

APPLIED CRYPTOGRAPHY

LAB-2

NAME: VISHWAS M

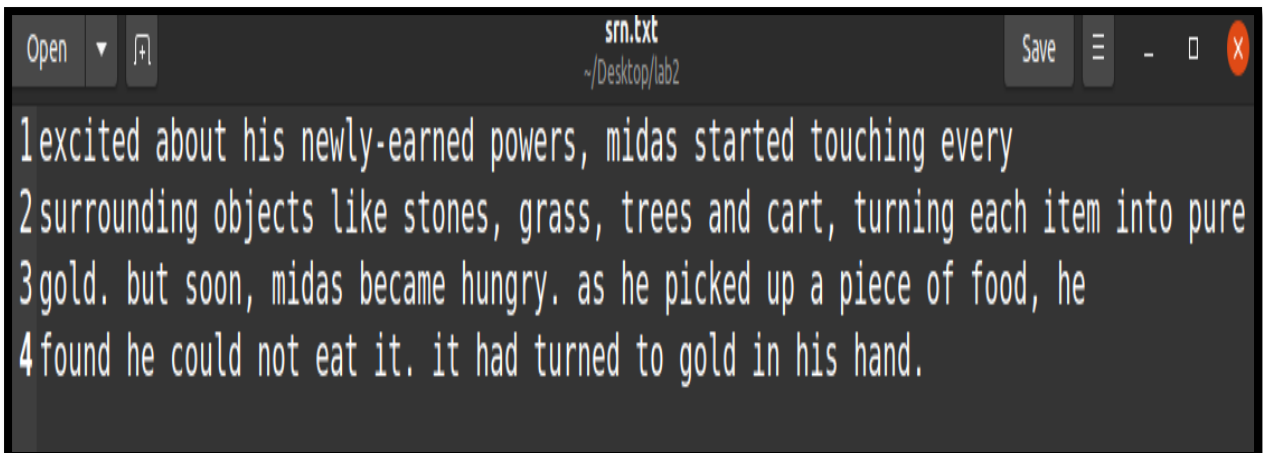
SRN: PES2UG20CS390

SEC: F

DATE: 08/09/2022

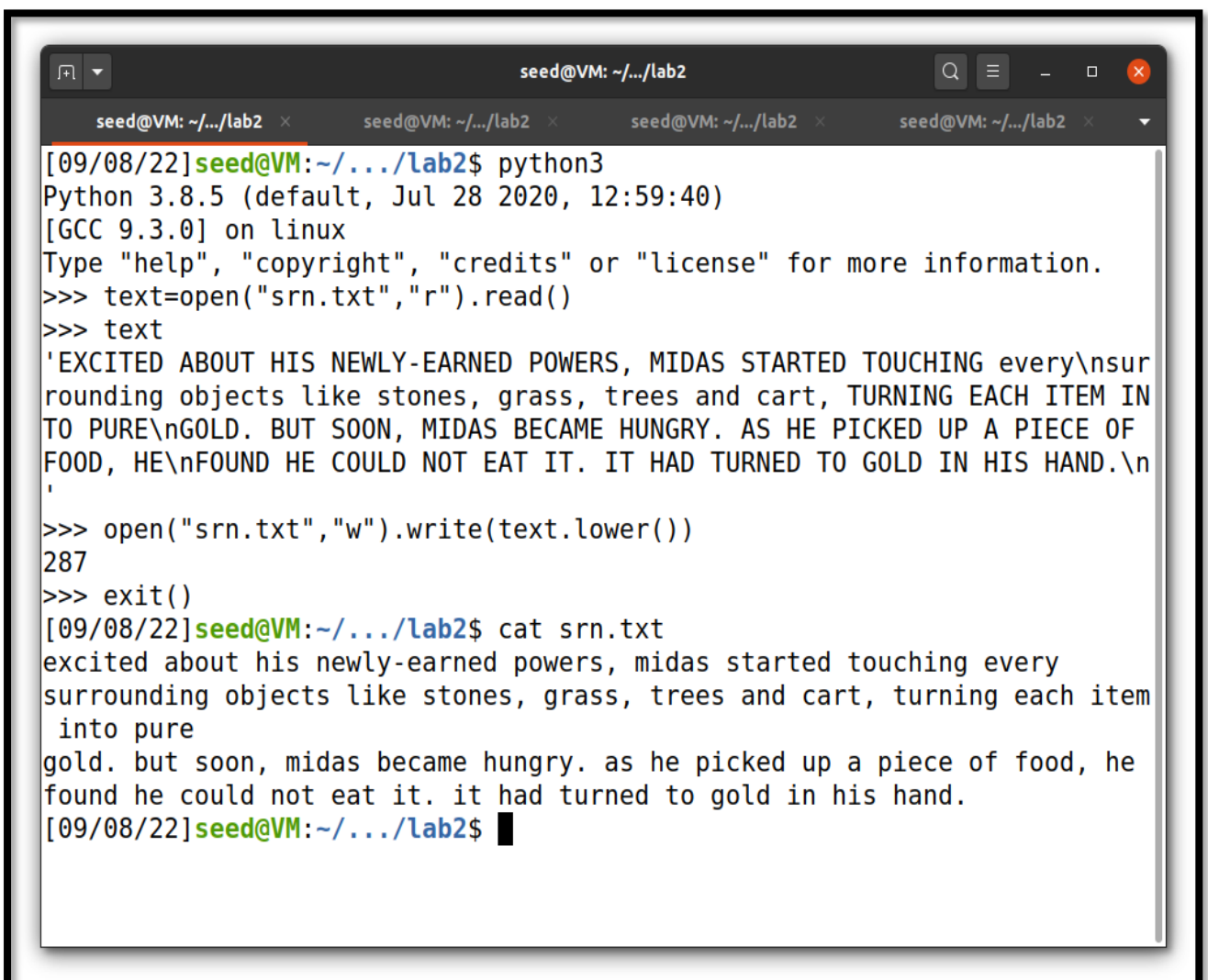
Question 1

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



A screenshot of a text editor window titled 'srn.txt' with a path of '~/Desktop/lab2'. The window contains four lines of text, each preceded by a line number (1-4). The text describes Midas's powers and his inability to eat food that turns to gold.

```
1excited about his newly-earned powers, midas started touching every
2surrounding objects like stones, grass, trees and cart, turning each item into pure
3gold. but soon, midas became hungry. as he picked up a piece of food, he
4found he could not eat it. it had turned to gold in his hand.
```



