CS445 Lab Report: **Secret-Key Encryption**

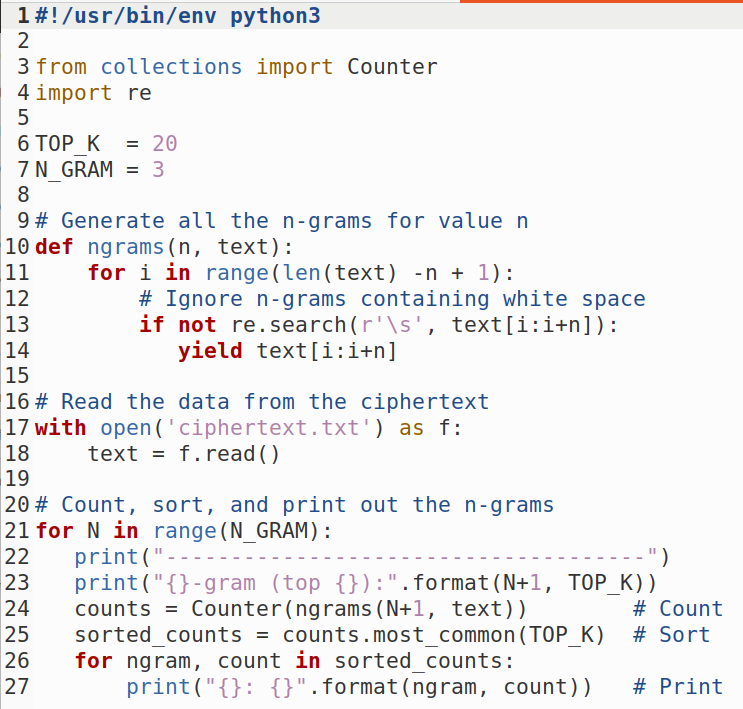
Austin Decker

13 December 2024

# Tasks:

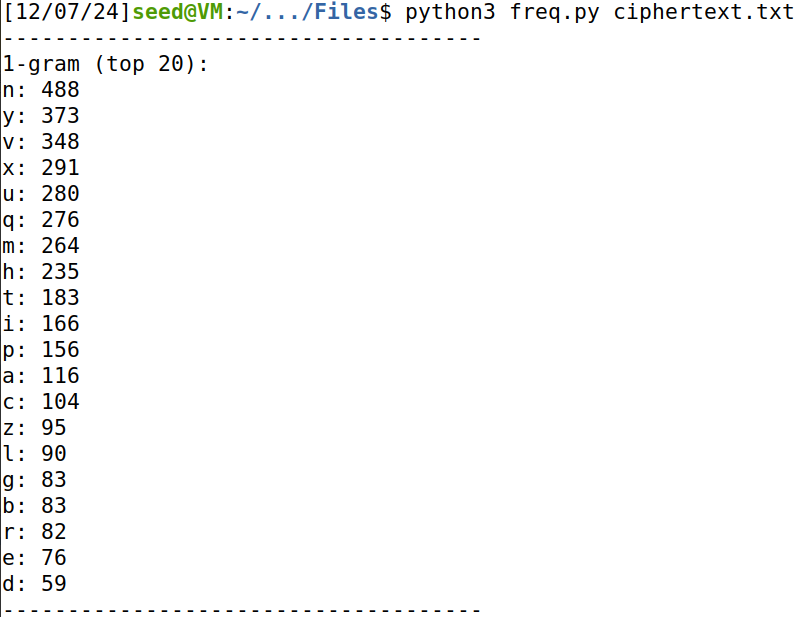
## Task 1: Frequency Analysis

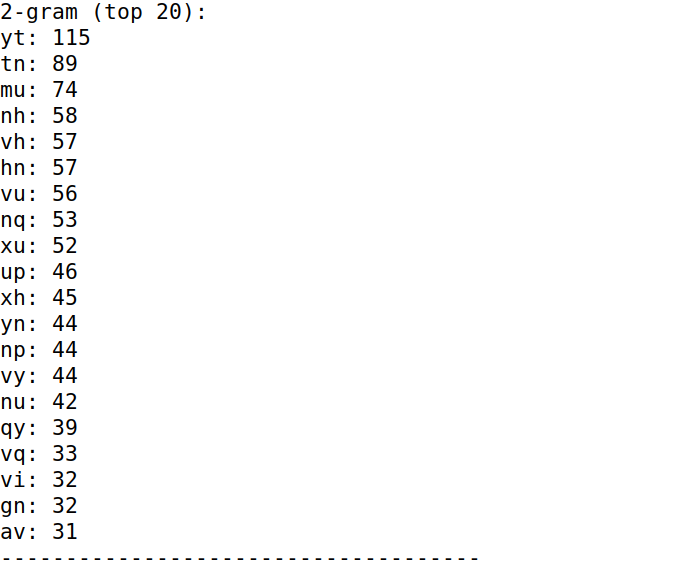
**Code used:**

****

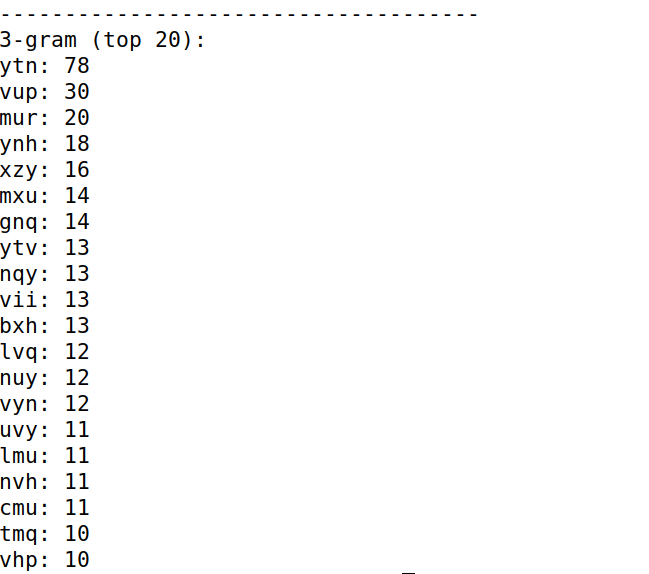
