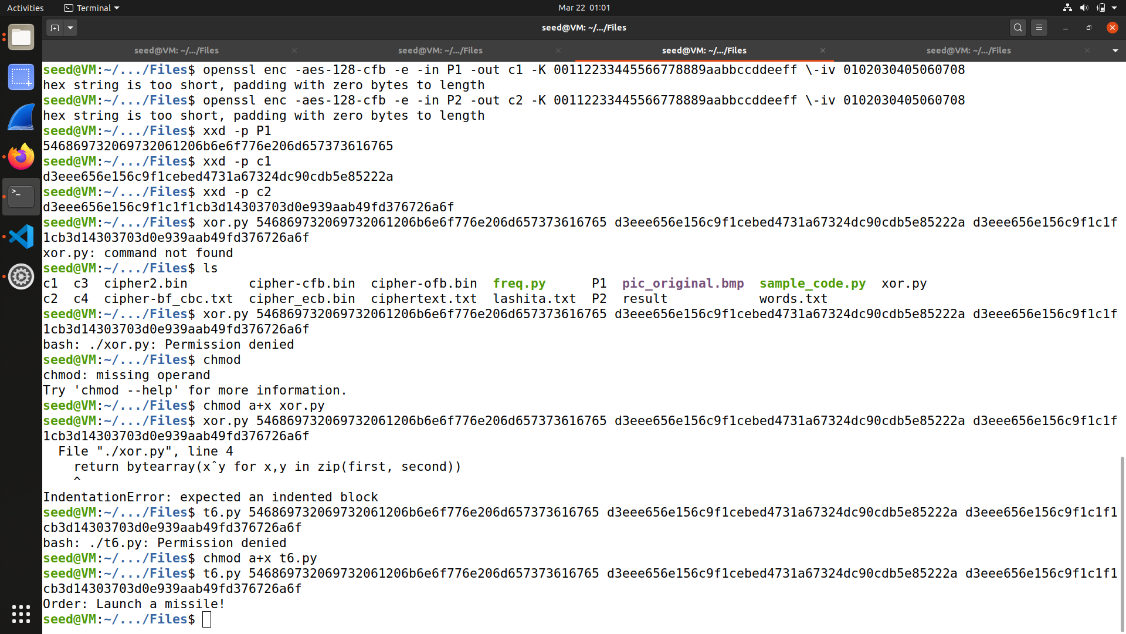
6.1  
Two different IV’s



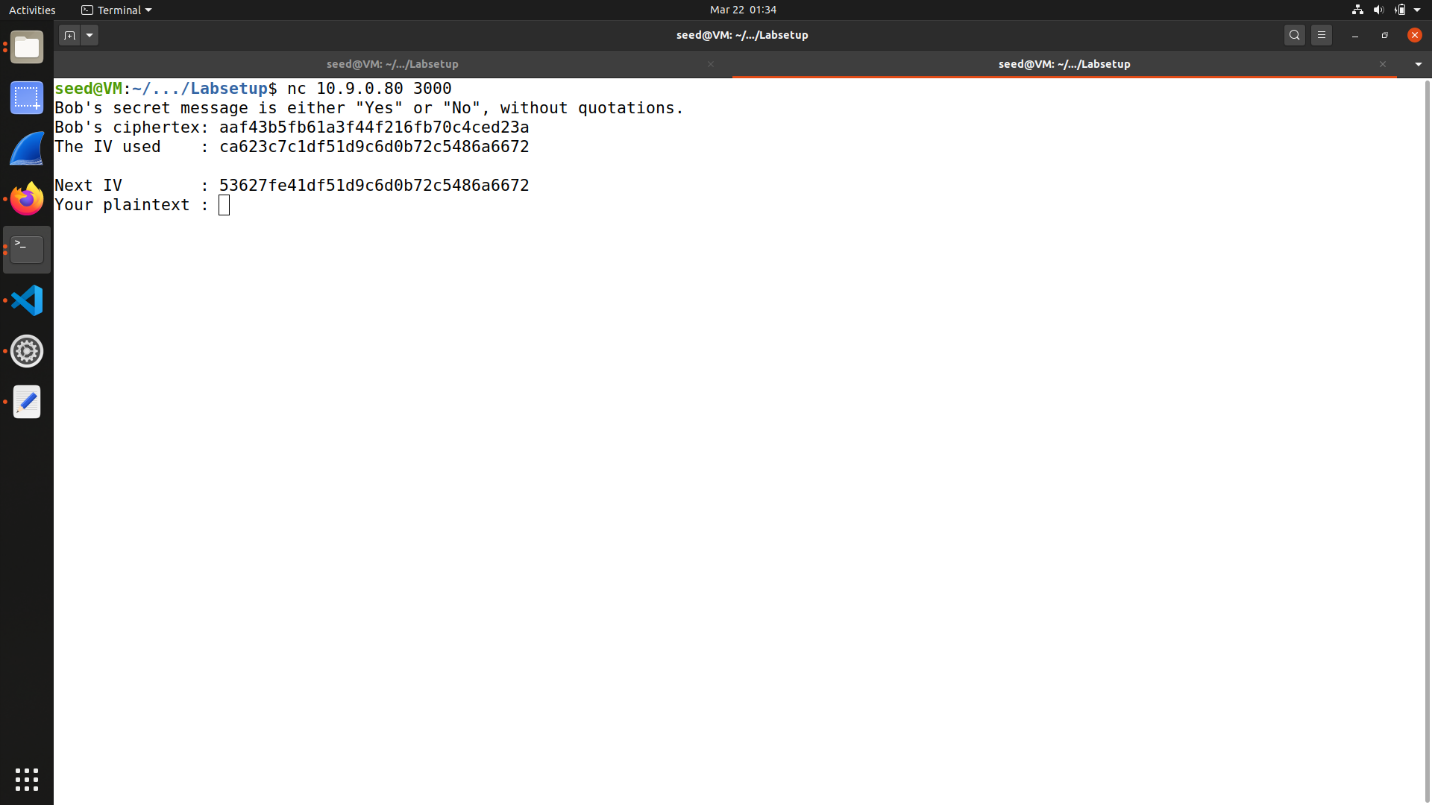
Using same IV on P1 & P2

