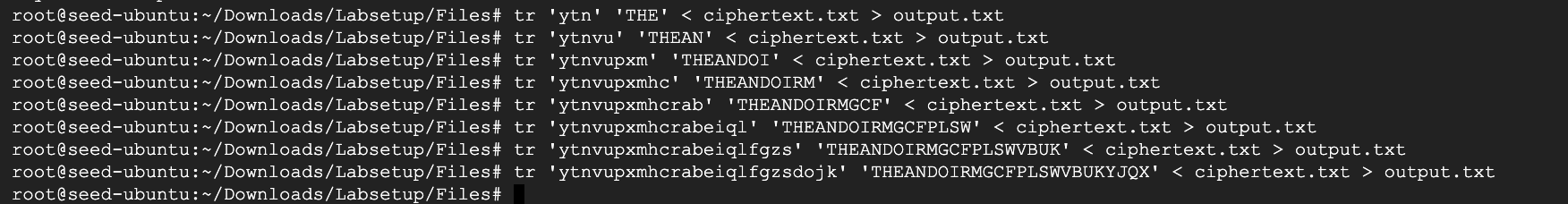
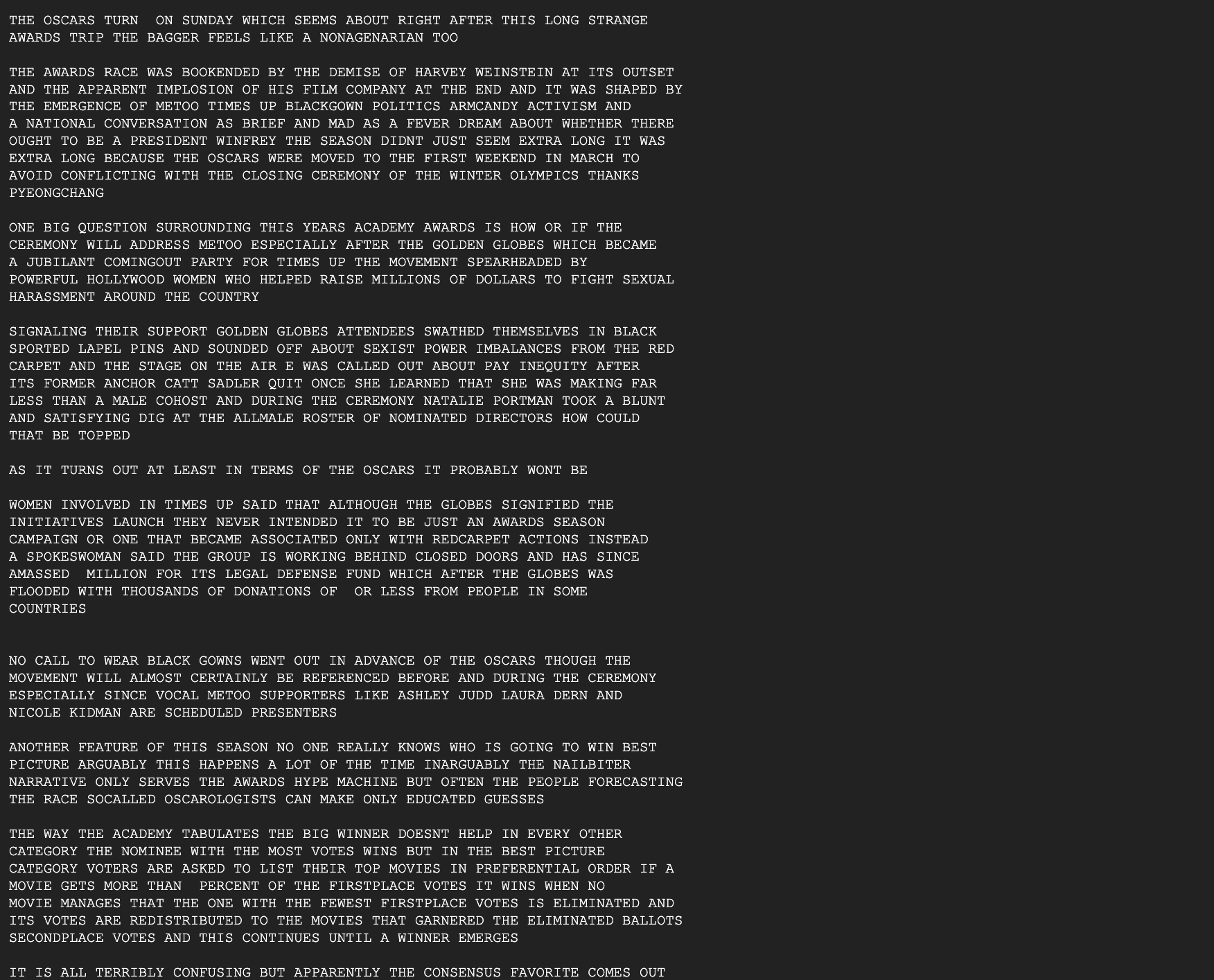
**Task 1: Frequency Analysis**

