**Applied Cryptography**

**UE20CS214**

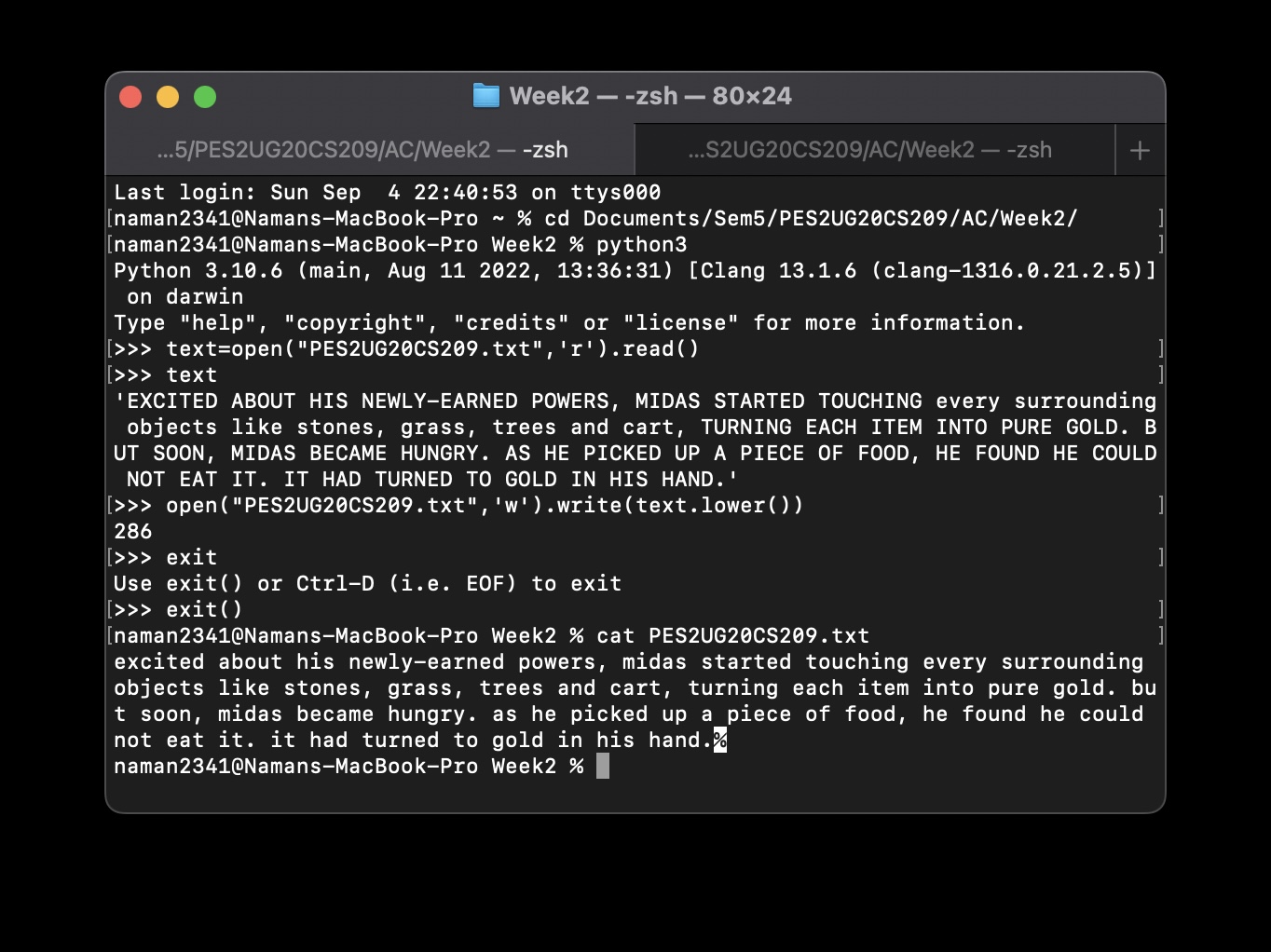
|  |  |
| --- | --- |
| Name | Naman Choudhary |
| SRN | PES2UG20CS209 |
| Section | D |

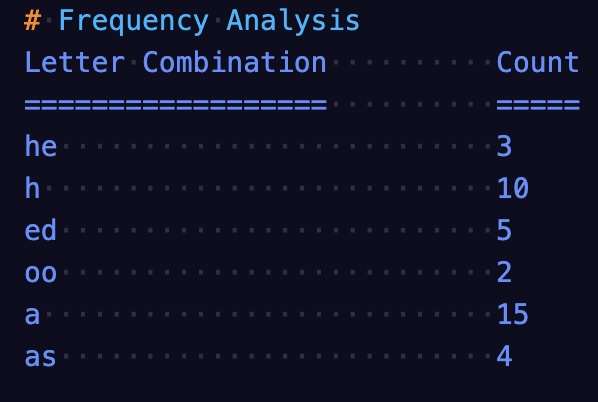
1. **Create and display a file SRN.txt with following contents:**