A screenshot of a terminal window titled 'seed@VM: ~/.../lab2'. It shows the execution of Python 3.8.5 to create a file 'srn.txt' and then use 'cat' to display its contents. The text in the terminal is as follows:

```
[09/08/22]seed@VM:~/.../lab2$ python3
Python 3.8.5 (default, Jul 28 2020, 12:59:40)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> text=open("srn.txt","r").read()
>>> text
'EXCITED ABOUT HIS NEWLY-EARNED POWERS, MIDAS STARTED TOUCHING every\nsur
rounding objects like stones, grass, trees and cart, TURNING EACH ITEM IN
TO PURE\nGOLD. BUT SOON, MIDAS BECAME HUNGRY. AS HE PICKED UP A PIECE OF
FOOD, HE\nFOUND HE COULD NOT EAT IT. IT HAD TURNED TO GOLD IN HIS HAND.\n'
>>> open("srn.txt","w").write(text.lower())
287
>>> exit()
[09/08/22]seed@VM:~/.../lab2$ cat srn.txt
excited about his newly-earned powers, midas started touching every
surrounding objects like stones, grass, trees and cart, turning each item
into pure
gold. but soon, midas became hungry. as he picked up a piece of food, he
found he could not eat it. it had turned to gold in his hand.
[09/08/22]seed@VM:~/.../lab2$
```