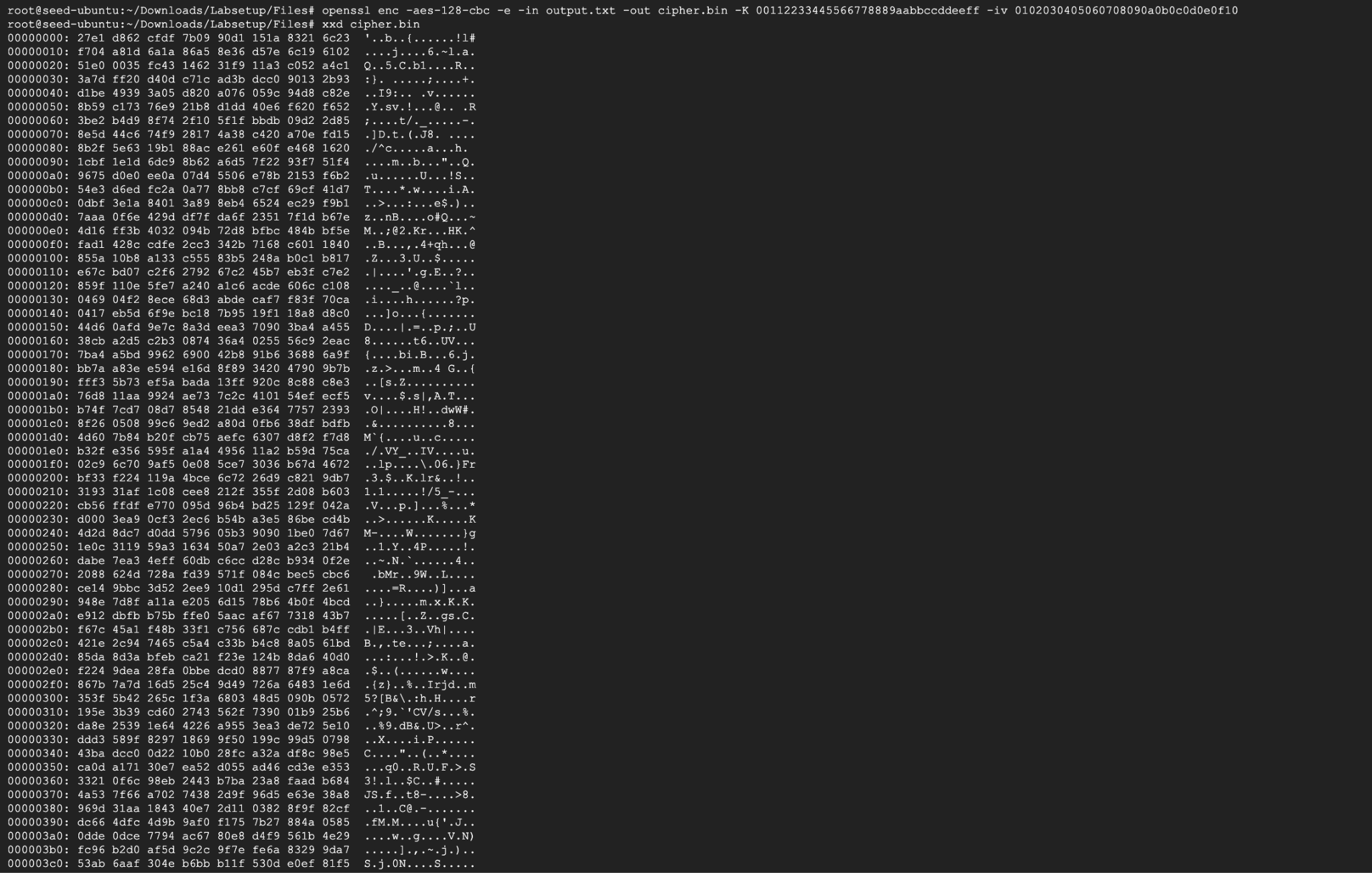


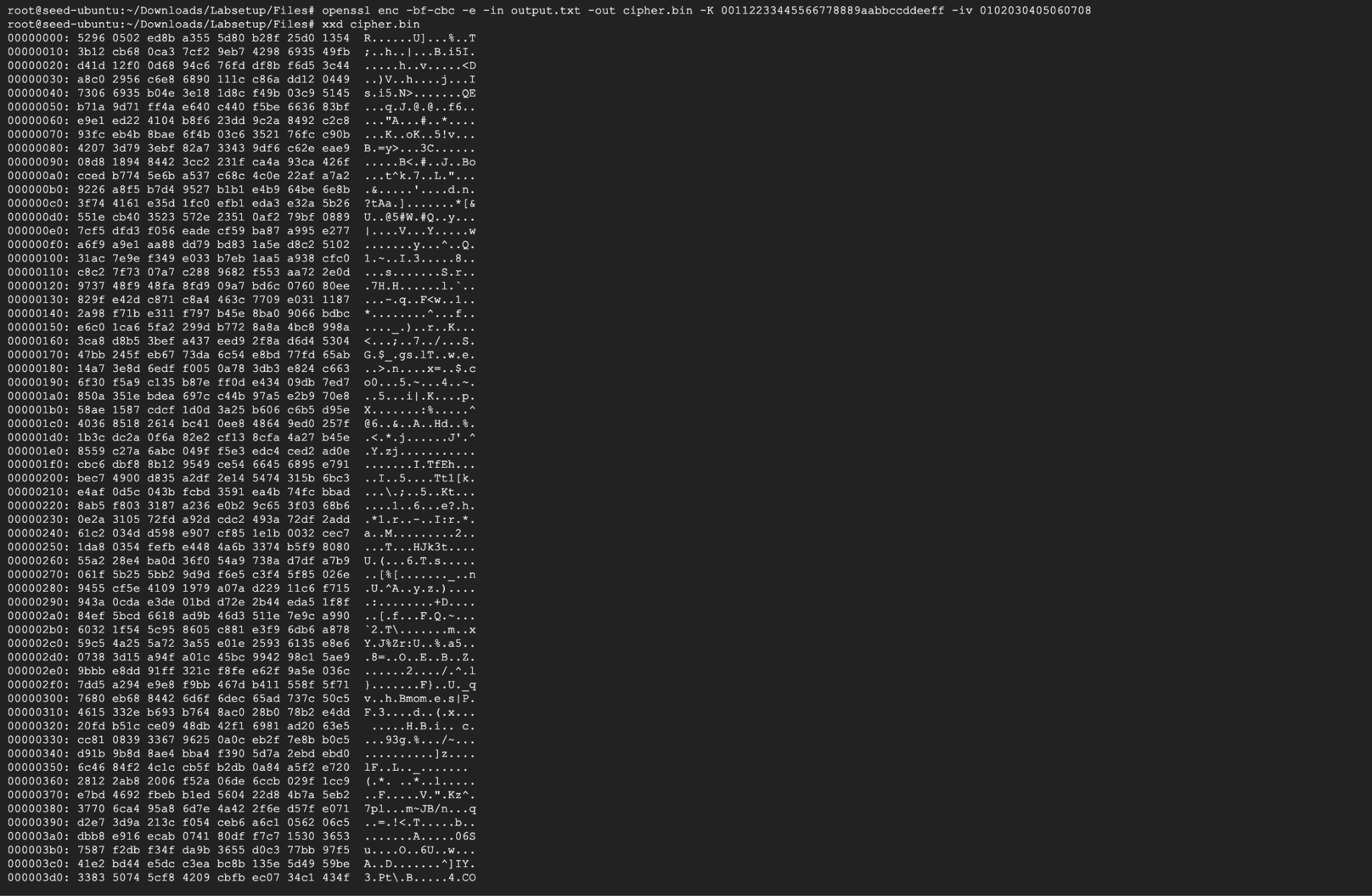
**Final Command:** tr 'ytnvupxmhcrabeiqlfgzsdojk' 'THEANDOIRMGCFPLSWVBUKYJQX' < ciphertext.txt > output.txt