***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.***

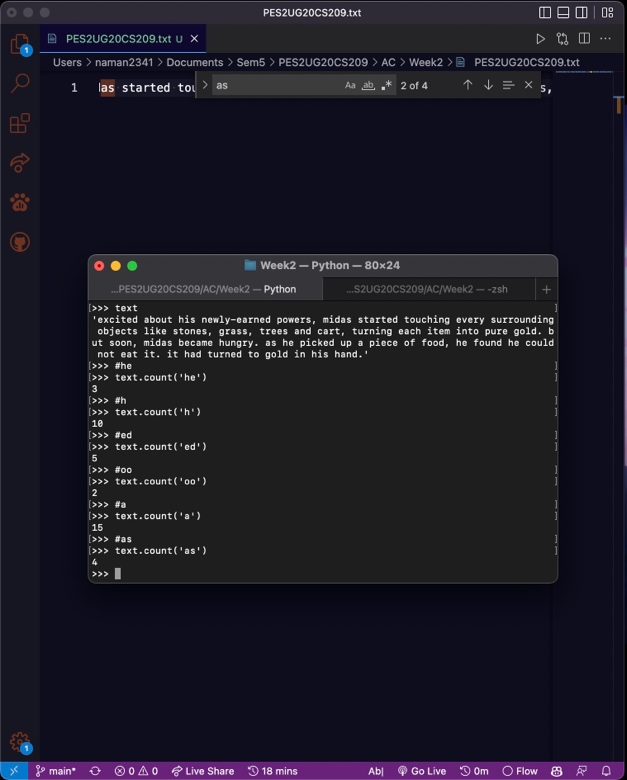
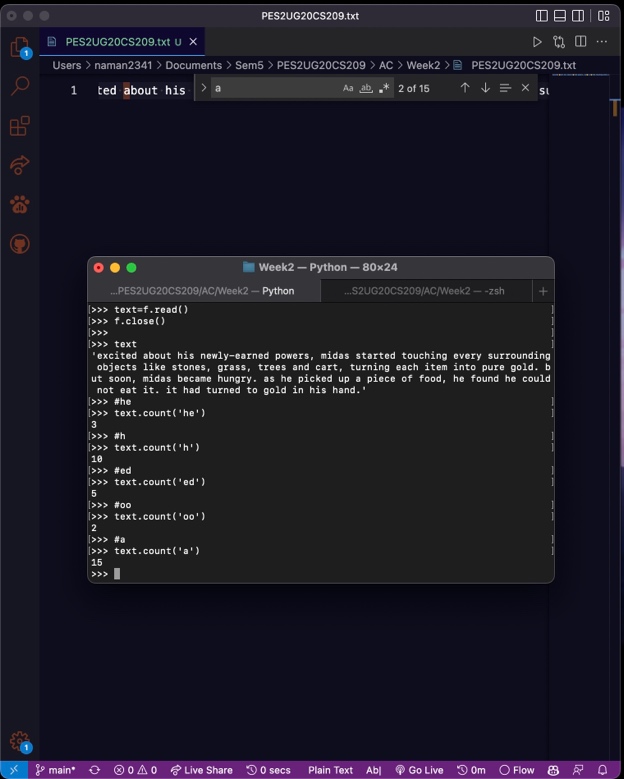
