**Lab 8**

**Pakshal Bhandari**

**Task 1: Frequency Analysis**

In this task we will be doing frequency analysis to decipher a monoalphabetic cipher and use that to figure out what is the encryption key.

I have created a plaintext.txt file and have used to watch it every 5 seconds to detect and display changes made to the file.



We use freq.py to see whch 1-grams, 2-grams and 3-grams are the most common in the ciphertext to decipher it.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Deciphering cipher text letter by letter

A screenshot of a computer screen

Description automatically generated

Encryption key used for encrypting the text is

'ytnvupxmgqahzbrisdleckfjo' => 'THEANDOIBSCRUFGLKYWPMXVQJ'

Deciphered plaintext

A screenshot of a computer

Description automatically generated

A screenshot of a computer

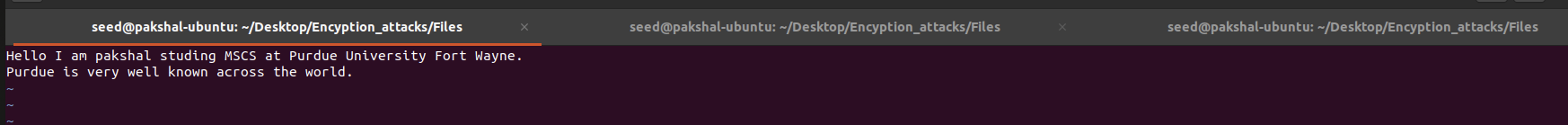
Description automatically generated

The cipher has been successfully deciphered.

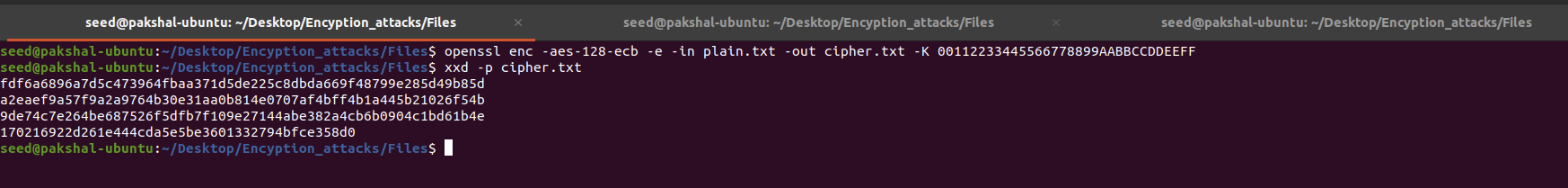
**Task 2: Encryption using Different Ciphers and Modes**

In this task, we experiment with 3 different kinds of encryption algorithms and modes.

I choose some random text in plain.txt



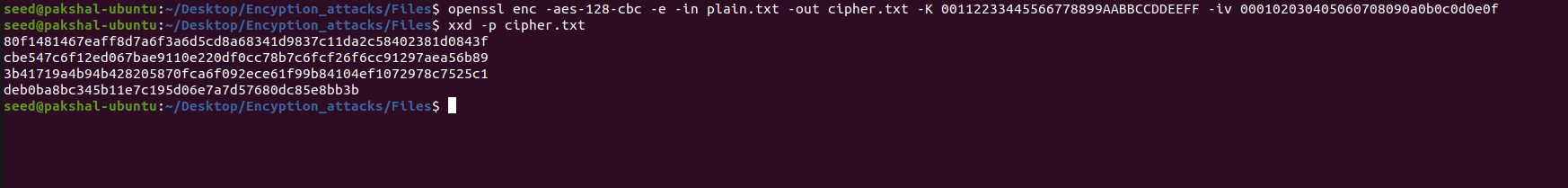
**AES 128**



The screenshot shows the encrypted text after we use the xxd -p command to convert the text into a hex string.

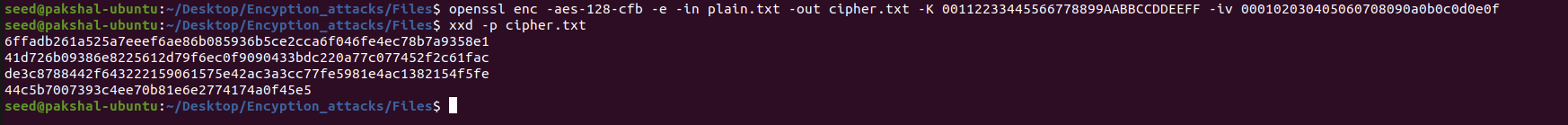
**AES CBC**

This mode needs an additional parameter of the initialization vector to be specified.