**Getting Metrics from the ciphertext:**

Single Letter Count

****

Bi letter count

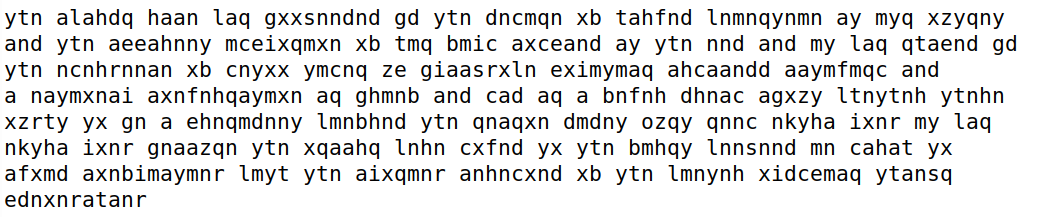
Tri letter count

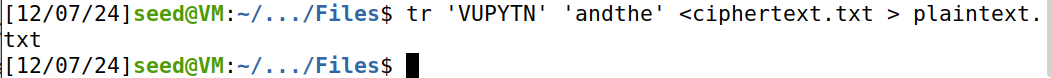


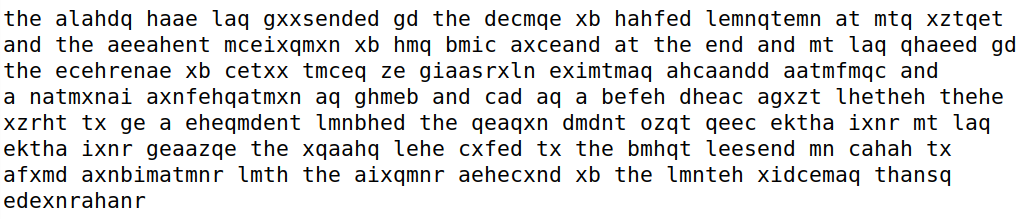
**Frequency Analysis:**

****

This is a small segment of the full text:

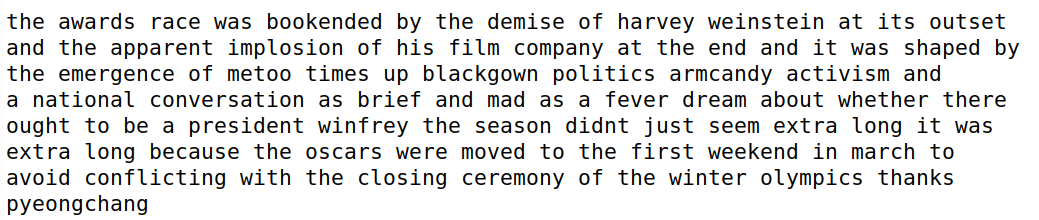
****

****

****

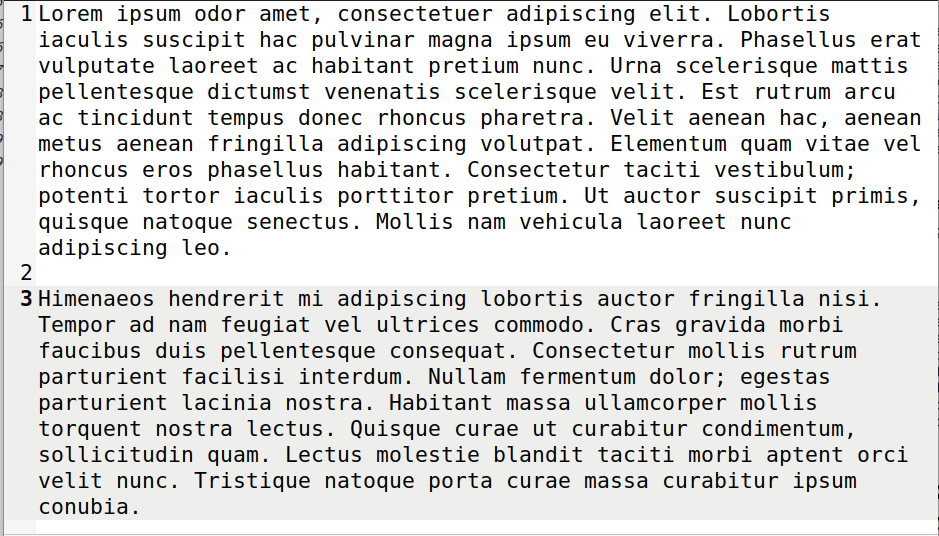
**Final Results:**

****

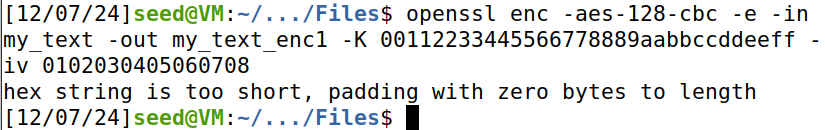
****

## Task 2: Encryption using different Ciphers and Modes

**Unencrypted Text:**

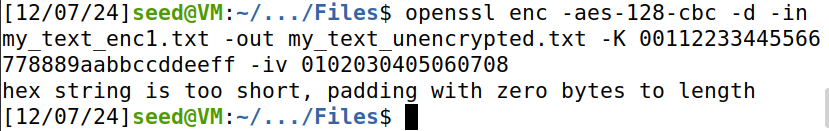
