Assignment 2 report:

CPTS 427

Hongqi Guo

Question #1—Decode this simple cipher, which is the title of a book:

ACVLQDMZ

Answer is : **sundiver**

This problem I used the Caesar Cipher to solve, I do this by changing the Shift value.

```
PS C:\Users\hongq\Desktop\527\427 a2>  & 'C:\Program Files\Python3/\python
es\lib\python\debugpy\launcher' '53863' '--' 'c:\Users\hongq\Desktop\527\4
Please enter the Ciphertext: ACVLQDMZ
Please enter the Shift: 8
Answer is sundiver
```

Question #2

Answer in **question2new.txt book name is**   <alice's adventures in wonderland>

This problem has consumed me for a long time. I originally decided to use **Caesar Cipher** to solve this problem, but the results were not satisfactory. I learned from the book that I can use **substitution cipher**.
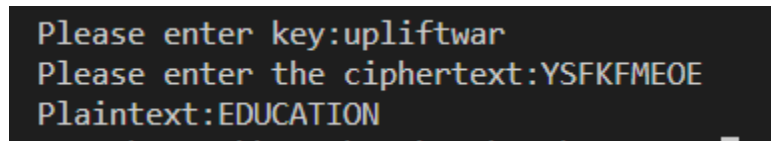
I first get the frequency of all the letters.

```
Letter Times Frequency
       33047   0.22887477577931836
I      13577   0.09403070871049733
P      10692   0.07404996225474239
S      8792    0.06089106510883793
J      8147    0.05642396581457036
A      7516    0.05205382681506209
R      7375    0.051077298132129176
H      7017    0.048597884880427177
O      6501    0.04502420544501312
M      5439    0.037669074513986524
D      4932    0.034157726696632015
F      4717    0.032668693598542825

       3600    0.02493264722381899
Q      3469    0.024025375894285574
W      2677    0.018540193505045398
E      2531    0.01752903614541274
N      2399    0.016614839080539377
Y      2265    0.015686790544986114
G      2107    0.014592524361274058
V      2002    0.013865322150579338
K      1525    0.010561746393423322
U      1475    0.010215459626425836
C      1159    0.008026927259001724
T      846     0.005859172097597462
L      209     0.0014474786860494914
X      149     0.001031934565652508
B      146     0.0010111157359632659
Z      78      0.0005402073565160781
```

Then I matched them against the English character frequency table in the book. The results were bad. I realized that it would take a lot of testing to get all the correct comparison tables, so I used a decompiler. I get all the keys from the decompiler and use Python to decipher the encrypted file.

Question #3—Decode this cipher (which has a connection to the plaintext in question #2) using the keyword from question2.txt (which has a connection to the keyword in question #1 and #2): YSFKFMEOE

Answer is : **EDUCATION**

```
Please enter key:upliftwar
Please enter the ciphertext:YSFKFMEOE
Plaintext:EDUCATION
```

This part did not take me too long. I used the **Vigenere cipher**, and the key value appears in the last line of the second question. I need to plug in the key value and ciphertext, and the final answer is' **EDUCATION** '.

Question #4—What is in the question4.txt file? Use the keyword from question #3 to unzip question4.zip.

Answer: **The keyword is THUNDERCASTLE.**