**APPLIED CRYPTOGRAPHY**

**LAB-2**

NAME: VISHWAS M

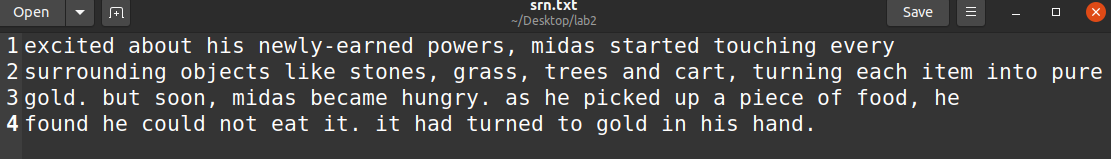
SRN: PES2UG20CS390

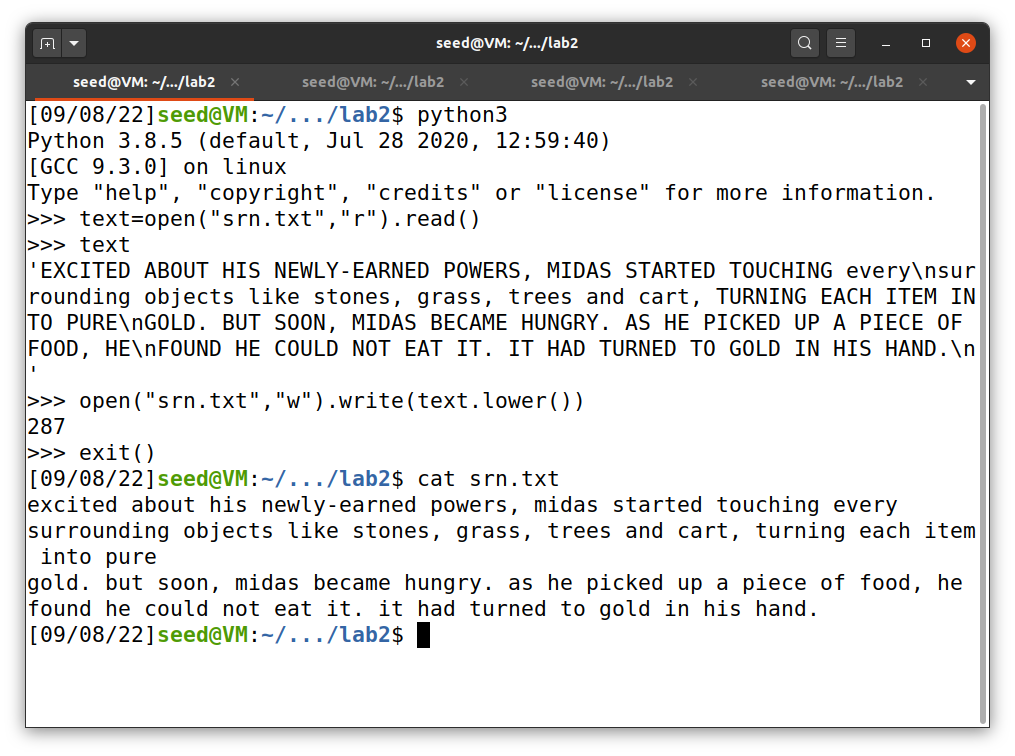
SEC: F

DATE: 08/09/2022

**Question 1**

Create and display a file SRN.txt with the following contents:





**Question 2**

In SRN.txt, convert uppercase letters to lowercase and find the frequencies of the following words:

a. he

b. h

c. ed

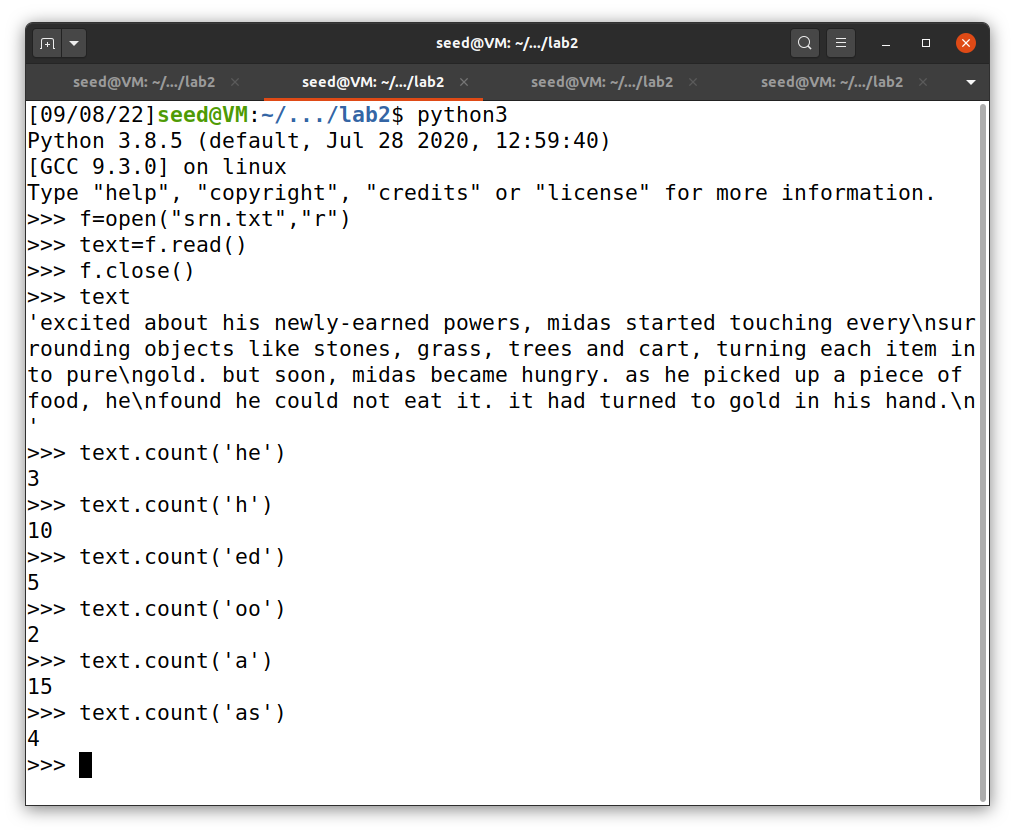
d. oo

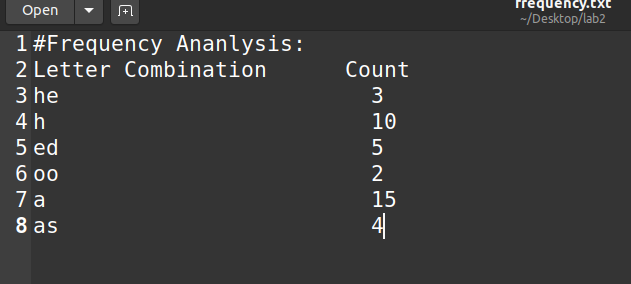
e. a

f. as

**Finding Frequencies**

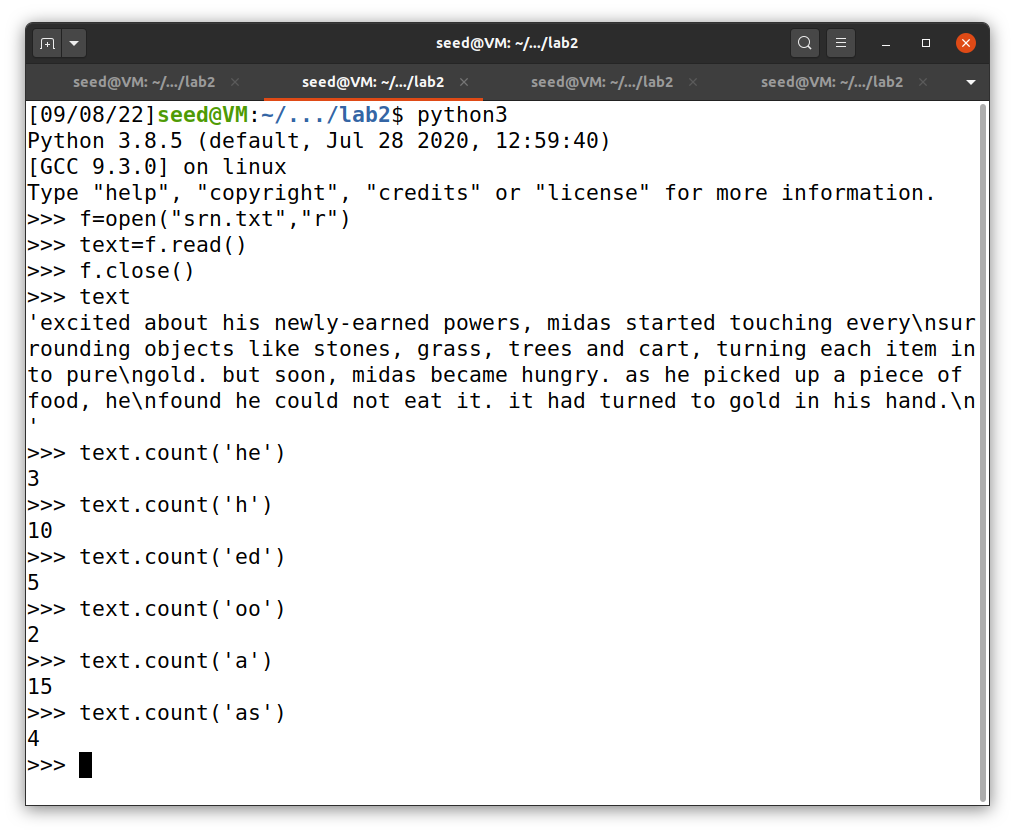
This is also achieved using python as follows:





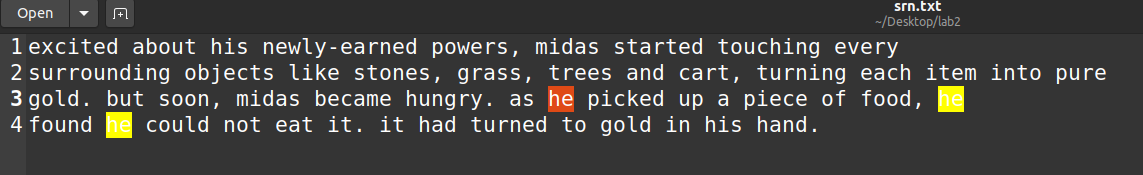
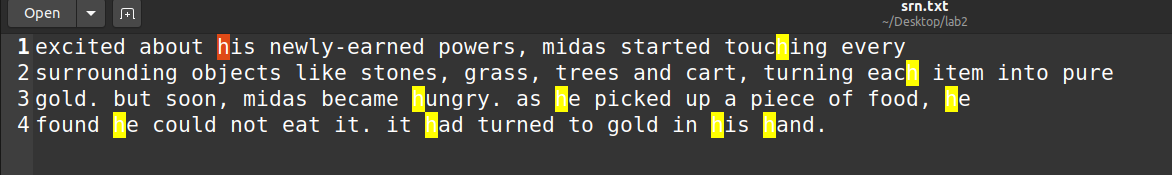
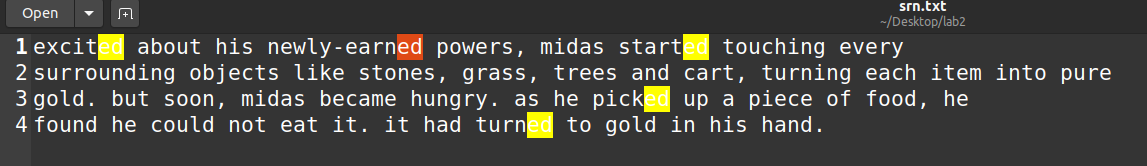
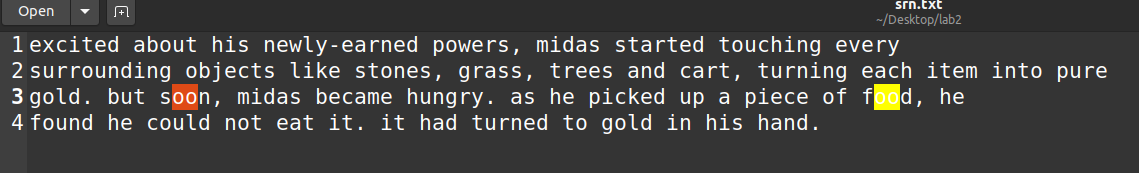
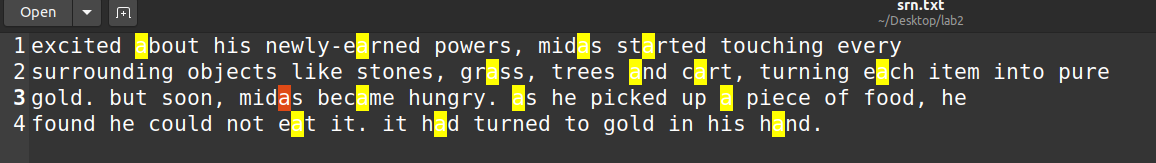
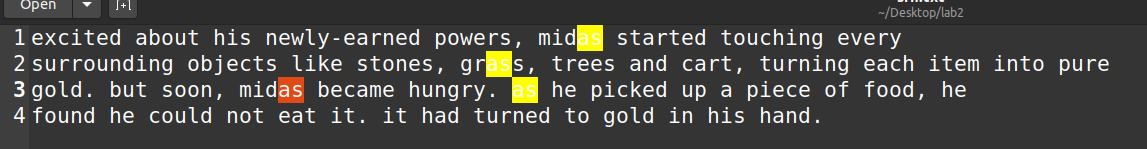
**Converting to lowercase**

A simple python script helps achieve this:



**Question 3**

Highlighting the words given in question 2

1. Occurrences of 'he' highlighted:
2. Occurrences of 'h' highlighted:
3. Occurrences of 'ed' highlighted:
4. Occurrences of 'oo' highlighted:
5. Occurrences of 'a' highlighted:
6. Occurrences of 'as' highlighted:

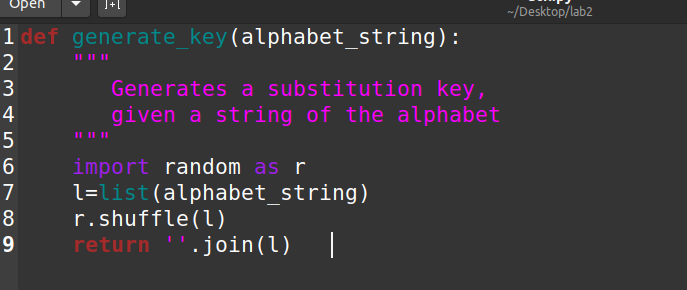
**Question 4**

Generate the substitution cipher key

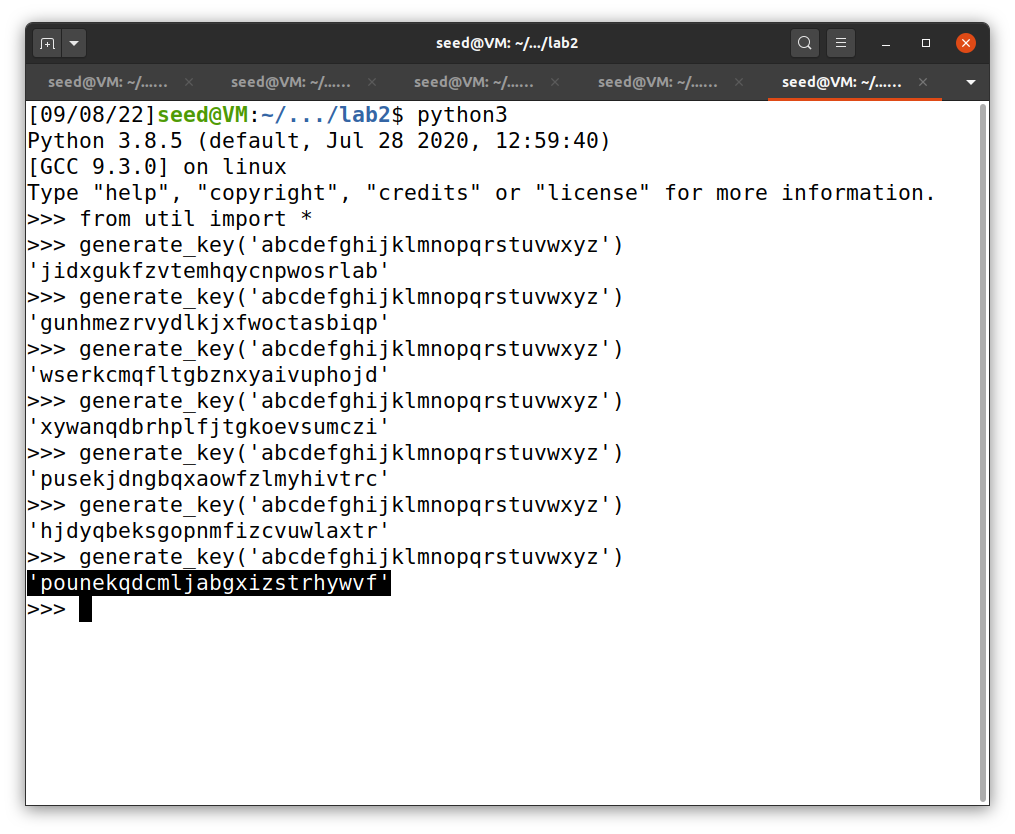
Python's random module has a 'shuffle' functionality that lets us generate random permutations of a list. This has been used to generate the

substitution cipher key from the alphabet. However, a key can be generated from online sources like random.org as well.