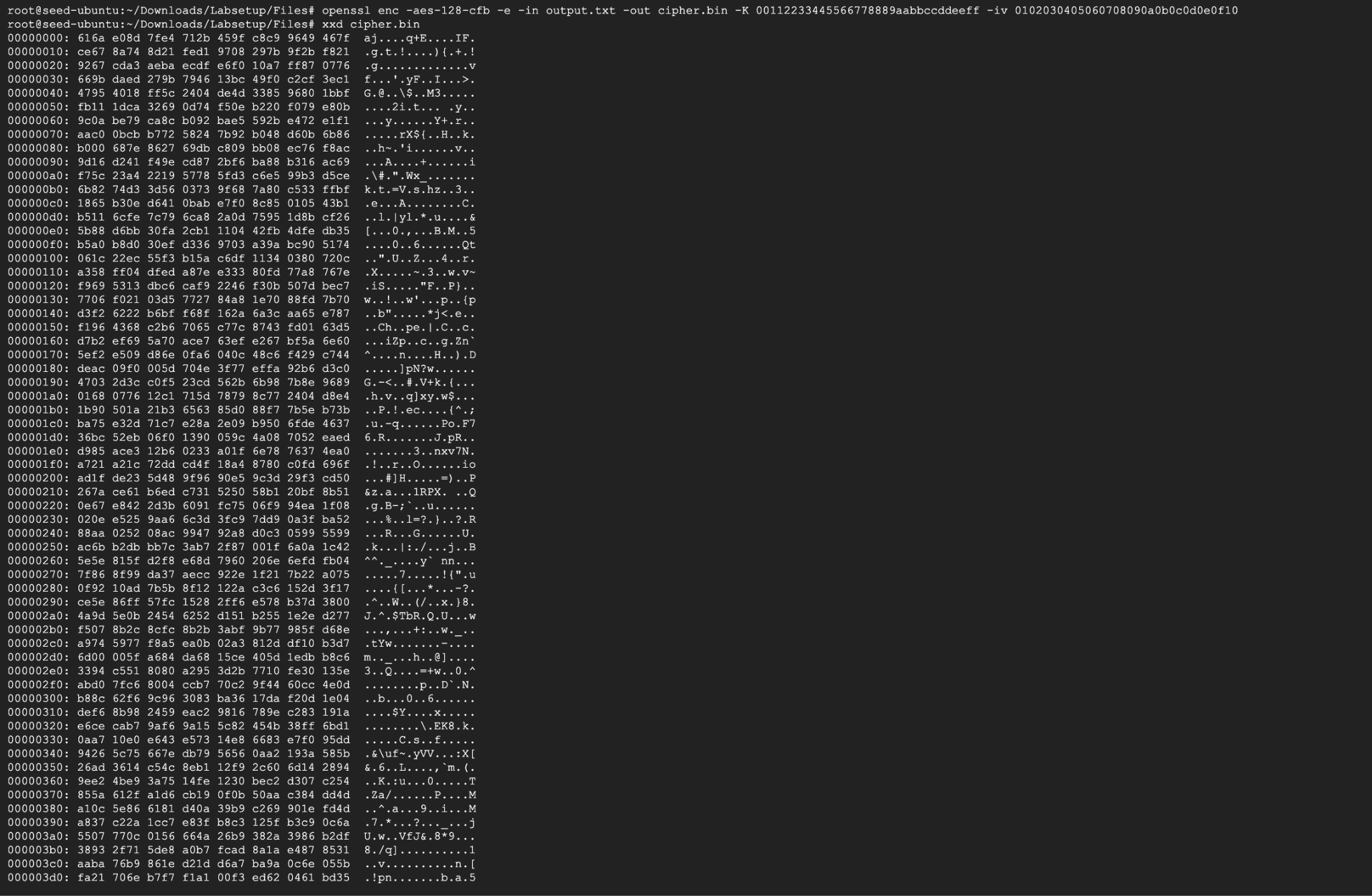
Final Output file content:



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

****

****

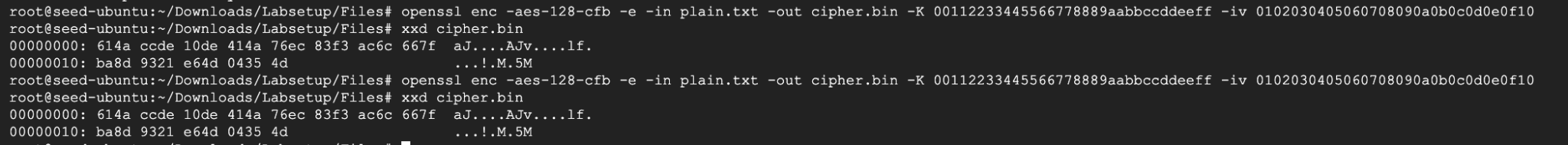
****

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

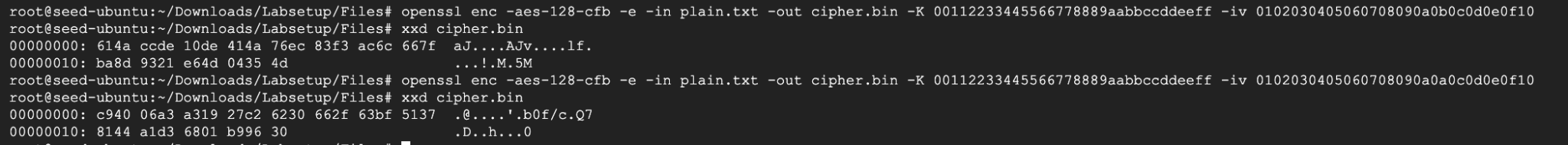
**Task 6.1**

1. **Same IV**

****

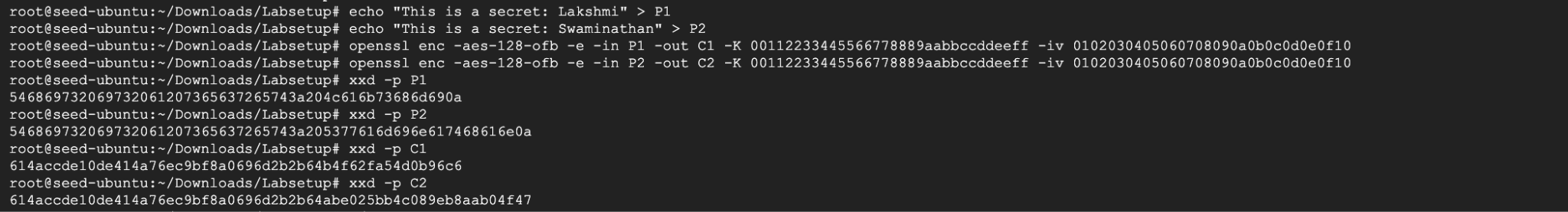
****

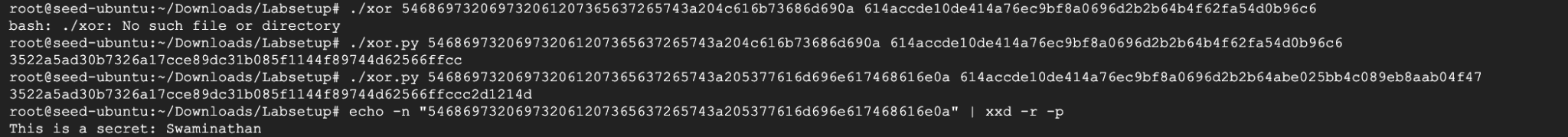
1. **Different IV**

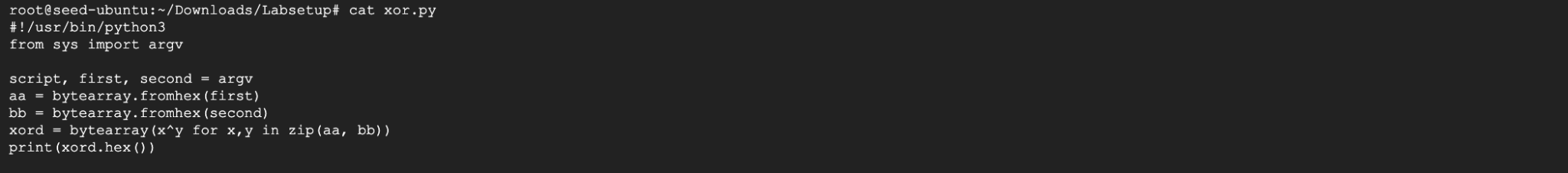


IV needs to be unique because if the content of the msg is same, encryption of that content will result in same ciphertext which can pave a way to backtrack and figure out the actual plain text is and can also be used to figure out encryption key and IV.