****

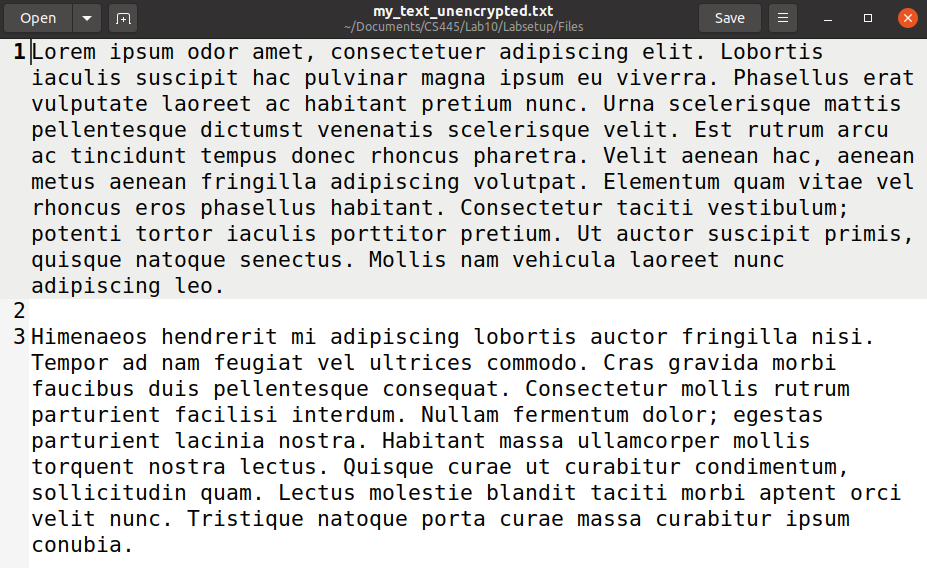
**AES 128 CBC:**

****

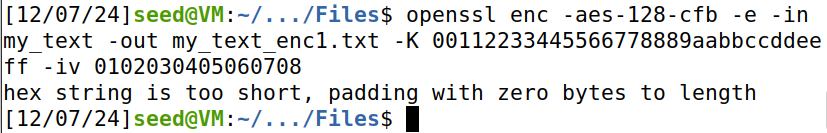
****

**Decrypting to Verify:**

****

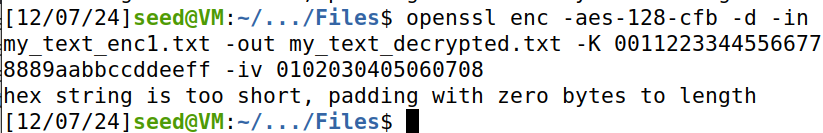
****

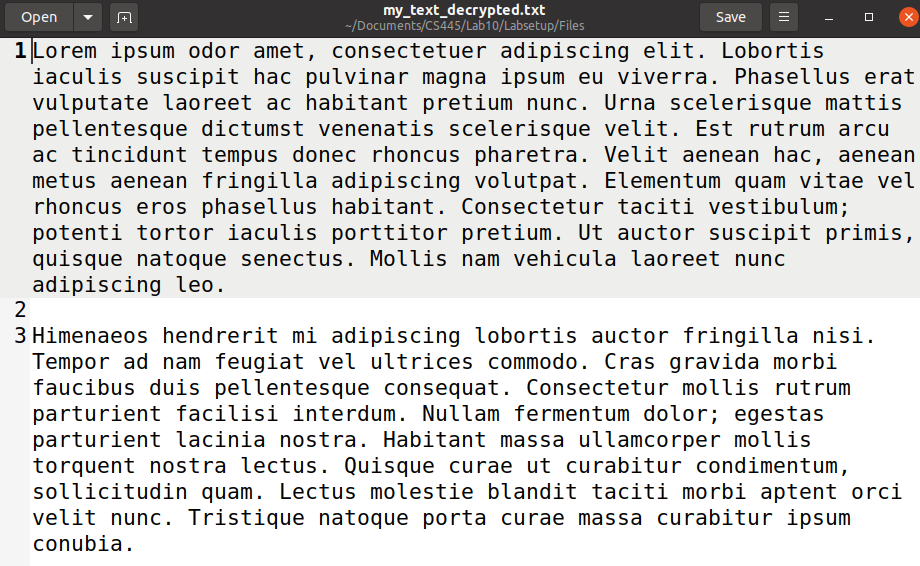
**AES-128-CFB**

****

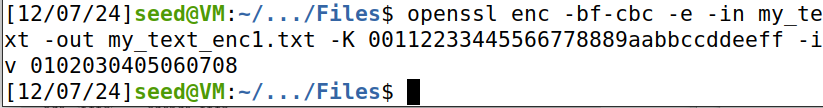