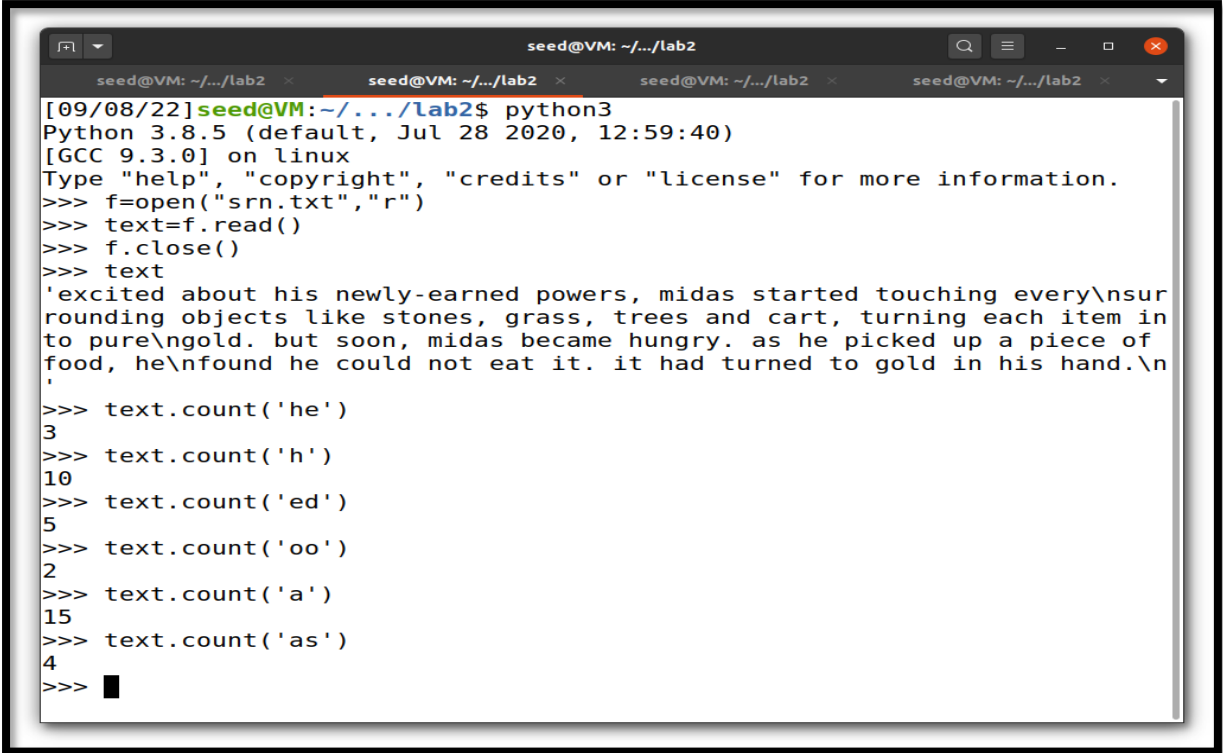
Question 2

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

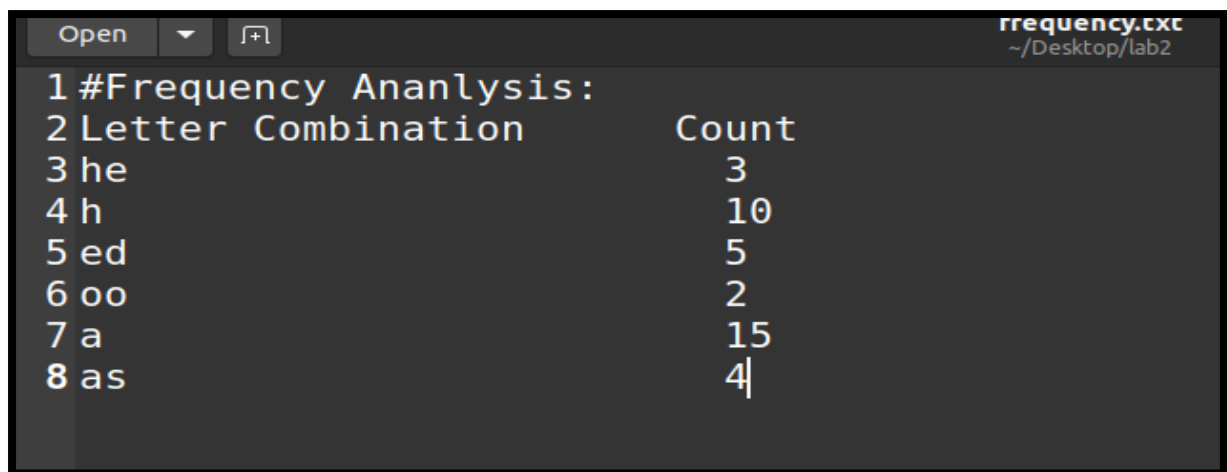
- a. he
- b. h
- c. ed
- d. oo
- e. a
- f. as

Finding Frequencies

This is also achieved using python as follows:



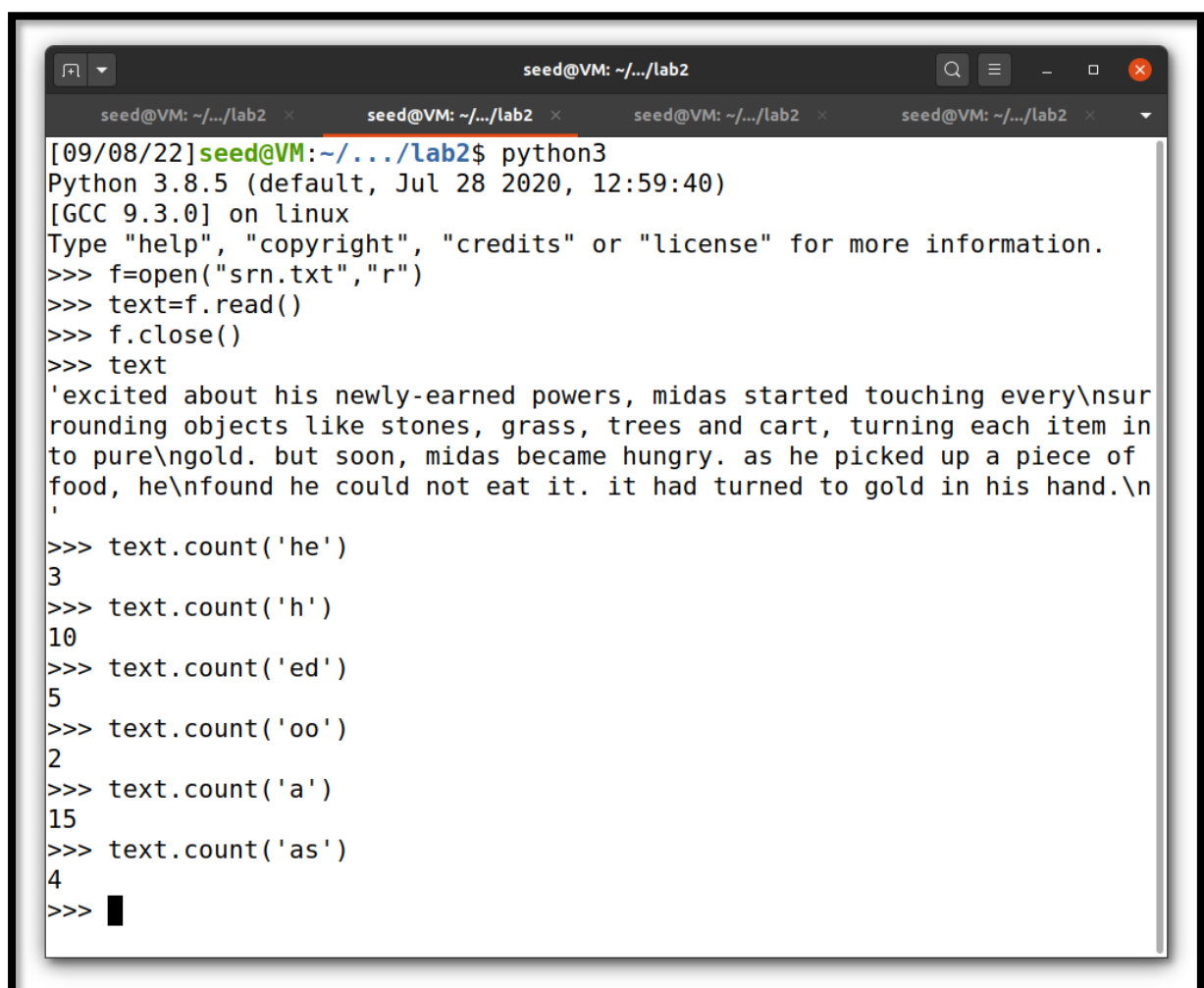
```
seed@VM: ~/.../lab2
[09/08/22] seed@VM: ~/.../lab2$ python3
Python 3.8.5 (default, Jul 28 2020, 12:59:40)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> f=open("srn.txt","r")
>>> text=f.read()
>>> f.close()
>>> text
'excited about his newly-earned powers, midas started touching every\nsur
rounding objects like stones, grass, trees and cart, turning each item in
to pure\ngold. but soon, midas became hungry. as he picked up a piece of
food, he\nfound he could not eat it. it had turned to gold in his hand.\n'
>>> text.count('he')
3
>>> text.count('h')
10
>>> text.count('ed')
5
>>> text.count('oo')
2
>>> text.count('a')
15
>>> text.count('as')
4
>>> █
```



```
Open  [+] frequency.txt ~/Desktop/lab2
1 #Frequency Ananlysis:
2 Letter Combination      Count
3 he                      3
4 h                      10
5 ed                     5
6 oo                     2
7 a                      15
8 as                      4
```

