Working for Julius's secret service

RWH

due September IX MMXIX (2019)

This tests your programming.

You find an odd DeLorean parked around the corner. Realizing that Doc Brown has left the keys in the ignition, you decide that a quick trip back to Rome in 40 BC is in order. A few mint condition coins, and possibly a picture of Vincengetorix will be highly remunerative.

As usual, the car fails and you are stranded.

All is not lost, Julius Caesar recruits you for his secret service as a cryptographer. Falerian wine is palatable and there are more than enough other attractions to make your life comfortable.

Fortunately, you have your laptop, with a python interpreter, and by the use of lemon juice, copper denari and zinc you are able to rig up a battery to keep it running.

1. Write a python program (anything but Java) that takes a key (a number from 1 to 26) an input file name, and an output file name from the command line and uses the key to encrypt it with a Caesar cipher. A Caesar cipher performs modular addition of the key and the letter. If the key is 1 then a->b, b->c, ..., y->z, z->a . Ignore all the things that aren't the letters from a to z (simply pass them through) and you will want to put the letters into lower case. Use the file message1.txt and a key of 7 to encrypt it.

2. Cato and Junius Brutus are using the cipher to encrypt their communications. In Latin as well as that vulgar Germanic language Englisc the letter 'e' is the most common letter. 't' is the second most common. 'o' is the third most common. Write a python program to count the numbers of each letter in the message. (i.e. how common is each symbol) Then use that to find the key for the message. Use the file caesar1.txt for input.

   Note that the naive approach of assuming that 'e' and 't' are the first two may not work. But the correct key will have high values for both.

3. Caesar ciphers form a group. Therefore repeated encryption with any key will recover the message. Use the results from your answer to the second question to find the message. The proper decryption will be when 'e' is the most common letter and 't' is the second most common. Use the file caesar2.txt for input.