****

**Decryption To Verify**

****

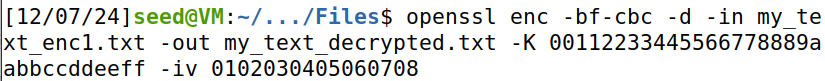
****

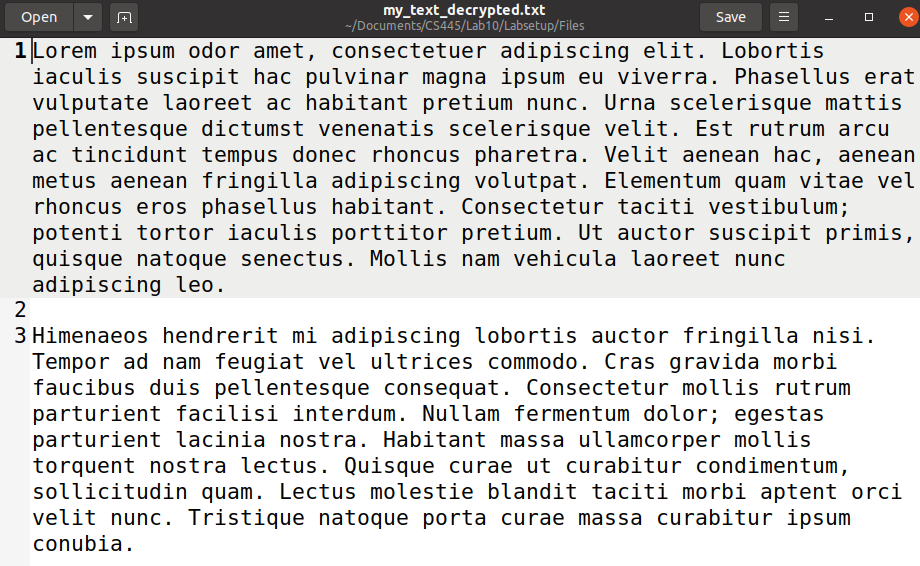
**BF-CBC Encryption**

****

****

**Decrypting to verify:**

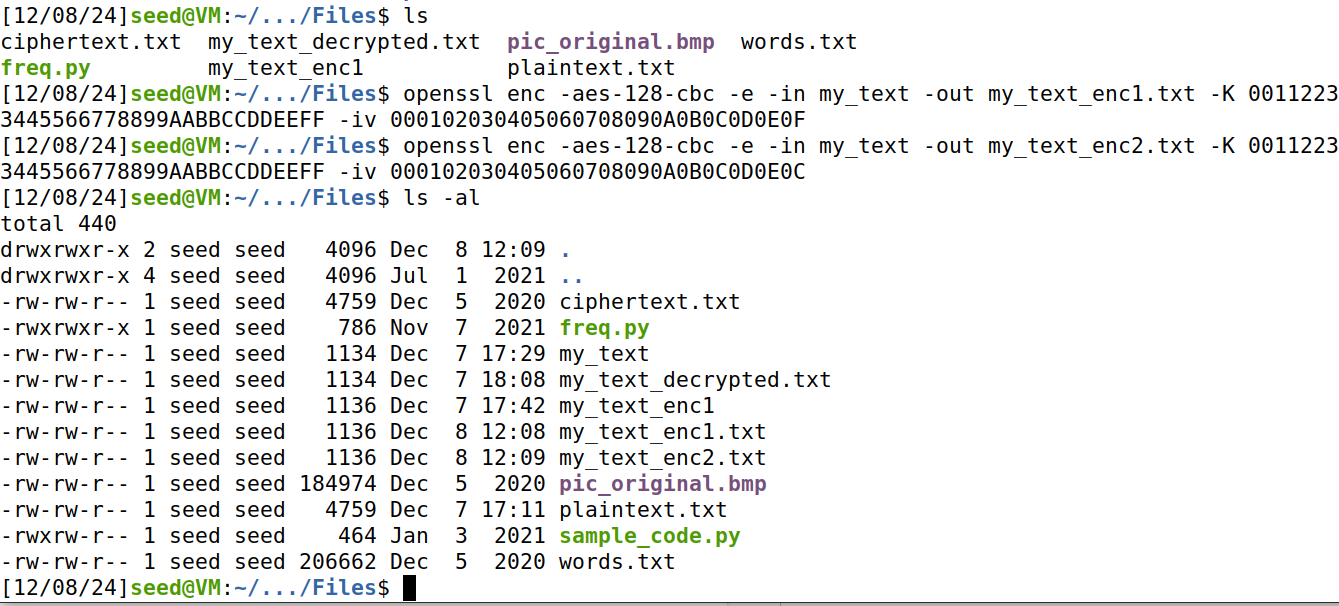
****

****

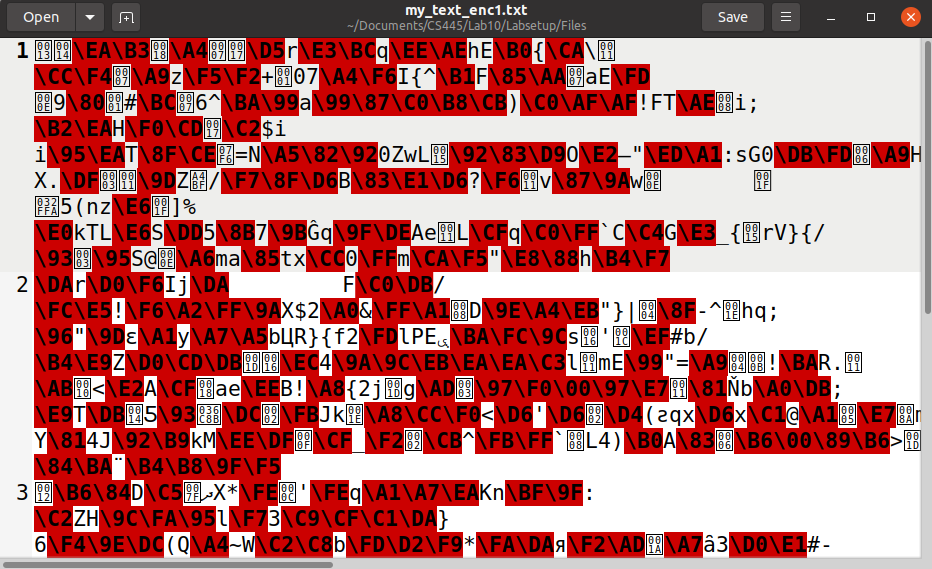
## **Task 6: Initial Vector and Common Mistakes**