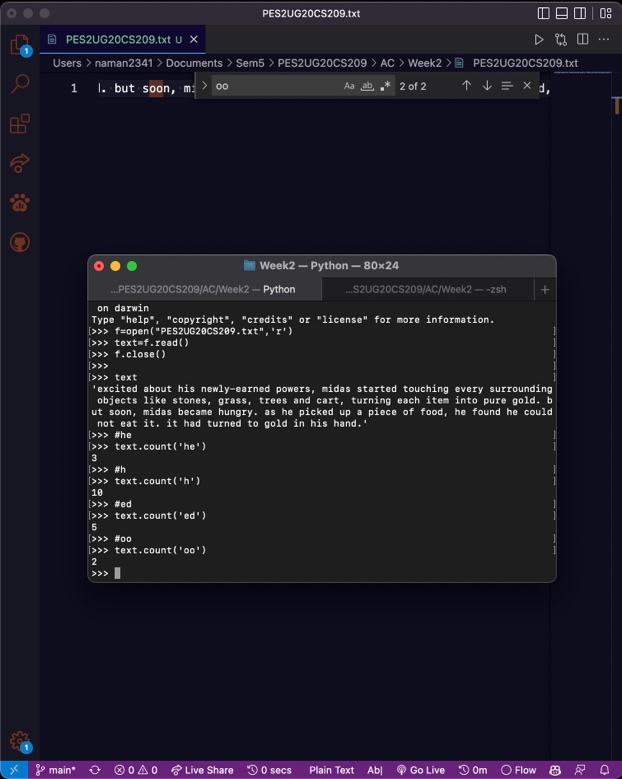
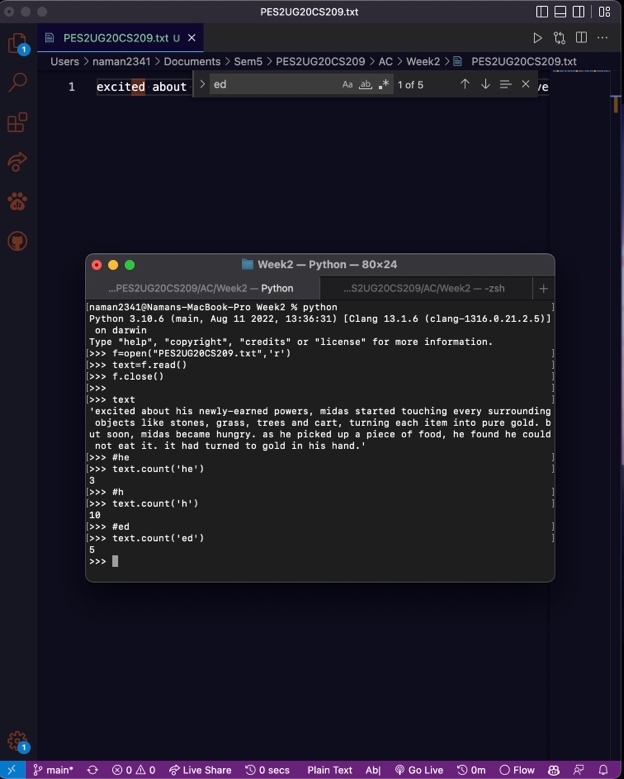
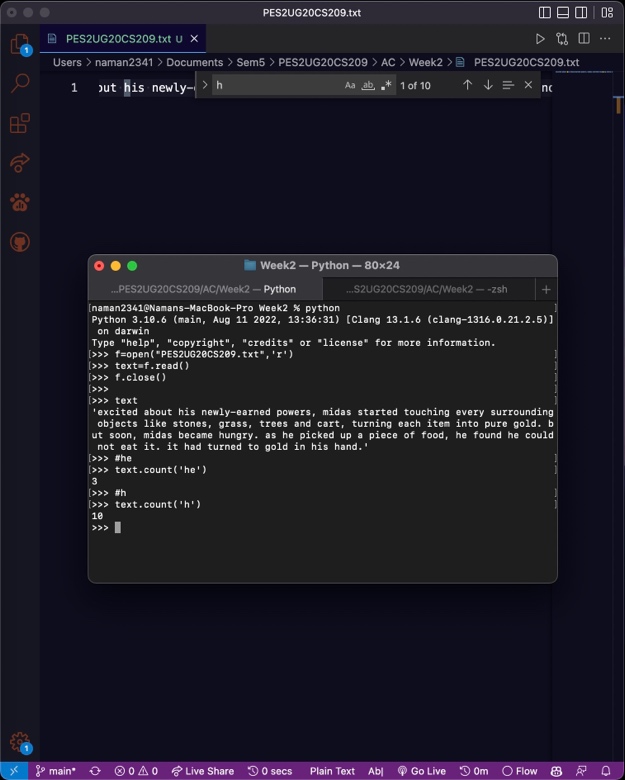
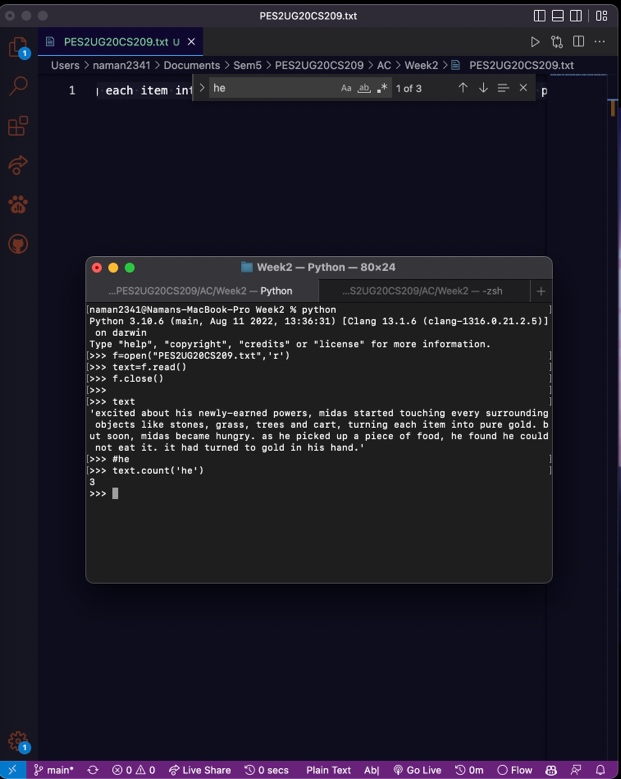