Converting to lowercase

A simple python script helps achieve this:



```
seed@VM: ~/.../lab2
[09/08/22]seed@VM:~/.../lab2$ python3
Python 3.8.5 (default, Jul 28 2020, 12:59:40)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> f=open("srn.txt","r")
>>> text=f.read()
>>> f.close()
>>> text
'excited about his newly-earned powers, midas started touching every\nsurrounding objects like stones, grass, trees and cart, turning each item in to pure\ngold. but soon, midas became hungry. as he picked up a piece of food, he\nfound he could not eat it. it had turned to gold in his hand.\n'
>>> text.count('he')
3
>>> text.count('h')
10
>>> text.count('ed')
5
>>> text.count('oo')
2
>>> text.count('a')
15
>>> text.count('as')
4
>>>
```

Question 3

Highlighting the words given in question 2

a) Occurrences of 'he' highlighted:

```
srn.txt
~/Desktop/lab2

1excited about his newly-earned powers, midas started touching every
2surrounding objects like stones, grass, trees and cart, turning each item into pure
3gold. but soon, midas became hungry. as he picked up a piece of food, he
4found he could not eat it. it had turned to gold in his hand.
```

b) Occurrences of 'h' highlighted:

```
srn.txt
~/Desktop/lab2

1excited about his newly-earned powers, midas started touching every
2surrounding objects like stones, grass, trees and cart, turning each item into pure
3gold. but soon, midas became hungry. as he picked up a piece of food, he
4found he could not eat it. it had turned to gold in his hand.
```

c) Occurrences of 'ed' highlighted:

```
srn.txt
~/Desktop/lab2

1excited about his newly-earned powers, midas started touching every
2surrounding objects like stones, grass, trees and cart, turning each item into pure
3gold. but soon, midas became hungry. as he picked up a piece of food, he
4found he could not eat it. it had turned to gold in his hand.
```

d) Occurrences of 'oo' highlighted:

```
srn.txt
~/Desktop/lab2

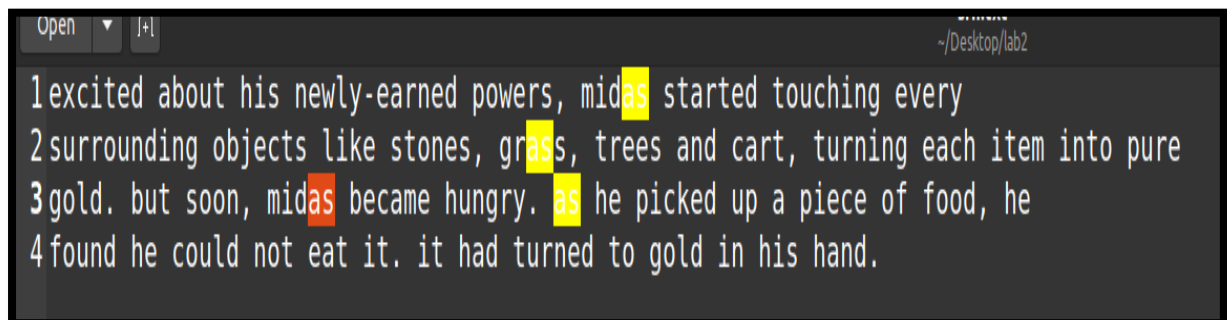
1excited about his newly-earned powers, midas started touching every
2surrounding objects like stones, grass, trees and cart, turning each item into pure
3gold. but soon, midas became hungry. as he picked up a piece of food, he
4found he could not eat it. it had turned to gold in his hand.
```

e) Occurrences of 'a' highlighted:



```
1excited aabout his newly-earned powers, midas started touching every
2surrounding objects like stones, grass, trees and cart, turning each item into pure
3gold. but soon, midas became hungry. as he picked up a piece of food, he
4found he could not eat it. it had turned to gold in his hand.
```

f) Occurrences of 'as' highlighted:



```
1excited about his newly-earned powers, midas started touching every
2surrounding objects like stones, grass, trees and cart, turning each item into pure
3gold. but soon, midas became hungry. as he picked up a piece of food, he
4found he could not eat it. it had turned to gold in his hand.
```

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:

```
Open  J+|  ~/Desktop/lab2
1 def generate_key(alphabet_string):
2     """
3     Generates a substitution key,
4     given a string of the alphabet
5     """
6     import random as r
7     l=list(alphabet_string)
8     r.shuffle(l)
9     return ''.join(l) |
```