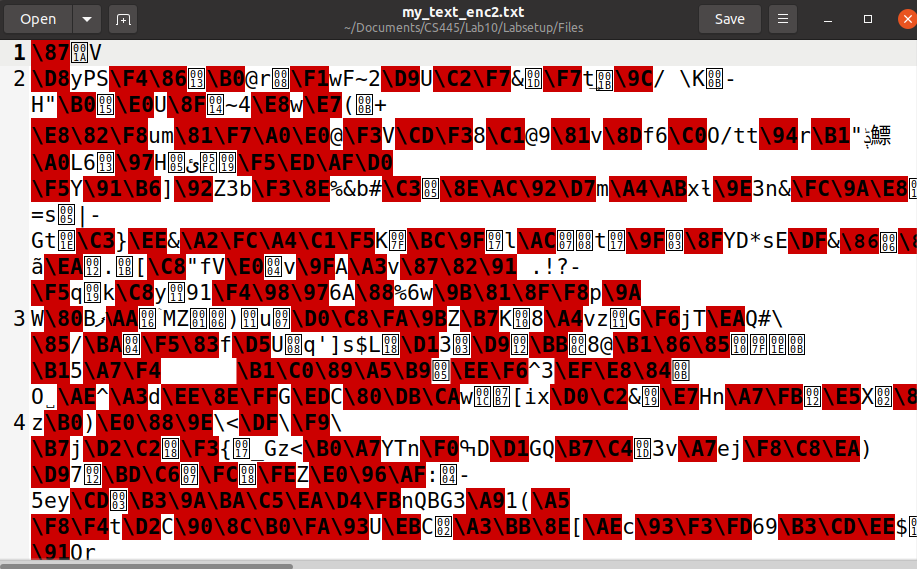
### Task 6.1: IV Experiment

**Different IV**

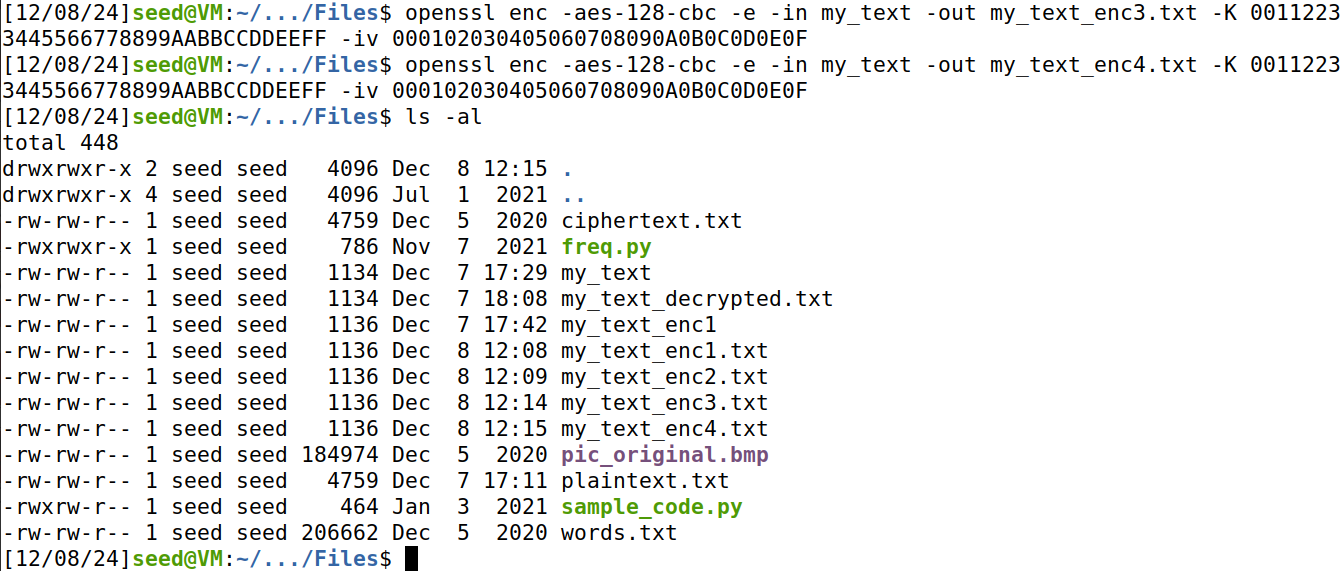
****

**Output:**

****

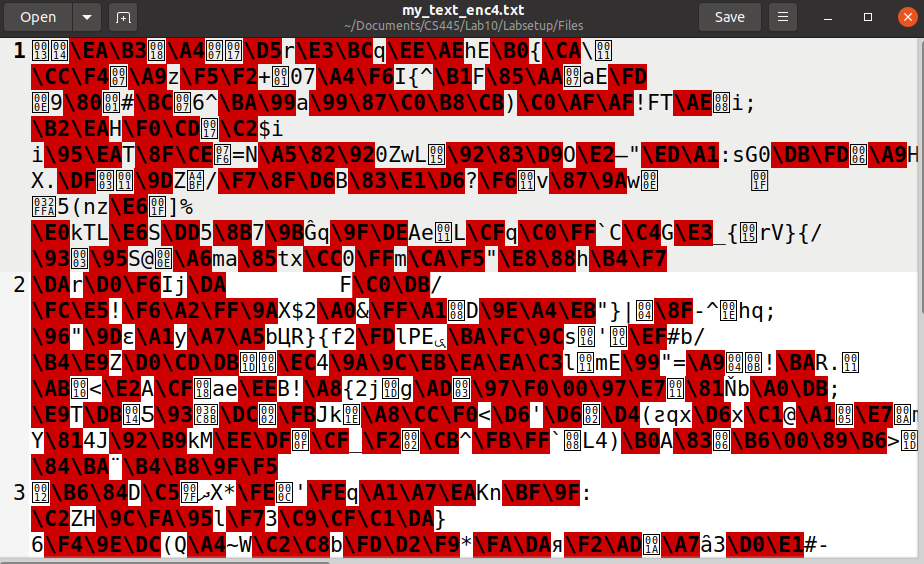
****

**Same IV:**

****

**Output:**

****

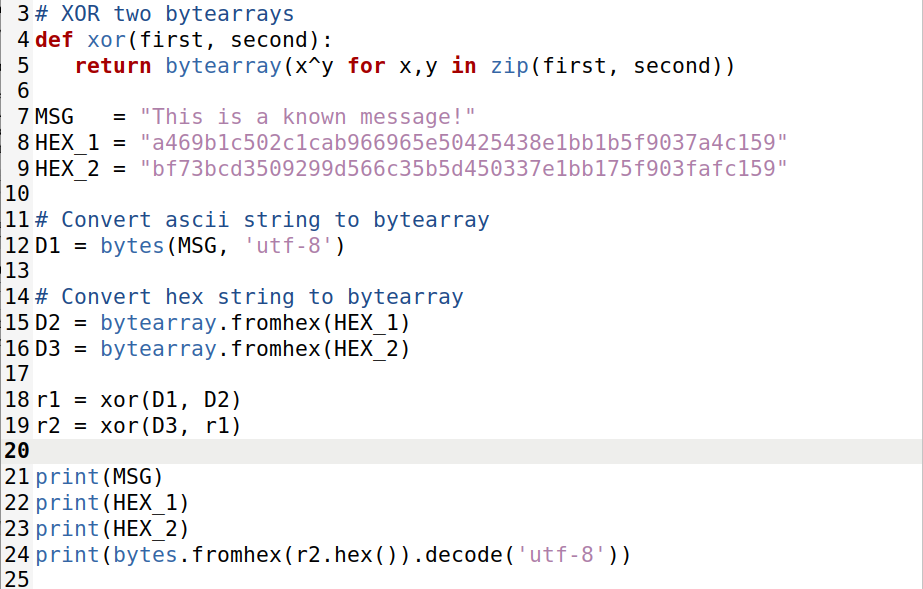
****

**Observation:**

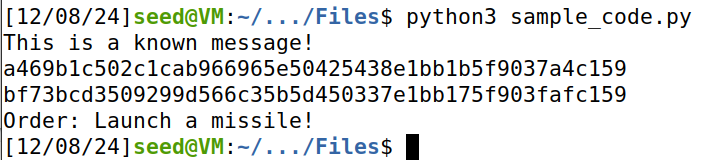
the plain text that used different IV values had a completely different output from one another, even though it was the same plain text. The output of the encryption with the same IV’s resulted in the output to be the same. Using different IV’s ensures