1. **In file SRN.txt, convert uppercase letters to lowercase and find the frequencies of following words:**
   1. **He**
   2. **H**
   3. **Ed**
   4. **Oo**
   5. **A**
   6. **As**

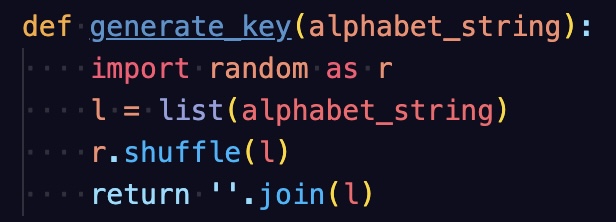
****



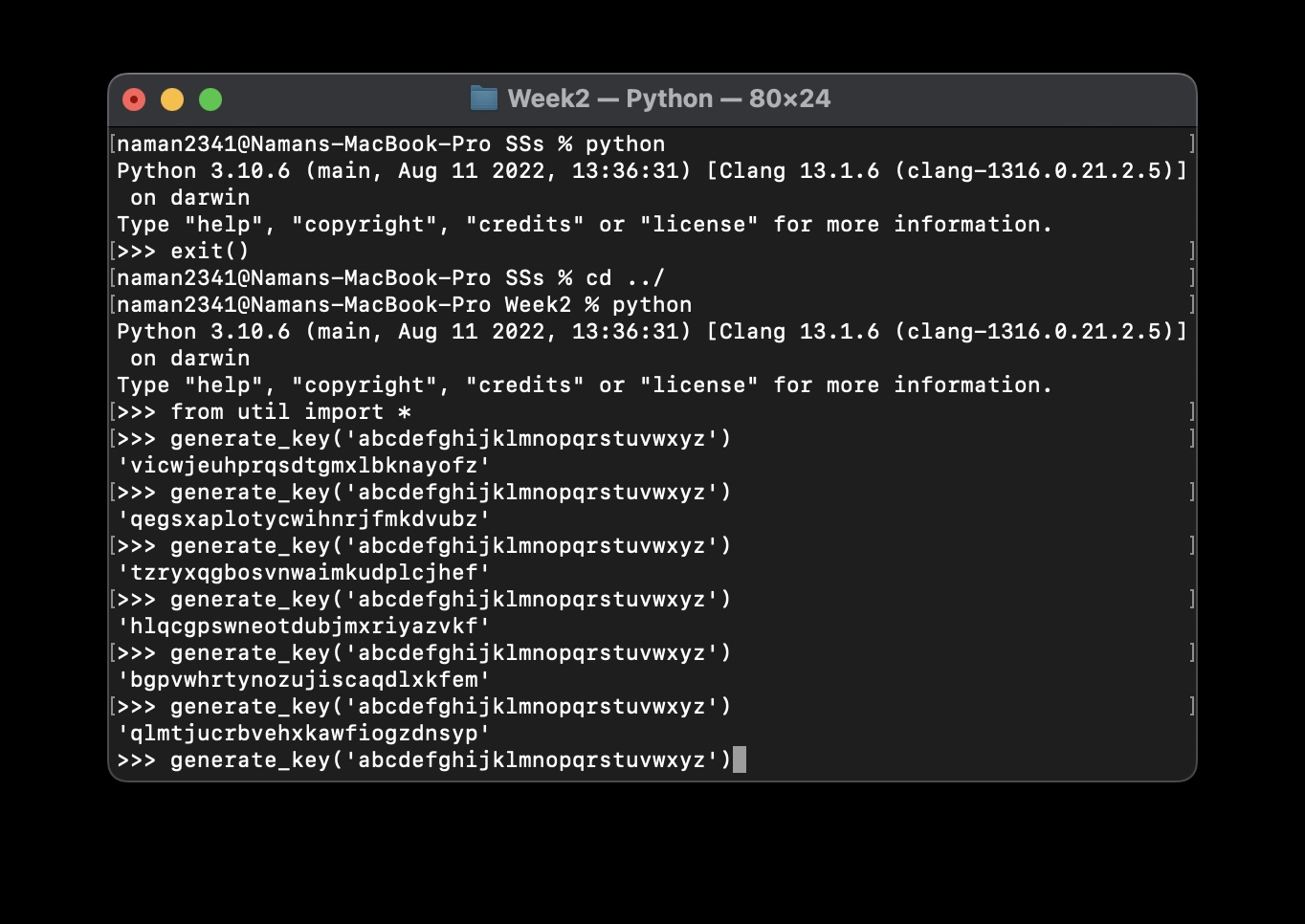