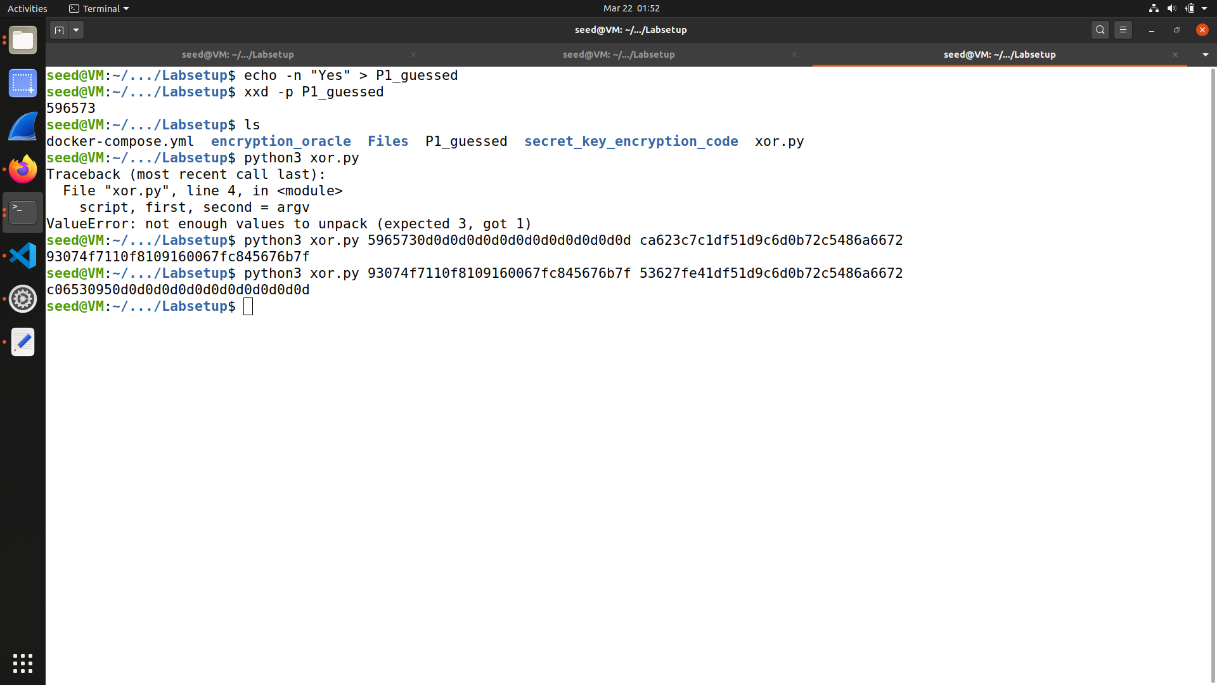


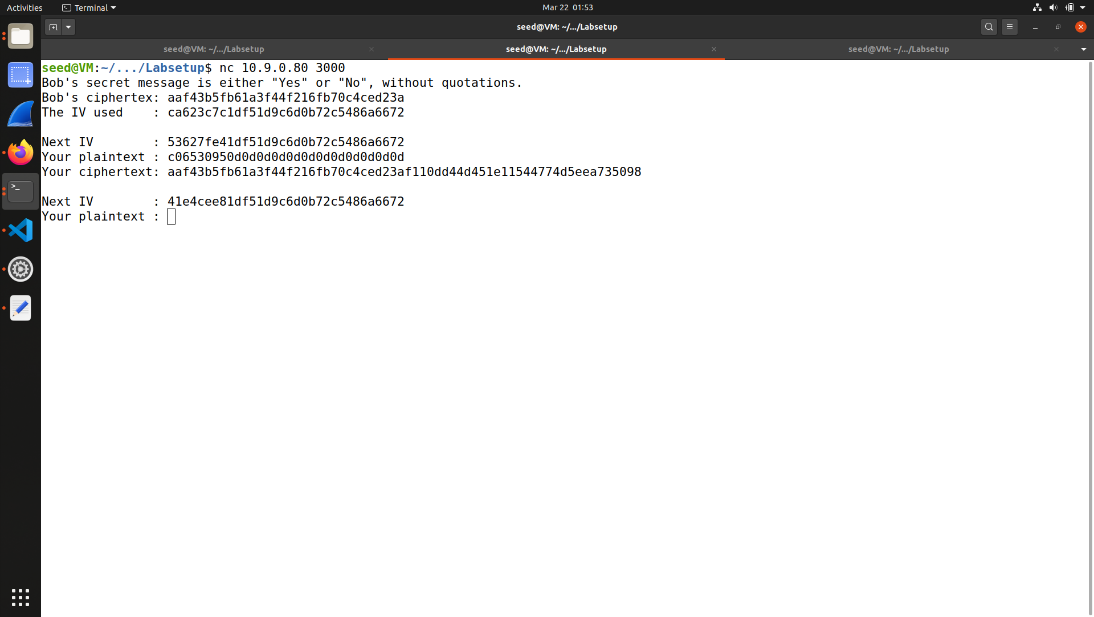
Using Different IV’s



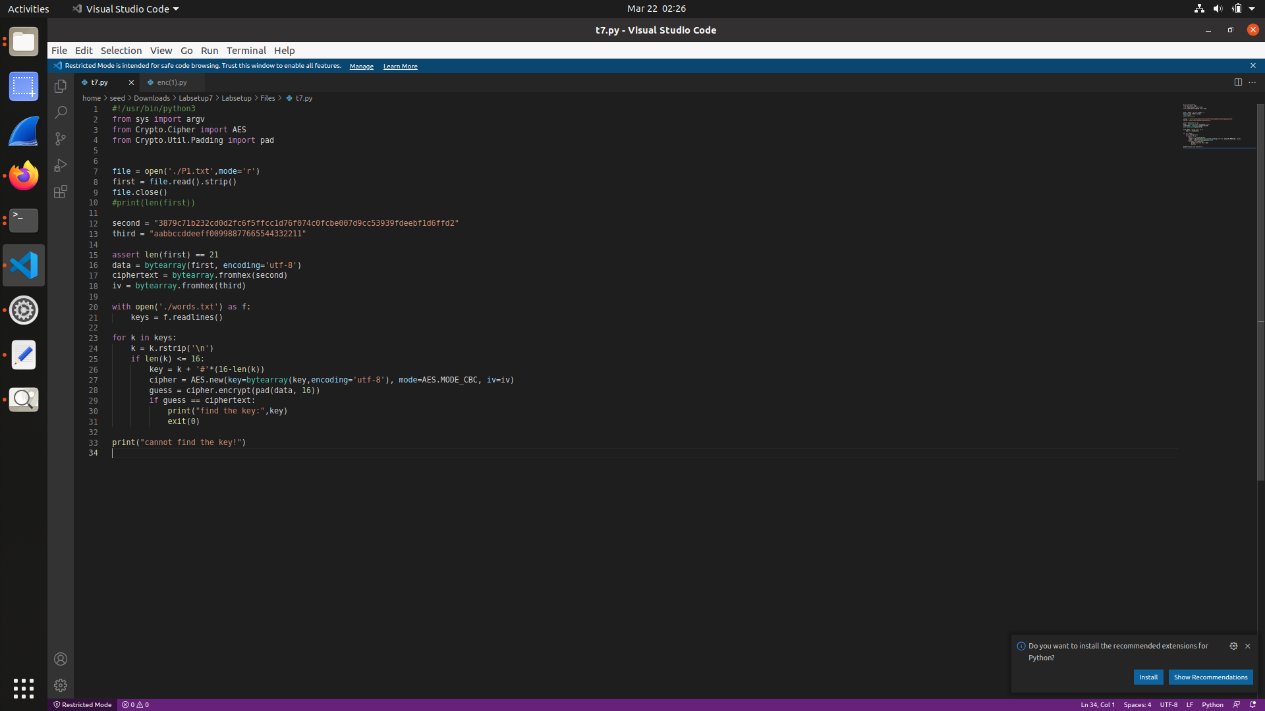
6.2  
using same IV

6.3  
Using a Predictable IV





Task 7: Programming using the Crypto Library



The aes-128-cbc cipher is used for the encryption