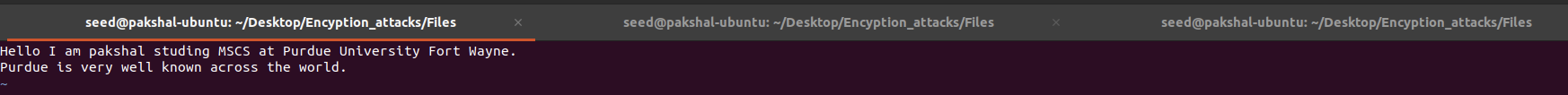
**AES CTR**

This mode also needs an additional parameter of the initialization vector to be specified. Below is the screenshot of the commands used to encrypt the plaintext.



**Task 6: Initial Vector (IV) and Common Mistakes**

For task 6 and its sub task below is the plain text I am using.



**Task 6.1:**

This subtask is an experiment with the uniqueness of IVs. We have to encrypt the plaintext first with the same IV twice, and then with two different IVs, and describe what is observed.

**Encryption using the same IV:**

A screen shot of a computer

Description automatically generated

The same IV to encrypt the same plaintext gives the same ciphertext regardless of the situation because the same mode of encryption and key are used. This makes it vulnerable to attacks. This means that no IV should be reused under the same key.

**Encryption using different IVs**

**A screenshot of a computer

Description automatically generated**

**Task 6.2:**

In this subtask, the goal is to prove that when using the same key, we can derive P2 if we know what P1, C1 and C2 are.

We modify the sample code provided to find P2 from the equations

**P1 xor P2 = C1 xor C2**

**P2 = C1 xor C2 xor P1**

A computer screen with a purple background

Description automatically generated



The second plaintext is “Order: Launch a missile”.

If we replaced OFB with CFB, then considering how CFB works, the attacker would not be able to fully recover the plaintext.

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

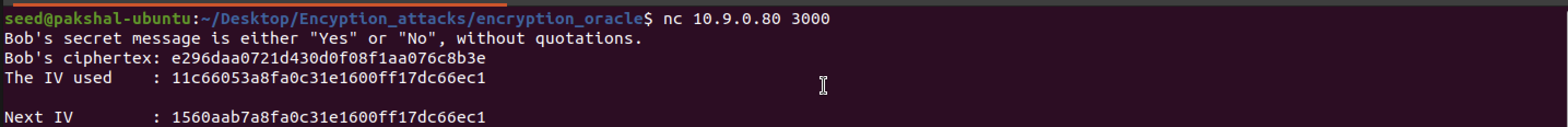
In this task we have to construct a message and ask Bob to encrypt it and give us the ciphertext. The objective is to figure out whether the actual content of Bob’s secret message is Yes or No.

A black background with a white letter

Description automatically generated

For this task, we are given an encryption oracle which simulates Bob and encrypts message with 128-bit AES with CBC mode.

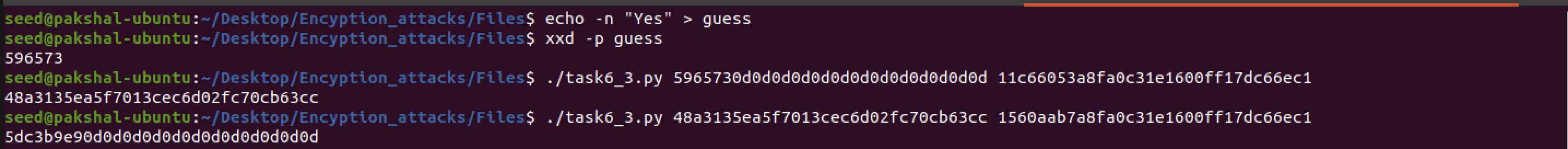
To connect to the oracle we run the netcat command as shown below.



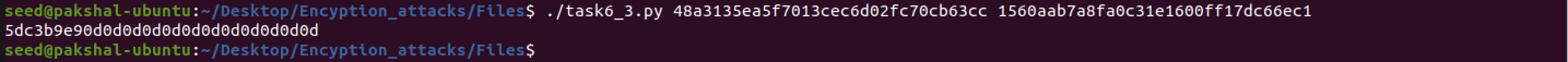
First I have used “Yes” and saved this in guess, and converted it into a hex string using the xxd -p command.

The encryption mode being used is CBC, which requires padding. The hex string 596573 has 3 bytes, so we need to add 13 more bytes of padding, which means 13 in hexadecimal that is 0d repeated 13 times.

We now xor the IV used by Bob with the result



Now we xor the above result obtained with next IV.



We input this result as our plaintext in the oracle.

A screenshot of a computer

Description automatically generated

When we omit the extra hex digits Bob’s ciphertext and our ciphertext are the same. Hence we have guessed the actual content of Bob’s message.

**Task 7: Programming using the Crypto Library**

In this task the job is to find the key that is used for the encryption, given a plaintext and a ciphertext.

A computer screen shot of a computer

Description automatically generated



On running the program it shows that the correct encryption key used is “**Purdue##########**”.