**3. Highlighting the words**

****

**4. Generate the substitution cipher key.**

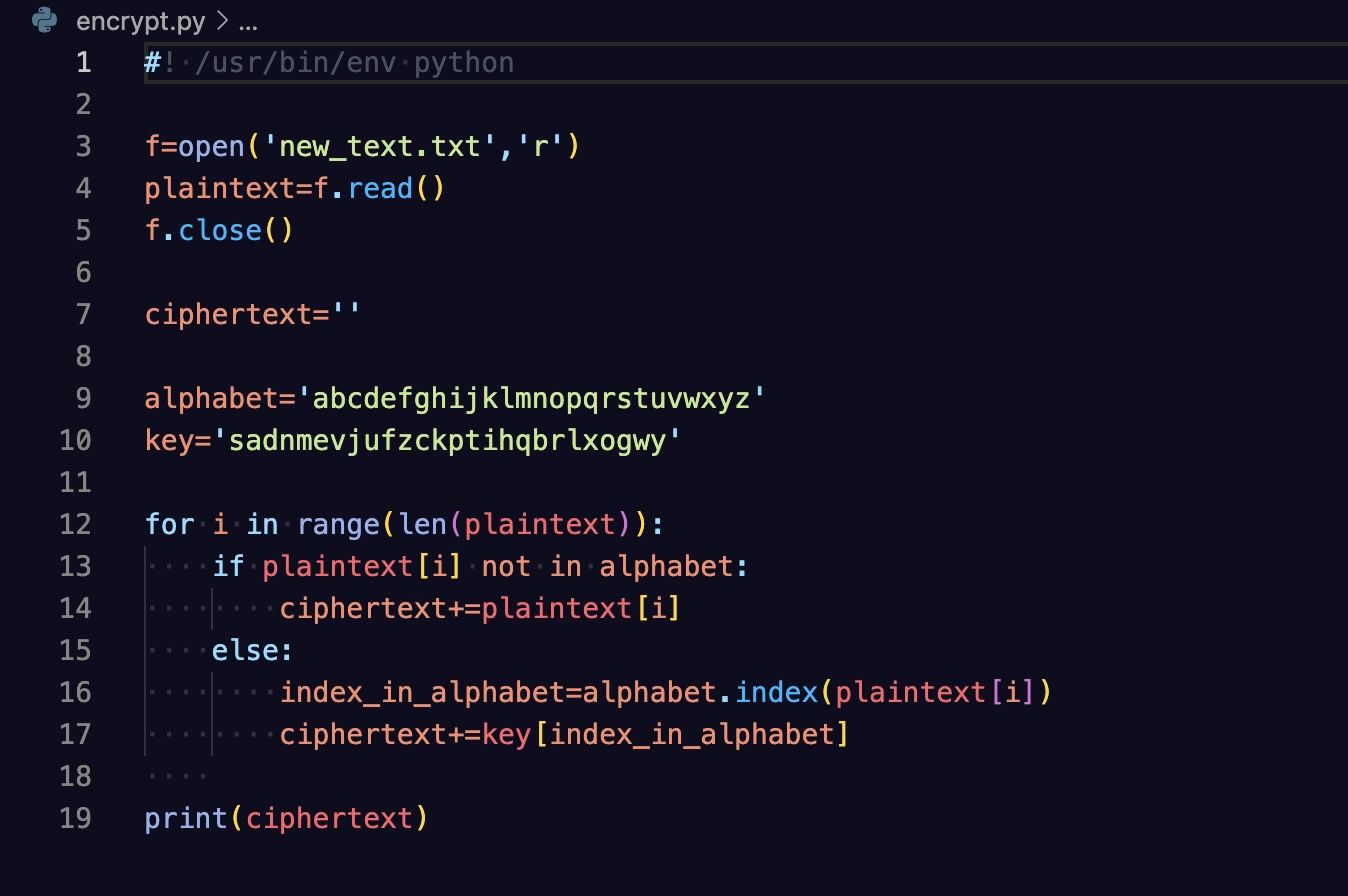
****

**Key Generation:**

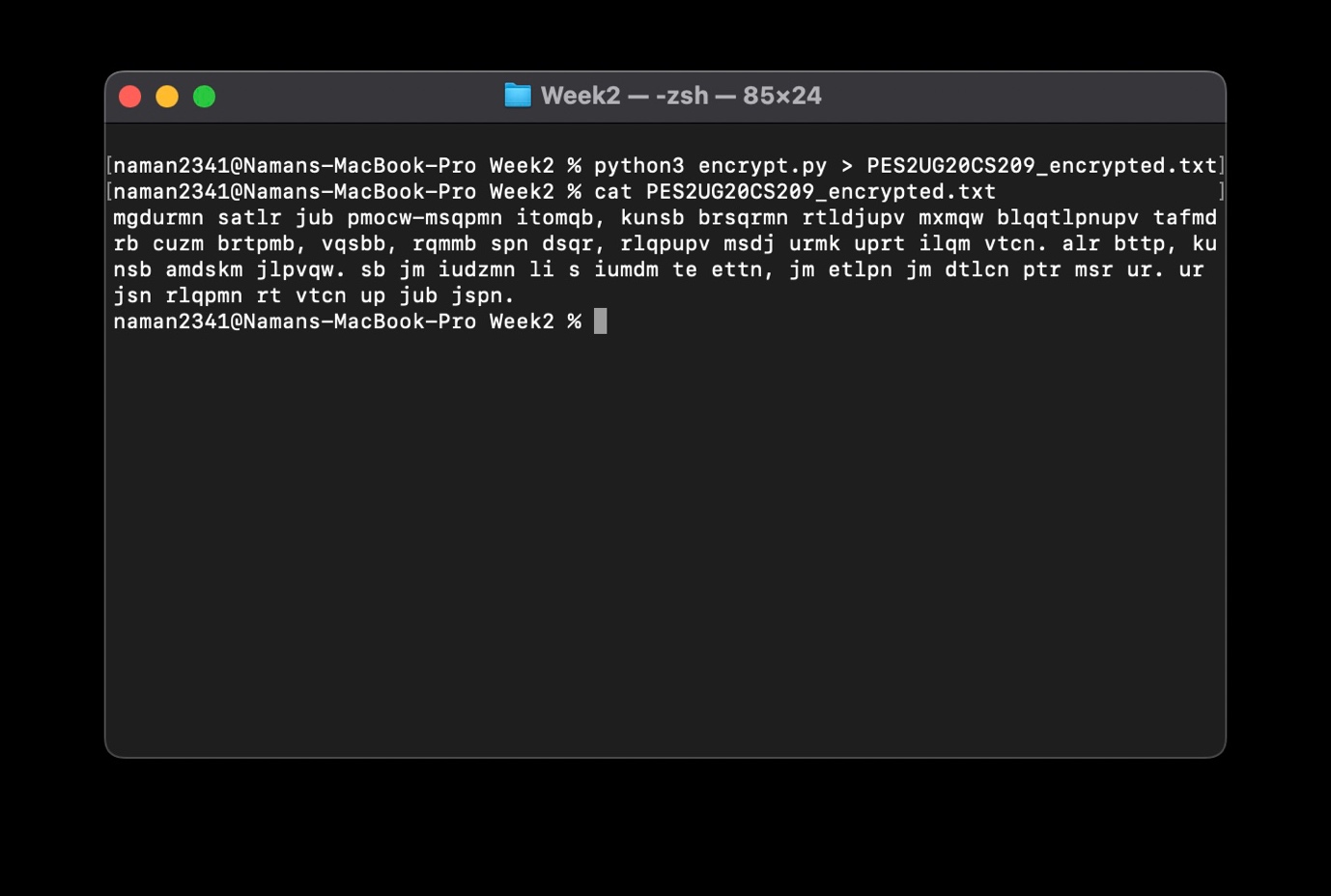
****

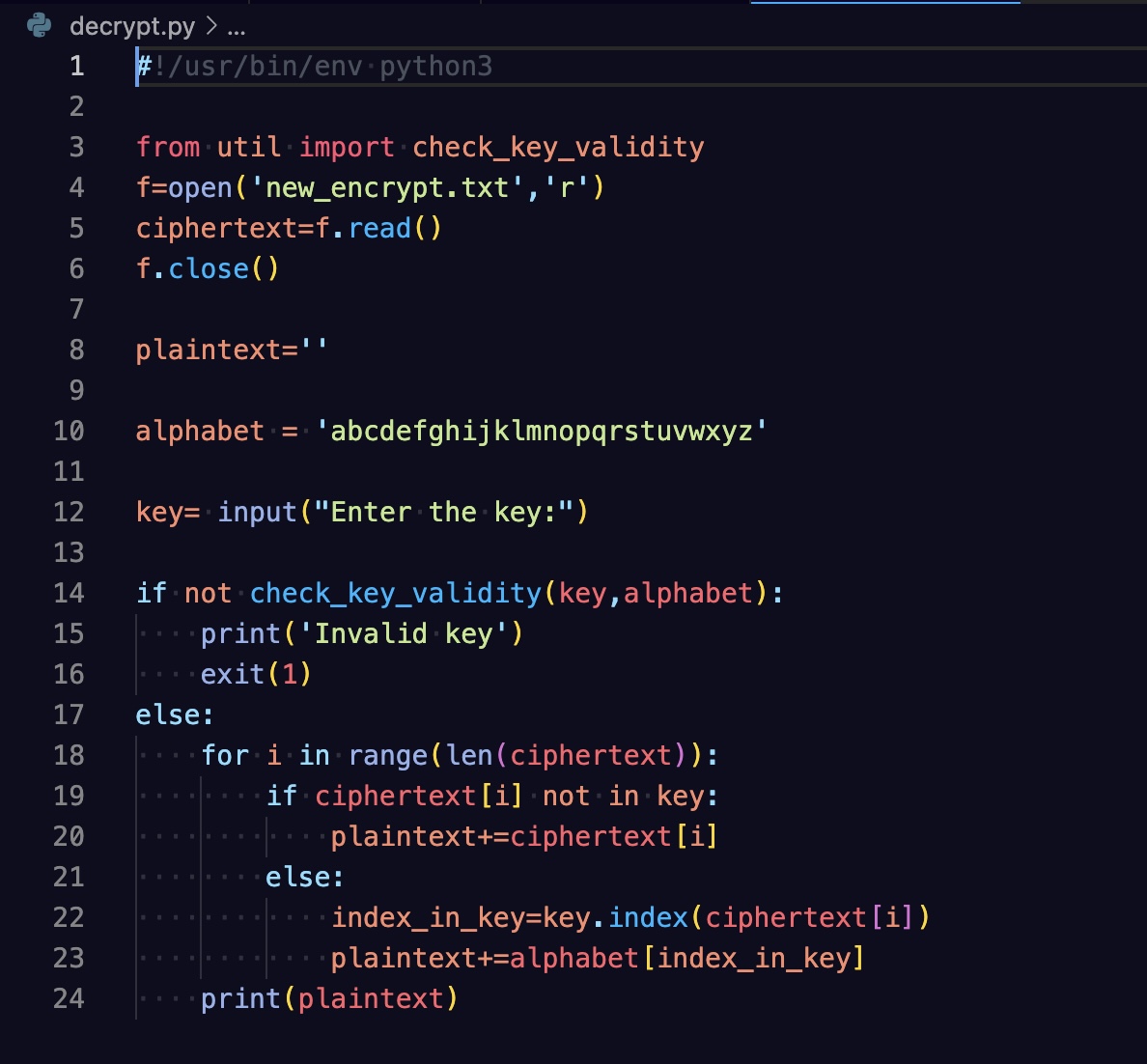
**Key: sadnmevjufzckptihqbrlxogwy**

**5. Generate the cipher