randomness in the encryption process so that the same text does not always result in the same output.

### Task 6.2: Common Mistake: use the same IV

**Code:**

****

**Output from script:**

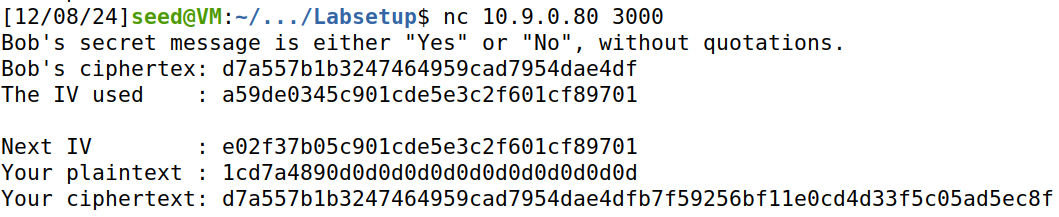
****

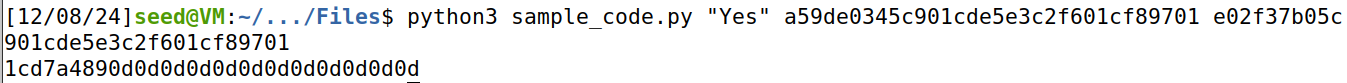
**Observation:**

In OFB mode, the encryption uses the same IV. Since we know the unencrypted message and the two encrypted messages, we can XOR the unencrypted message with the encrypted counterpart to get the key. Then XORing the Key with the unknown encrypted message will result in decrypting the unknown message.