Function used to generate the key:



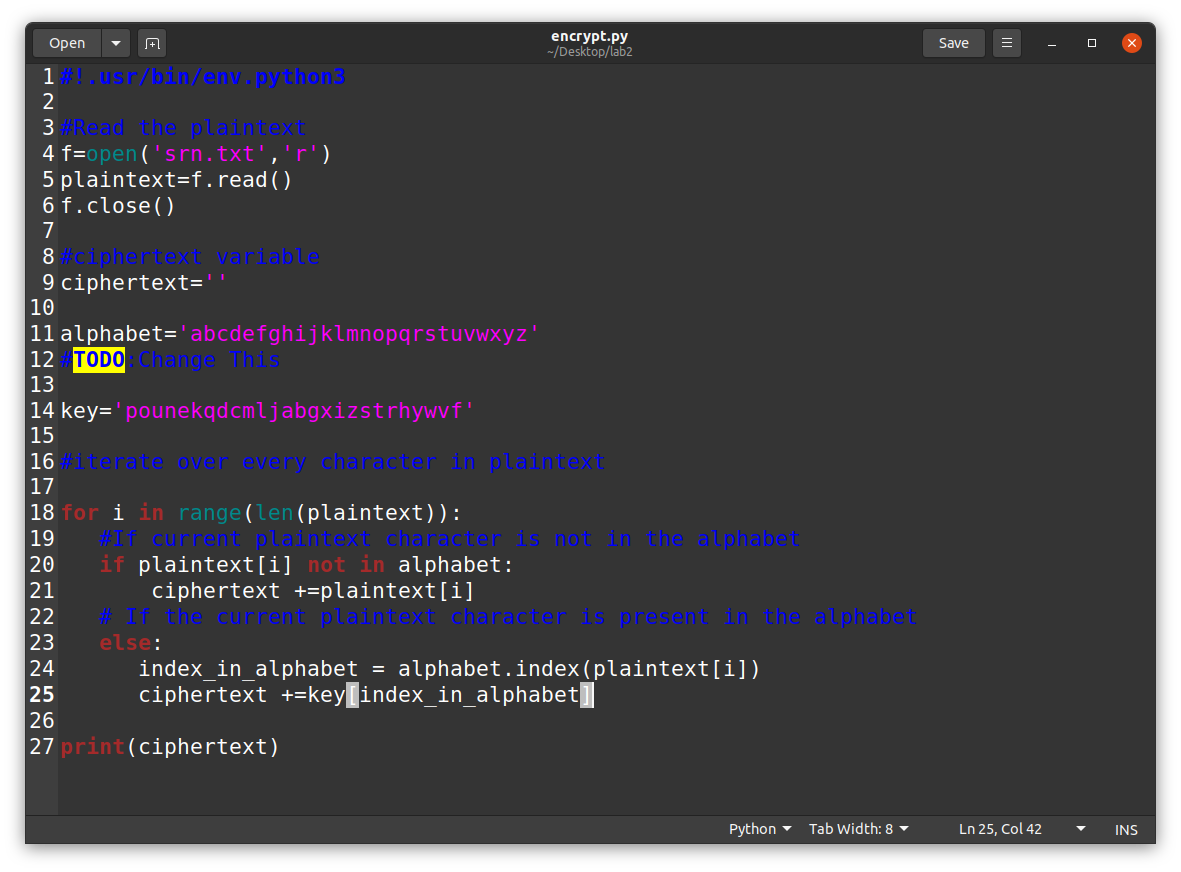
Key generation:

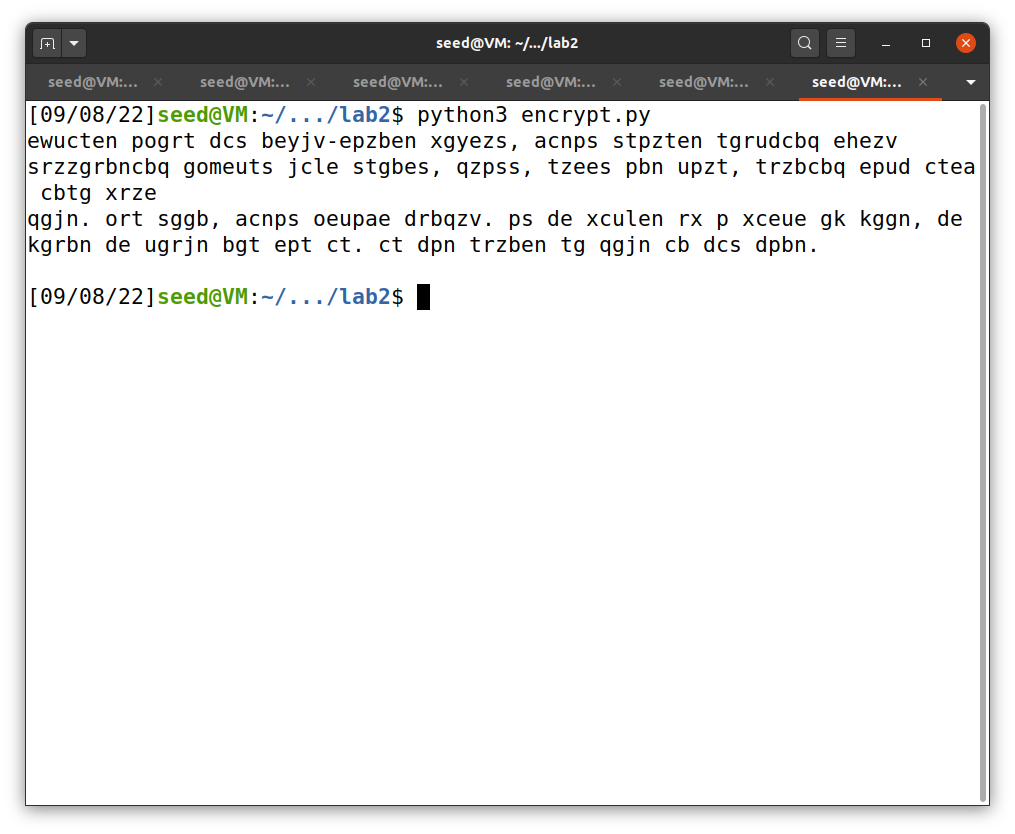


**Question 5**

Generate the ciphertext using the key generated in question 4

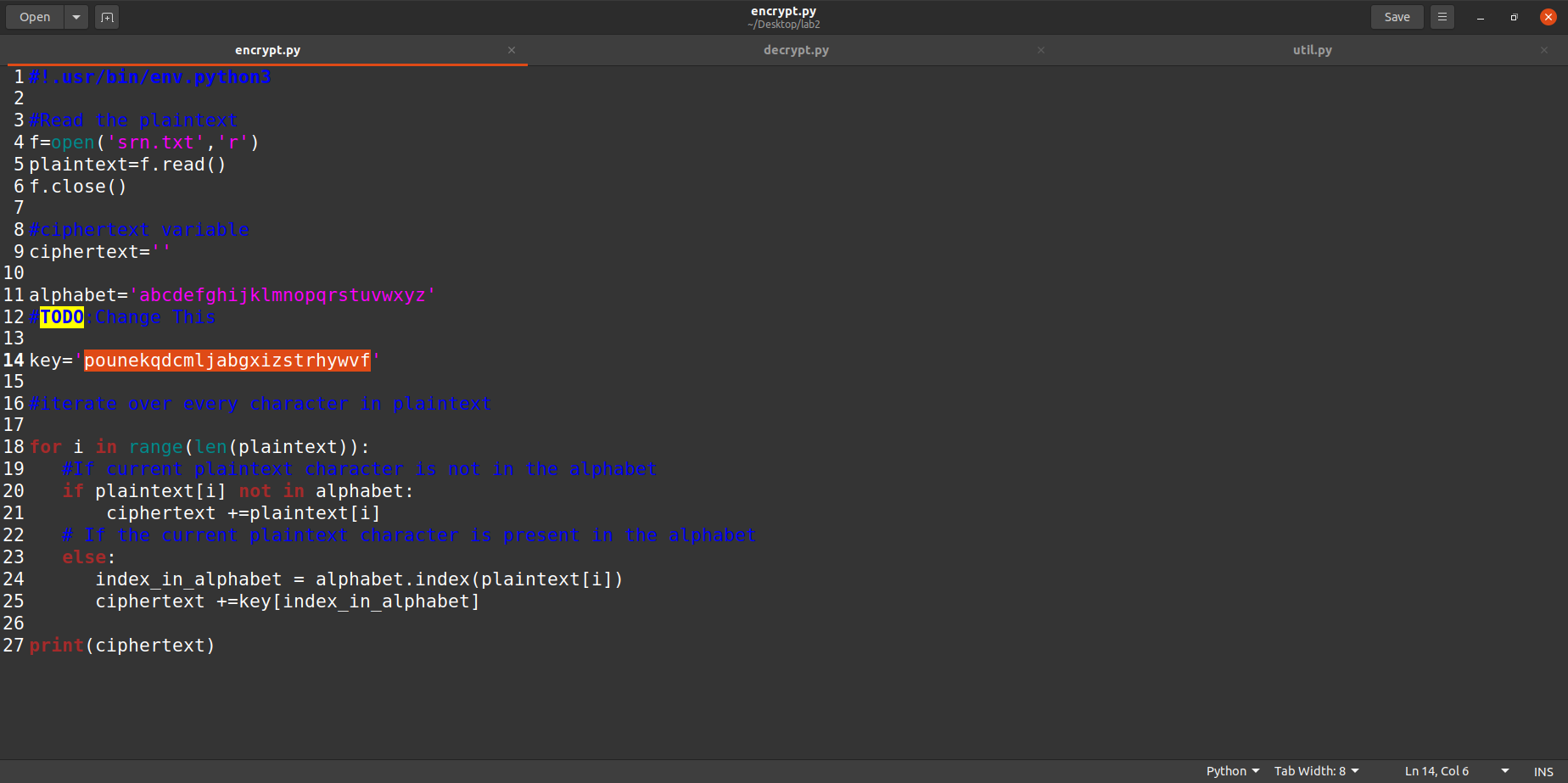
Writing a python script to achieve it:



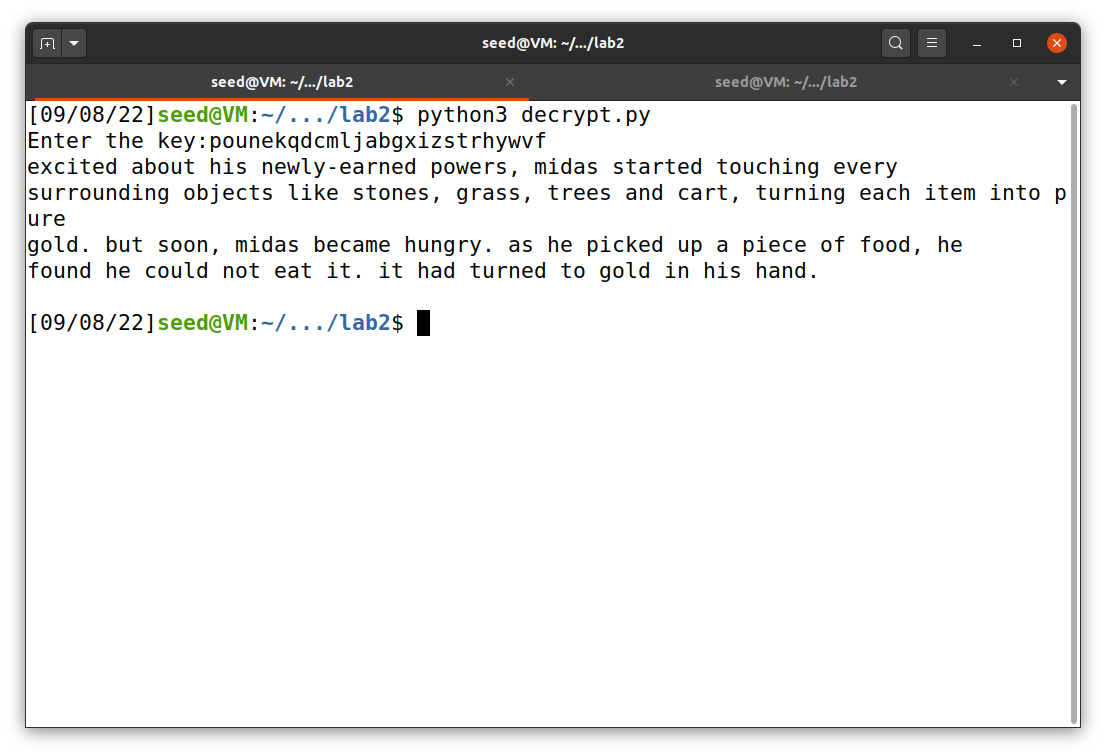
Ciphertext generated:

**Question 6**

Decrypt the ciphertext back to plaintext

The script used to achieve it:

Decrypted plaintext:

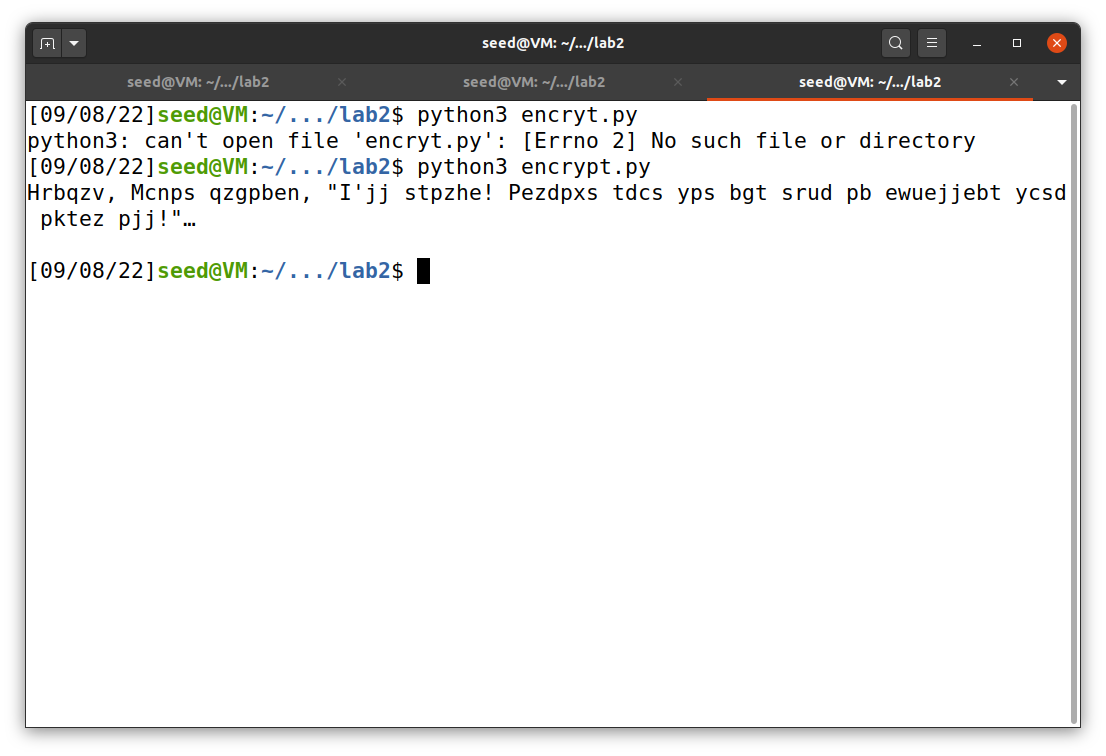


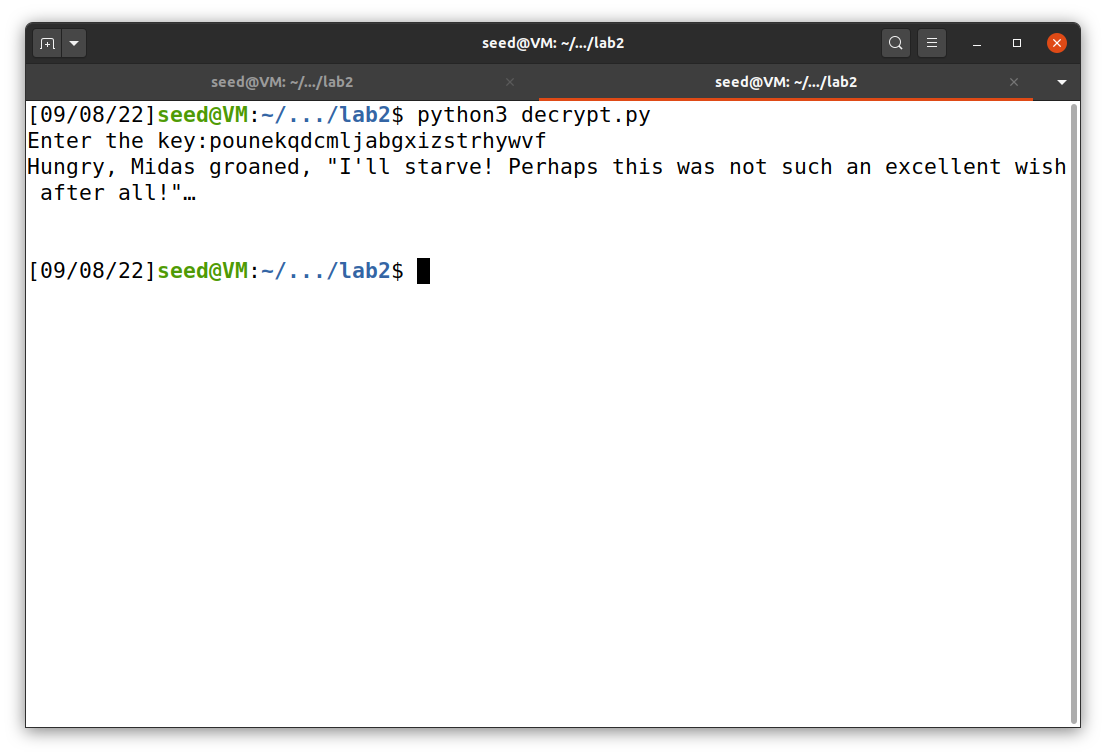
**Question 7**

Suppose the input file is:

Hungry, Midas groaned, "I'll starve! Perhaps this was not such an excellent wish after all!"…

Ciphertext generated:



Decrypted plaintext:

**Comment on the ciphertext generated:**

This ciphertext is shorter than the one before. The previous ciphertext, due to its long length, is more permeable to frequency analysis attacks. This ciphertext, though still insecure, is less vulnerable to frequency analysis attacks.

However, care must be taken to remove all punctuations, lest they give attackers hints as to the contents of the message (for example, it's pretty obvious that “ z'yy ” stands for “ i'll ”, hence two letters of the key are revealed).