text using the key generated in question 3.**

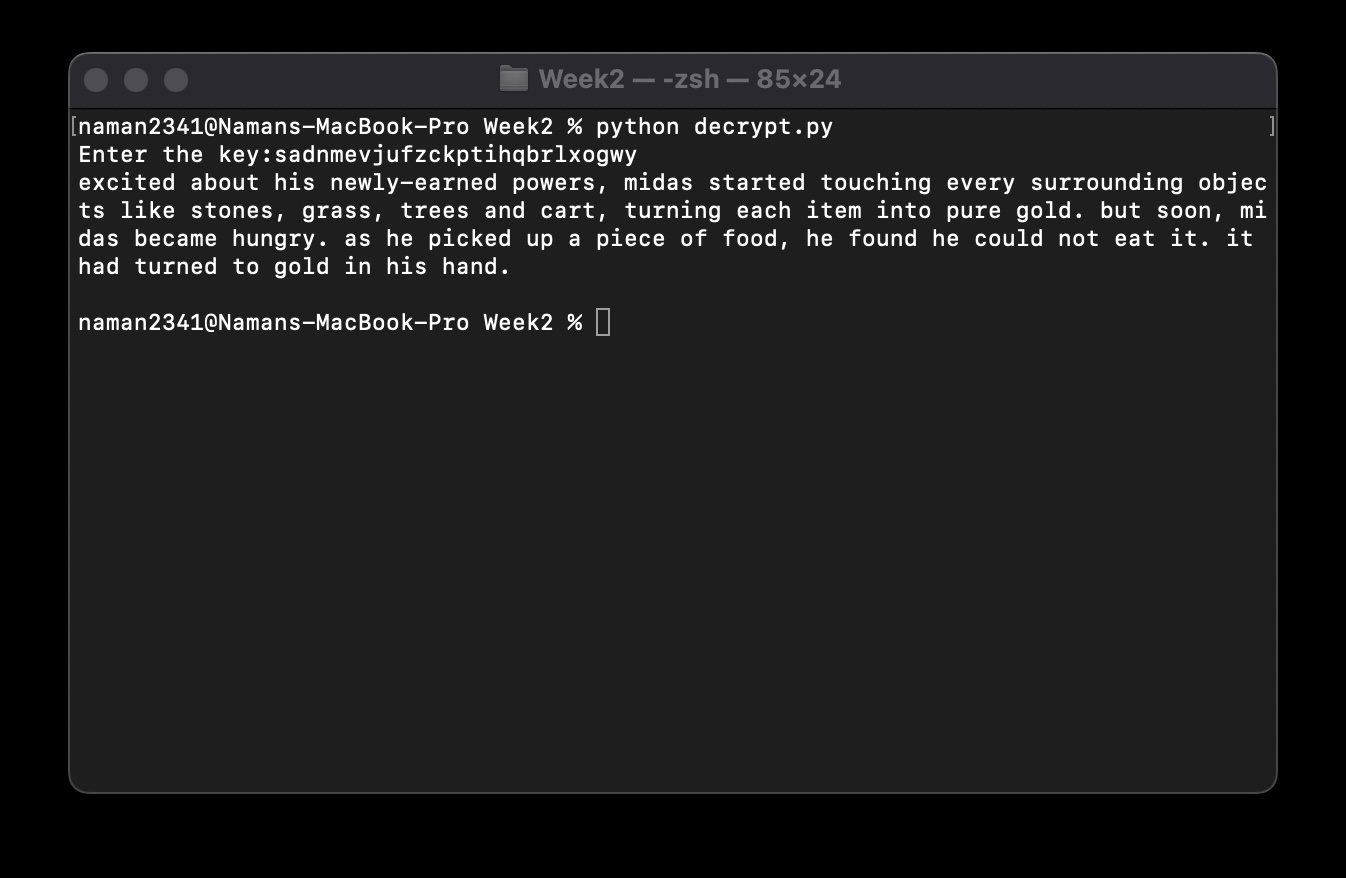
****

**Ciphertext:**

****

**6. Decrypt the cipher text back to plain text. **

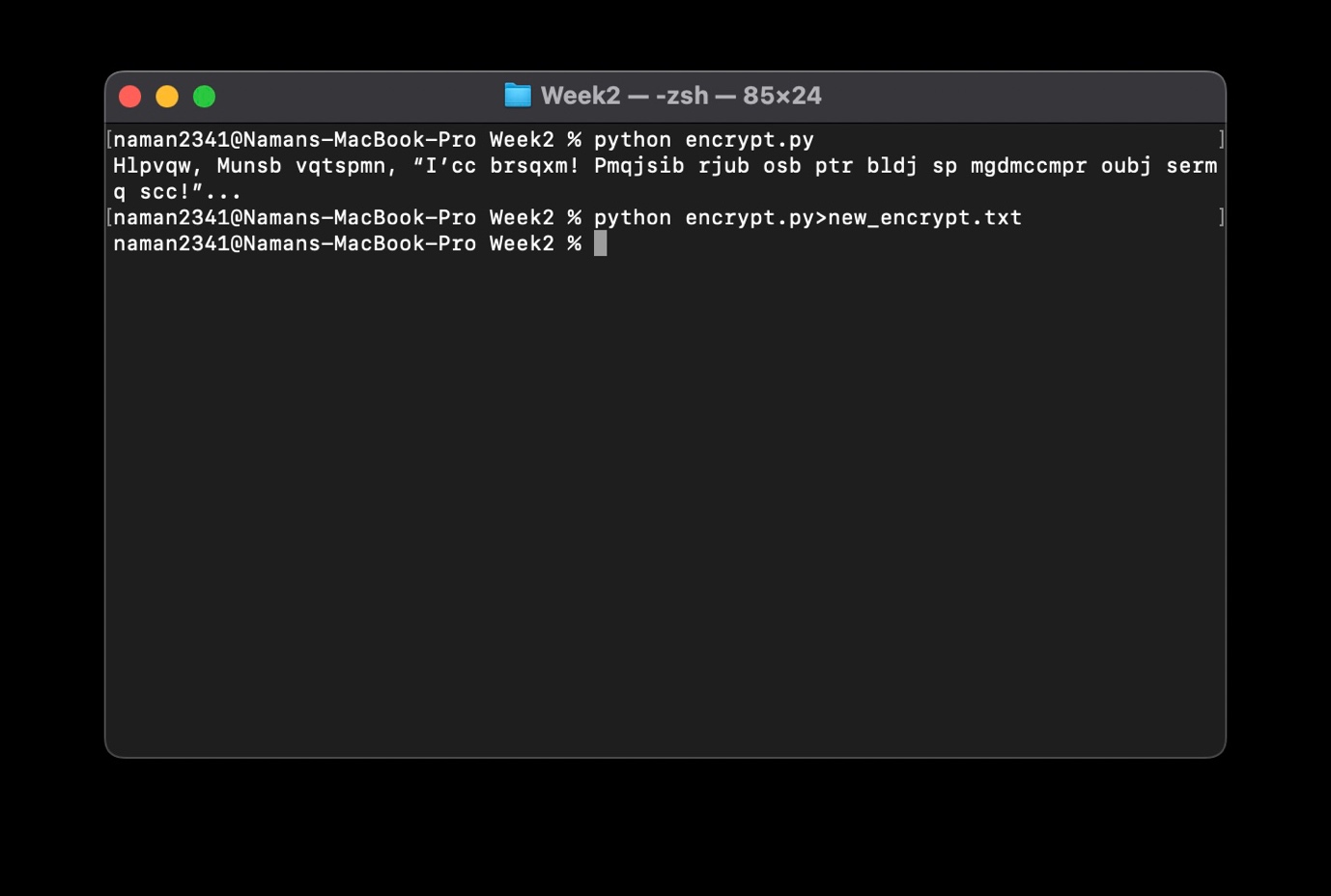
**Decrypted ciphertext to plaintext:**

****

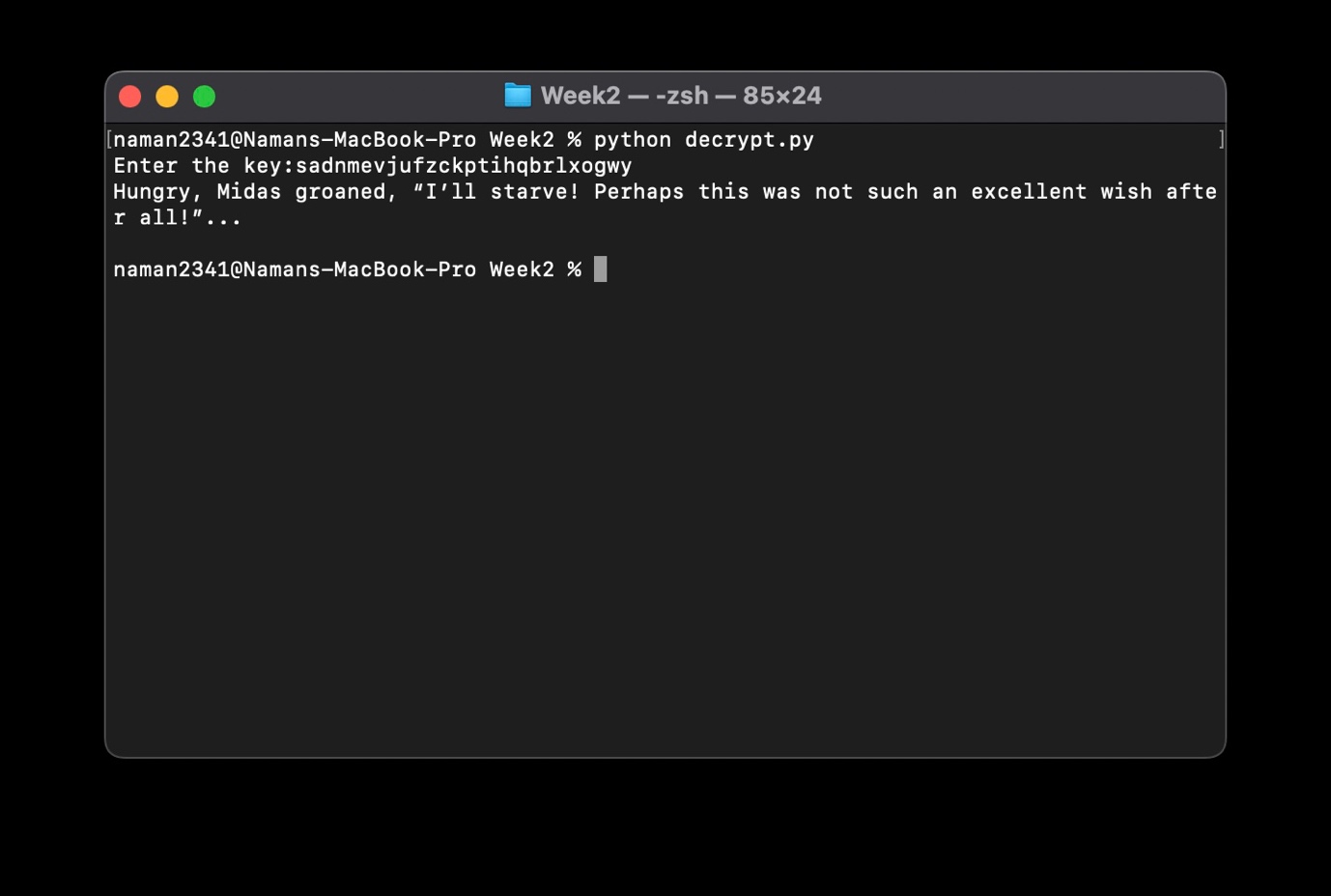
**7. Suppose the input file is :**

***Hungry, Midas groaned, “I’ll starve! Perhaps this was not such an excellent wish after all!”...***

**Ciphertext:**

****

**Decrypted ciphertext to plaintext:**

****

**Comments:**

We note that the newly generated cipher text is shorter than the previously generated ciphertext, and it appears to be the same length as the input plaintext, but this type of encryption is not safe, as modern computers can easily crack this with frequency distribution of letters, or simply by bruteforce attack(long but not impossible).