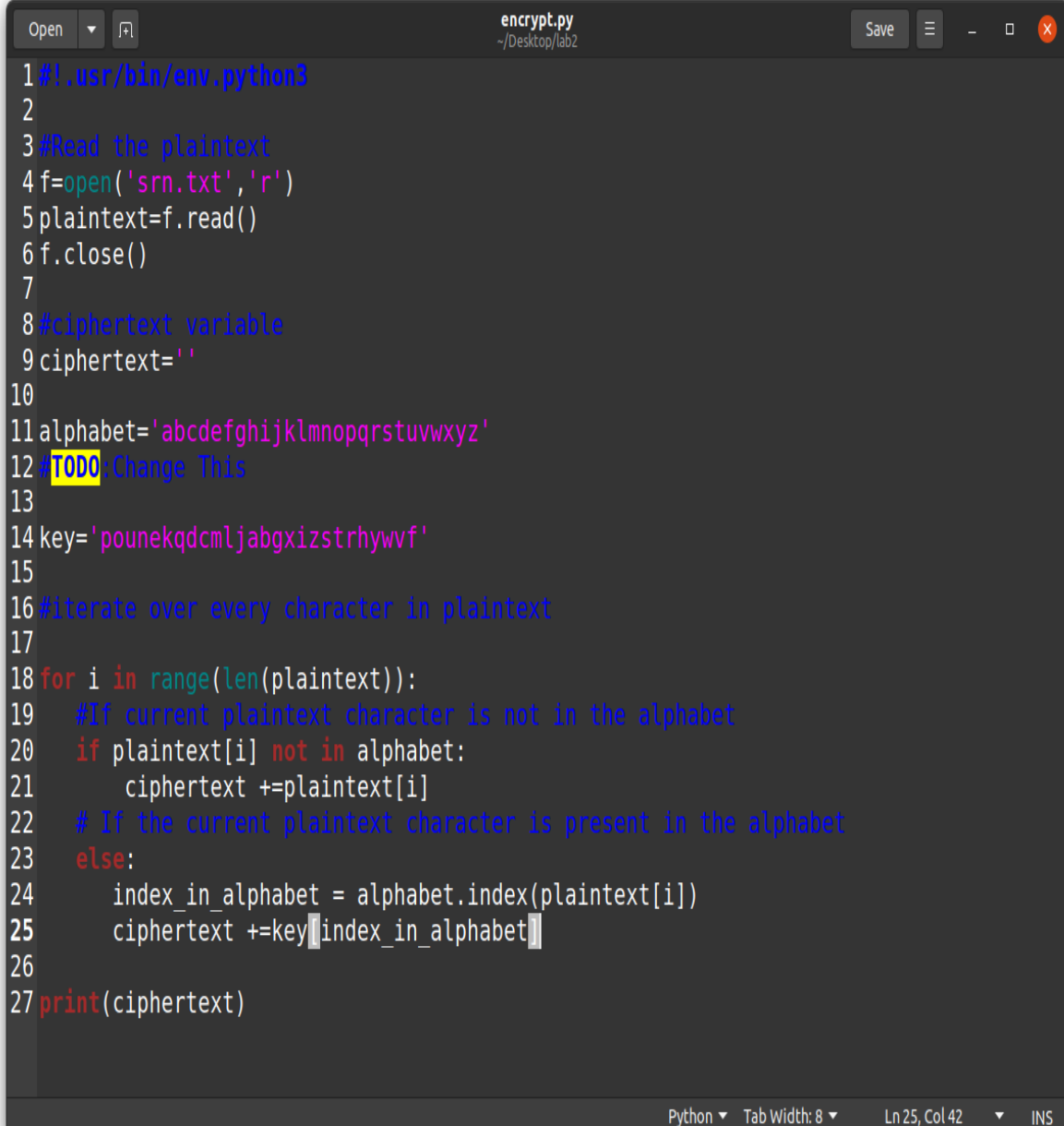
Key generation:

```
seed@VM: ~/.../lab2
[09/08/22] seed@VM: ~/.../lab2$ python3
Python 3.8.5 (default, Jul 28 2020, 12:59:40)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> from util import *
>>> generate_key('abcdefghijklmnopqrstuvwxyz')
'jidxgukfzvtemhqycnpwosrlab'
>>> generate_key('abcdefghijklmnopqrstuvwxyz')
'gunhmezrvydlkxfwoctasbiqp'
>>> generate_key('abcdefghijklmnopqrstuvwxyz')
'wserkcmqfltgbnxyaivuphojd'
>>> generate_key('abcdefghijklmnopqrstuvwxyz')
'xywanqdbhrplfjtgkoevsumczi'
>>> generate_key('abcdefghijklmnopqrstuvwxyz')
'pusekjdnbgqxaowfzlmvihvtrc'
>>> generate_key('abcdefghijklmnopqrstuvwxyz')
'hjdyqbeksgopnmfizcvuwlaxtr'
>>> generate_key('abcdefghijklmnopqrstuvwxyz')
'pounekqdcmljabgxizstrhywvf'
>>>
```

Question 5

Generate the ciphertext using the key generated in question 4

Writing a python script to achieve it:



```
1#!/usr/bin/env python3
2
3#Read the plaintext
4f=open('srn.txt','r')
5plaintext=f.read()
6f.close()
7
8#ciphertext variable
9ciphertext=''
10
11alphabet='abcdefghijklmnopqrstuvwxyz'
12#TODO:Change This
13
14key='pounekqdcmljabgxizstrhywvf'
15
16#iterate over every character in plaintext
17
18for i in range(len(plaintext)):
19    #If current plaintext character is not in the alphabet
20    if plaintext[i] not in alphabet:
21        ciphertext +=plaintext[i]
22    # If the current plaintext character is present in the alphabet
23    else:
24        index_in_alphabet = alphabet.index(plaintext[i])
25        ciphertext +=key[index_in_alphabet]
26
27print(ciphertext)
```

Python Tab Width: 8 Ln 25, Col 42 INS

Ciphertext generated:

A terminal window titled 'seed@VM: ~/.../lab2' with multiple tabs. The terminal shows the execution of 'python3 encrypt.py' which outputs a ciphertext. The prompt is '[09/08/22] seed@VM:~/.../lab2\$' followed by a cursor.