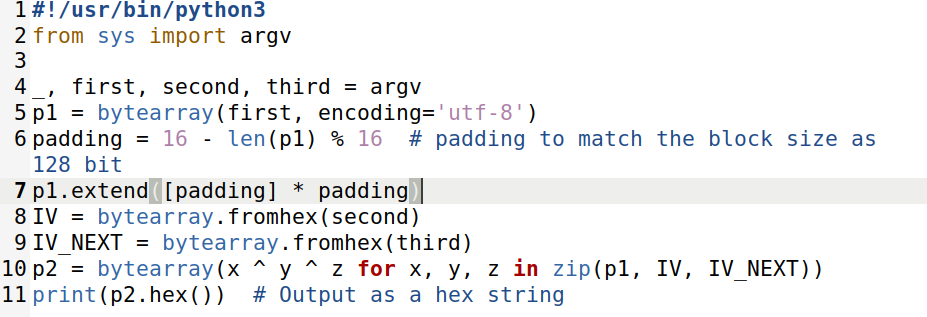
If we replace OFB with CFB in this experiment, only a portion of P2 can be revealed.

### Task 6.3: Using a Predictable IV





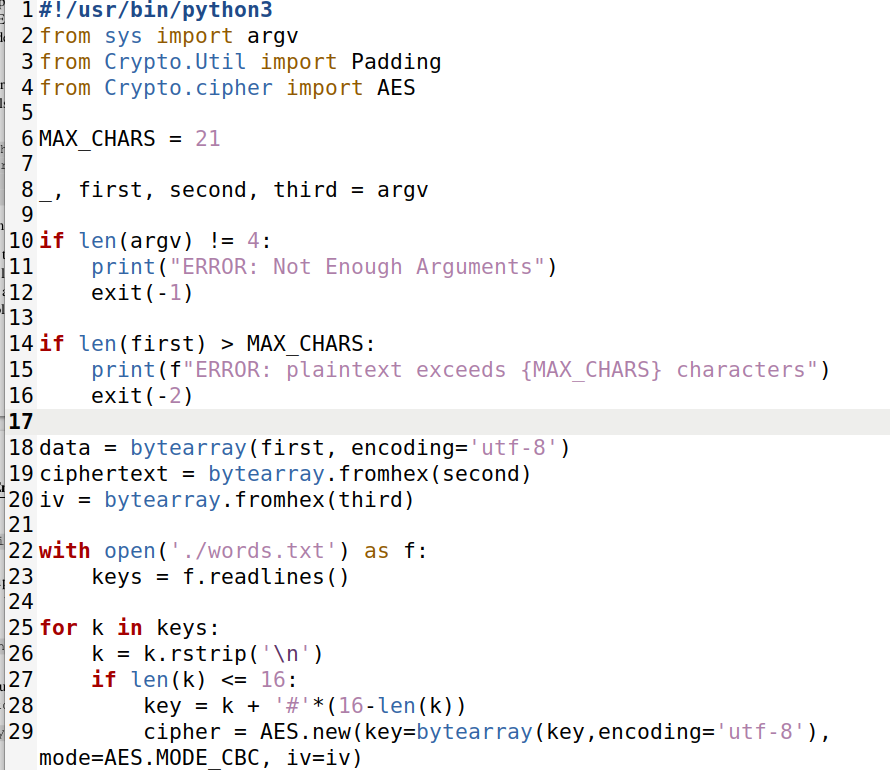
**Code Used to Get plaintext:**

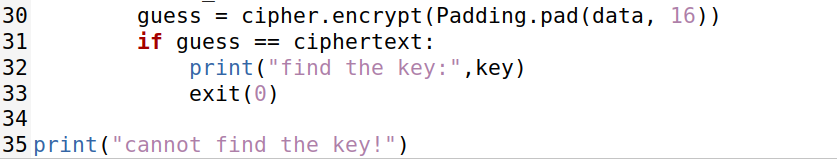
****

**Observation:**

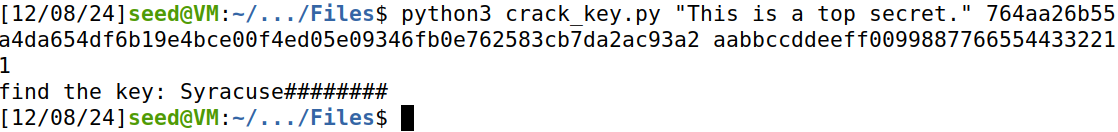
I guessed that Bob’s secret message was Yes. I XORed the previous IV and the next iv then XORed my guess to get the hex string I would send to the server. Since the cipher text came back the same as Bob’s cipher text, I can confidently say that his answer was “Yes”

## Task 7: Programming using the crypto library





**Running Script:**

****