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

****

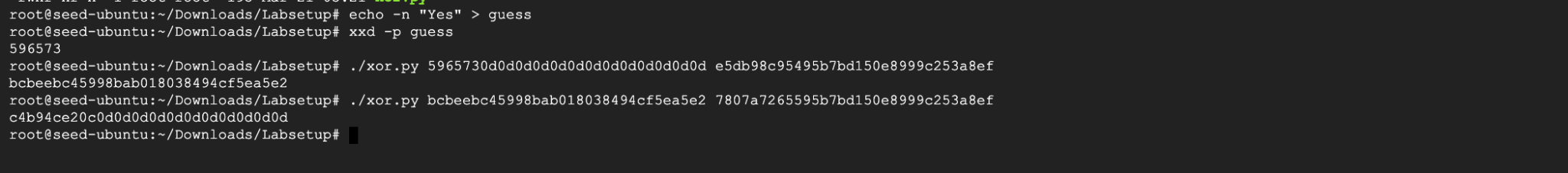
****

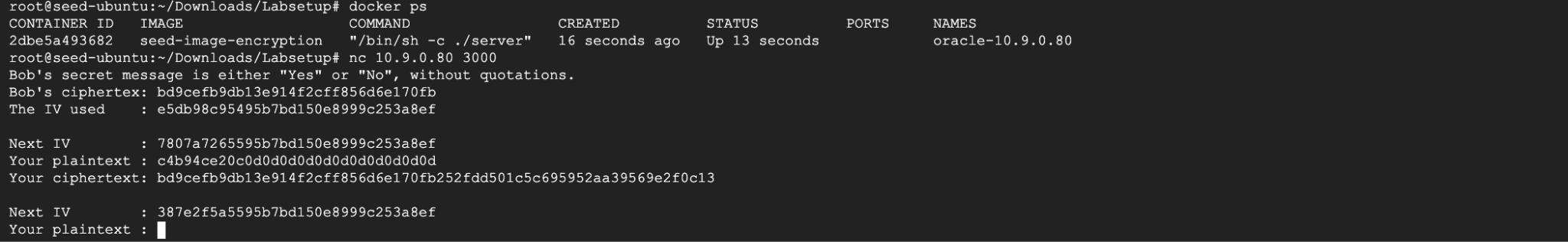
****

**Can he/she decrypt other encrypted messages if the IV is always the same?**

Yes, we can decrypt other encrypted messages if the IV is always the same