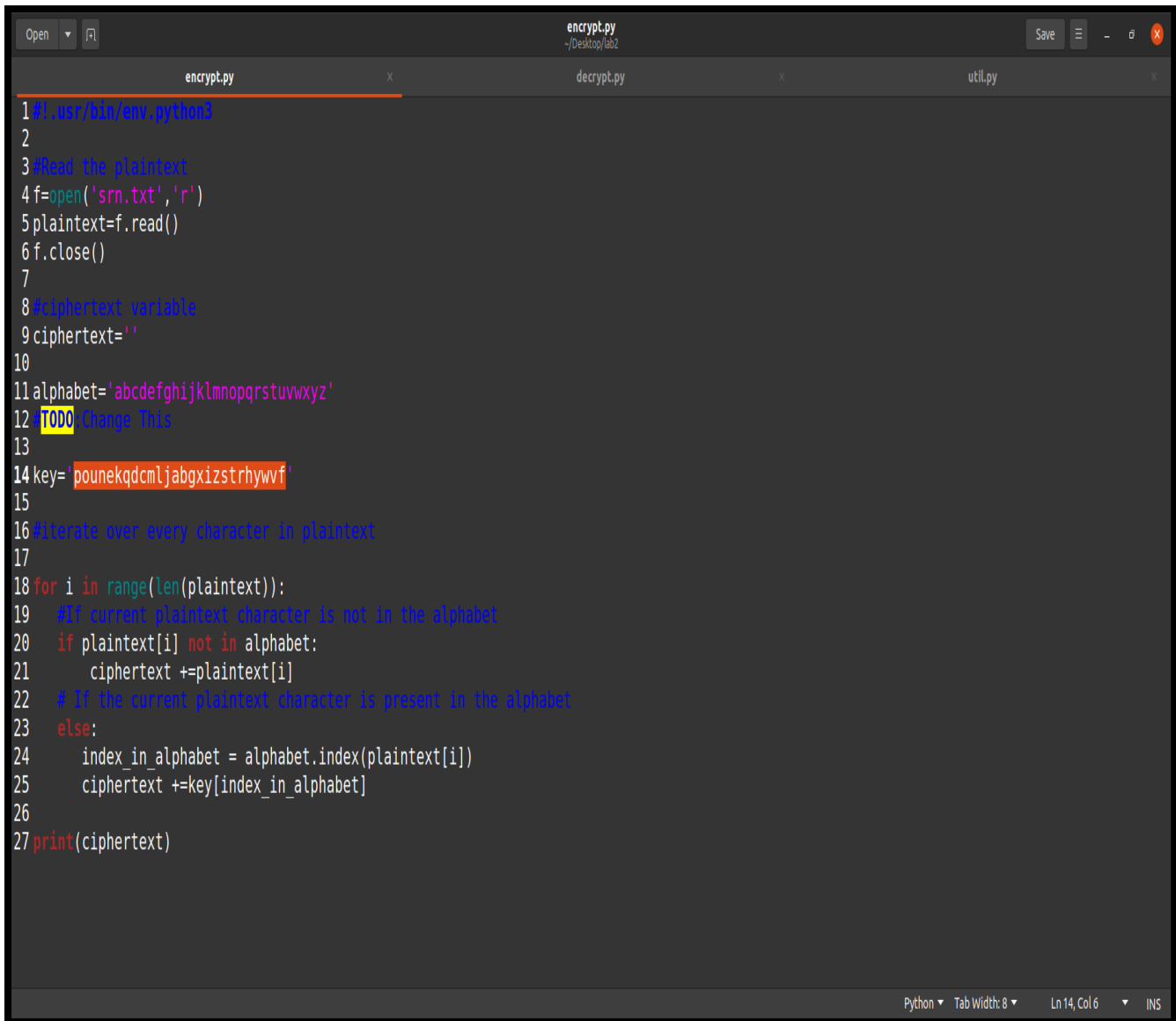
```
[09/08/22] seed@VM:~/.../lab2$ python3 encrypt.py
ewucten pogrt dcs beyjv-epzben xgyezs, acnps stpzten tgrudcbq ehezv
srzzgrbncbq gomeuts jcle stgbes, qzpss, tzees pbn upzt, trzbcbq epud ctea
cbtg xrze
qgjn. ort sggb, acnps oeupae drbqzv. ps de xculen rx p xceue gk kggn, de
kgrbn de ugrjn bgt ept ct. ct dpn trzben tg qgjn cb dcs dpbn.

[09/08/22] seed@VM:~/.../lab2$
```

Question 6

Decrypt the ciphertext back to plaintext

The script used to achieve it:

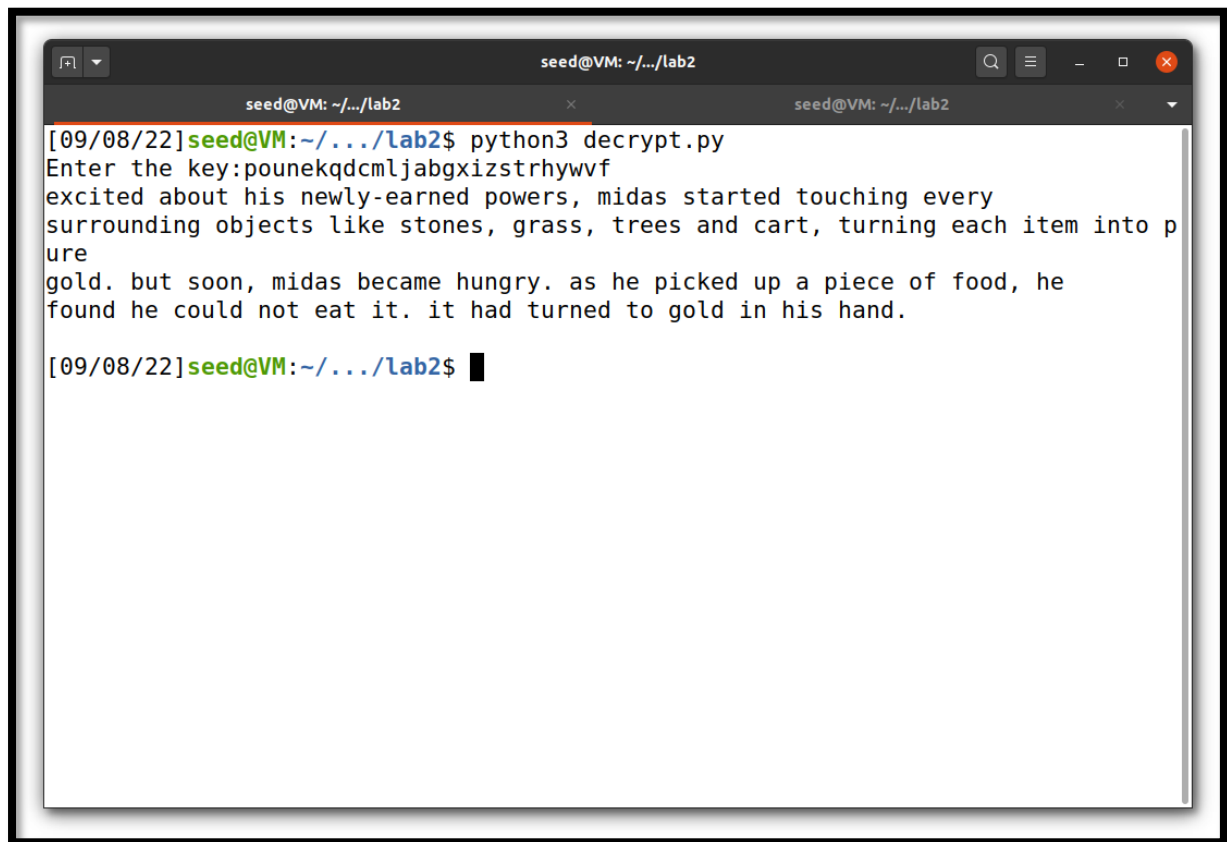


The image shows a code editor window with three tabs: 'encrypt.py', 'decrypt.py', and 'util.py'. The 'encrypt.py' tab is active and displays a Python script. The script reads a file 'srn.txt', iterates over its characters, and encrypts them using a Vigenere cipher. A 'TODO' comment is present on line 12, and a key is defined on line 14. The script uses a standard alphabet and a custom key to perform the encryption.

```
1#!/usr/bin/env python3
2
3#Read the plaintext
4f=open('srn.txt','r')
5plaintext=f.read()
6f.close()
7
8#cipher text variable
9ciphertext=''
10
11alphabet='abcdefghijklmnopqrstuvwxyz'
12TODO:Change This
13
14key='pounekqdcmljabgxizstrhywvf'
15
16#iterate over every character in plaintext
17
18for i in range(len(plaintext)):
19    #If current plaintext character is not in the alphabet
20    if plaintext[i] not in alphabet:
21        ciphertext +=plaintext[i]
22    # If the current plaintext character is present in the alphabet
23    else:
24        index_in_alphabet = alphabet.index(plaintext[i])
25        ciphertext +=key[index_in_alphabet]
26
27print(ciphertext)
```

Python ▾ Tab Width: 8 ▾ Ln 14, Col 6 ▾ INS

Decrypted plaintext:

A terminal window titled 'seed@VM: ~/.../lab2' with three tabs. The active tab shows the command 'python3 decrypt.py' being executed. The output displays a key and a paragraph of text. The text is a story about Midas, where he turns everything he touches into gold, but then becomes hungry and cannot eat because his food has also turned into gold.

```
[09/08/22]seed@VM:~/.../lab2$ python3 decrypt.py
Enter the key:pounekqdcmljabgxizstrhywvf
excited about his newly-earned powers, midas started touching every
surrounding objects like stones, grass, trees and cart, turning each item into p
ure
gold. but soon, midas became hungry. as he picked up a piece of food, he
found he could not eat it. it had turned to gold in his hand.

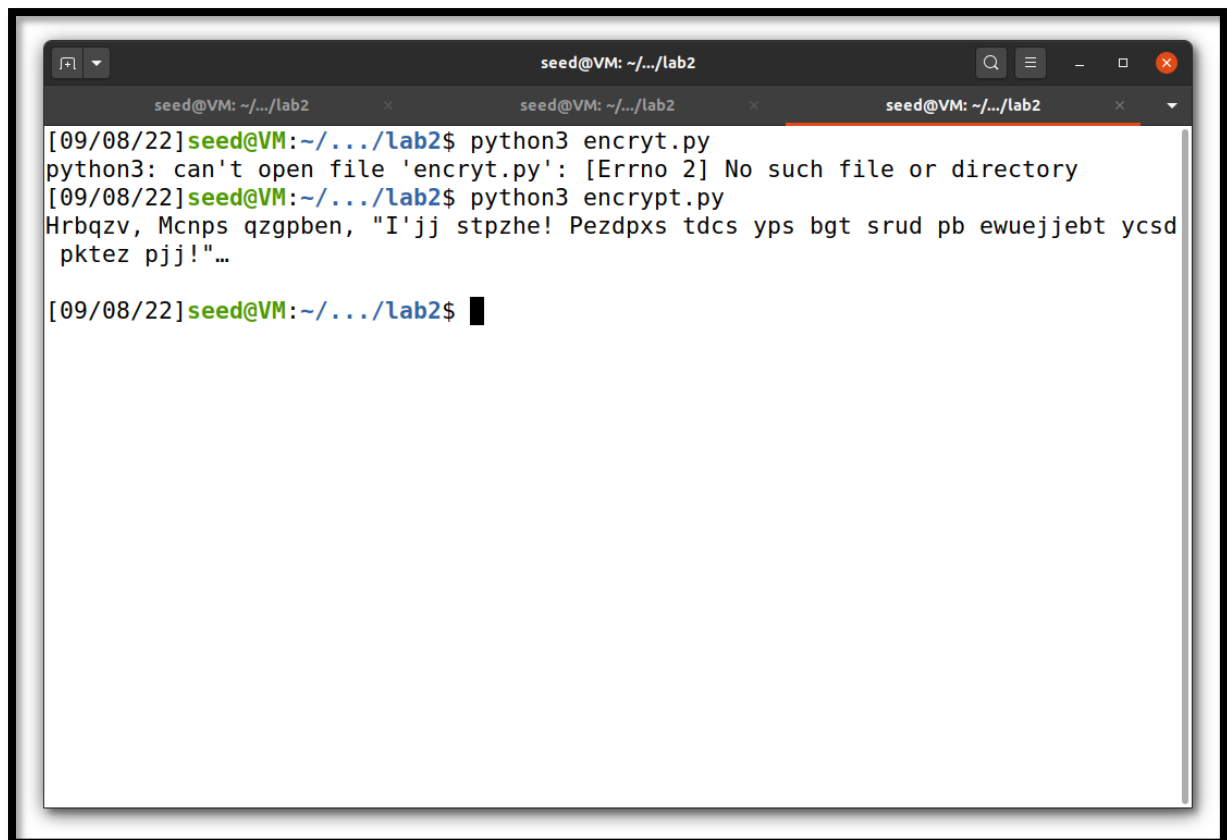
[09/08/22]seed@VM:~/.../lab2$
```