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

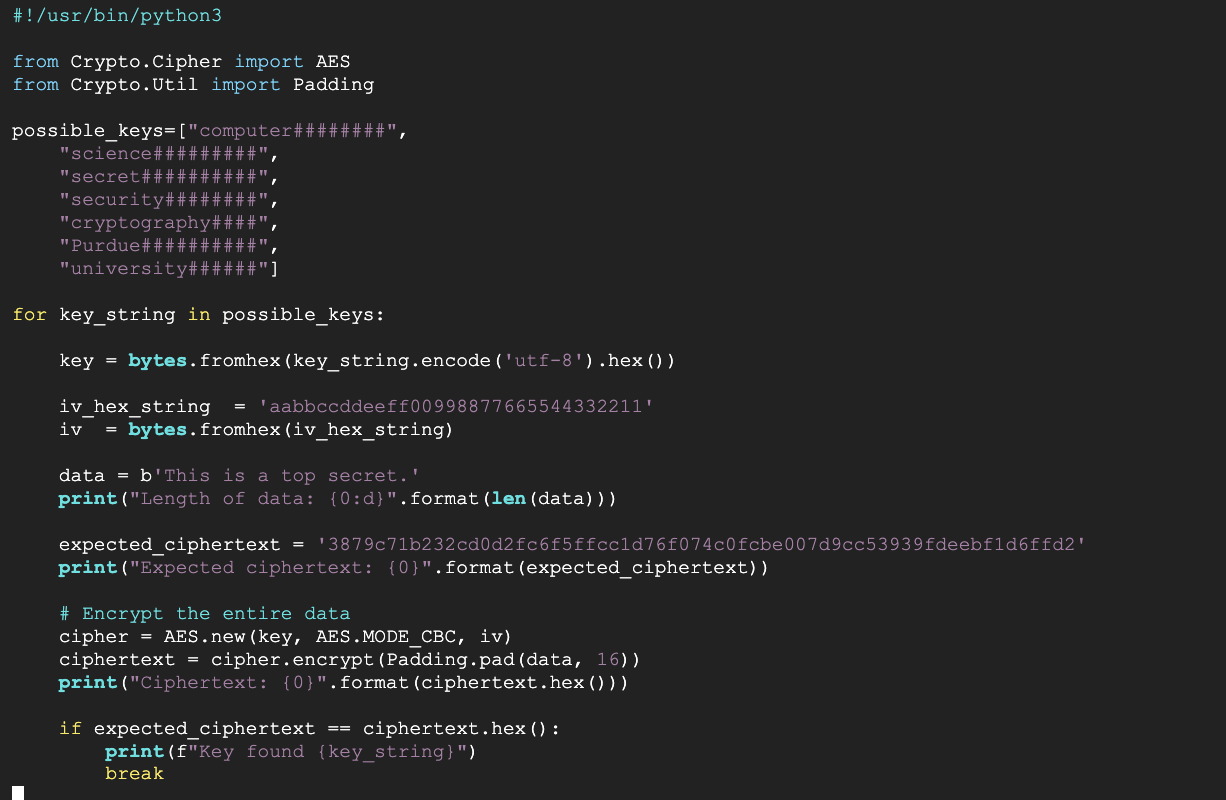
****

****

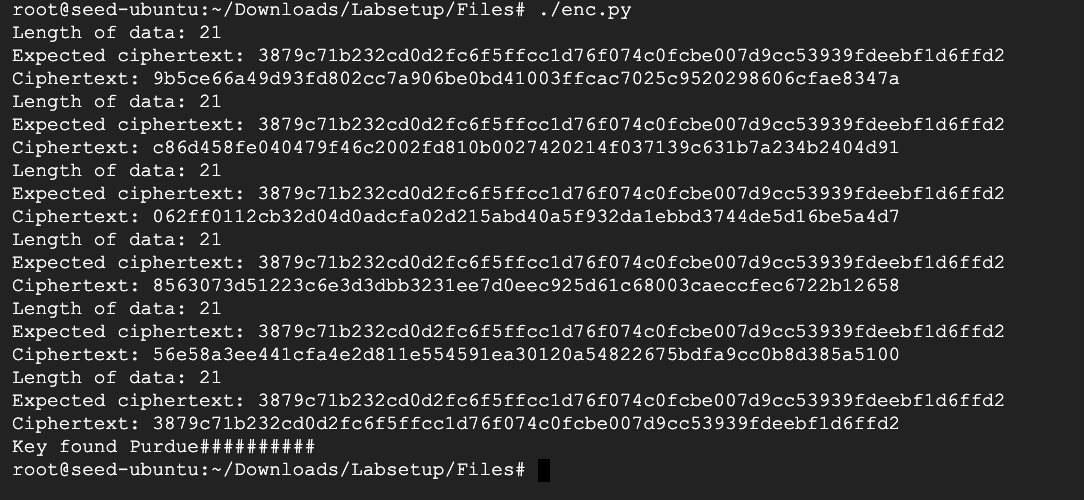
Therefore, the actual content of Bob’s secret message is “Yes”

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

**Code:**

****

**Output:**

****

Therefore, the encryption key used is “Purdue##########”