Question 7

Suppose the input file is:

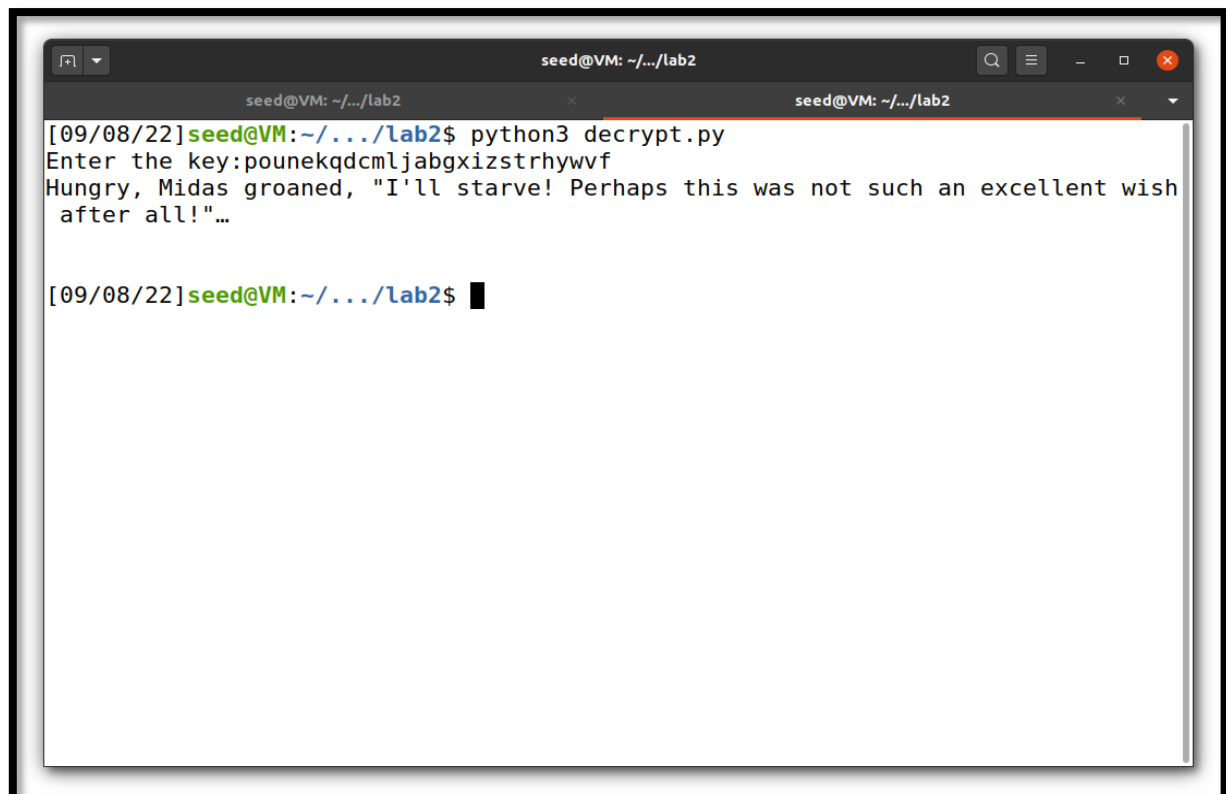
Hungry, Midas groaned, "I'll starve!
Perhaps this was not such an
excellent wish after all!"...

Ciphertext generated:

A terminal window titled 'seed@VM: ~/.../lab2' with three tabs. The first tab shows the command 'python3 encryt.py' and an error message: 'python3: can't open file 'encryt.py': [Errno 2] No such file or directory'. The second tab shows the command 'python3 encrypt.py' and the output: 'Hrbqzv, Mcnps qzgpben, "I'jj stpzhe! Pezdpxs tdcs yps bgt srud pb ewuejjebt ycsd pktez pj!"...'. The third tab is empty.

```
[09/08/22]seed@VM:~/.../lab2$ python3 encryt.py
python3: can't open file 'encryt.py': [Errno 2] No such file or directory
[09/08/22]seed@VM:~/.../lab2$ python3 encrypt.py
Hrbqzv, Mcnps qzgpben, "I'jj stpzhe! Pezdpxs tdcs yps bgt srud pb ewuejjebt ycsd
pktez pj!"...
[09/08/22]seed@VM:~/.../lab2$
```

Decrypted plaintext:

A terminal window titled 'seed@VM: ~/.../lab2' with two tabs. The first tab shows the command 'python3 decrypt.py', the prompt 'Enter the key:pounekqdcmljabgxizstrhywvf', and the output: 'Hungry, Midas groaned, "I'll starve! Perhaps this was not such an excellent wish after all!"...'. The second tab is empty.

```
[09/08/22]seed@VM:~/.../lab2$ python3 decrypt.py
Enter the key:pounekqdcmljabgxizstrhywvf
Hungry, Midas groaned, "I'll starve! Perhaps this was not such an excellent wish
after all!"...
[09/08/22]seed@VM:~/.../lab2$
```

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).