Programming using Python

Assignment-2: Caesar Cipher

Problem

You are working for Julius Caesar and he asks you to implement his favorite encryption scheme, the Caesar Cipher, in Python as a module named caesar.py. The scheme is fairly simple and all details you need about the cipher are available at its Wikipedia page (http://en.wikipedia.org/wiki/Caesar_cipher). Here is what you need to make within the module:

1. A function called 'cleanup' which will take a file name as input. The file contains a string in English. The function will remove all punctuation, spaces etc. so that all you are left with is nothing but English alphabet which you then convert to lower case. Henceforth, this contiguous string of characters from a-z only will be referred to as the 'cleaned-up string'. The function returns this cleaned up string along with the original text.
2. A function called 'encrypt' which takes a cleaned up string and a shift argument and returns the cipher text for that string using the Caesar Cipher. The function should print an error if the shift parameter is not within the range 1-26 and the program should stop.
3. A function called 'decrypt' which takes a string and a shift parameter and returns the decrypted string.
4. A function called 'breakCipher' which predicts the shift parameter used to encrypt an encrypted string. This it does by analyzing the frequency of usage of all words in an encrypted string passed to it as input and assigning the most used character in the encrypted string with 'e' which is the most used character in English. For more details, see the Wikipedia page.

I will use code similar to the snippet given below to test your modules. Please use this to figure out what the function interfaces (inputs and return arguments) are. Note that I will test with different input strings on which the simple algorithm for breaking the cipher works.

```
from caesar import cleanup, encrypt, decrypt, breakCipher
import random
actualText, cleanText=cleanup('input.txt')
print "Actual Text:", actualText
print "Clean Text:",cleanText
shift=random.randint(1,26)
encText=encrypt(cleanText,shift)
print "Encrypted Text:",encText
predShift=breakCipher(encText)
print "Predicted Shift is",predShift,"and actual shift is",shift
decText=decrypt(encText,predShift)
   print "Results of breaking the cipher:",decText
```

The expected output for the example 'input.txt' using the above test snippet is given below.

```
Actual Text:
In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift
cipher, Caesar's code or Caesar shift, is one of the simplest and most widely
known encryption techniques. It is a type of substitution cipher in which
each letter in the plaintext is replaced by a letter some fixed number of
positions down the alphabet. For example, with a left shift of three, D would
be replaced by A, E would become B, and so on. The method is named after
Julius Caesar, who used it in his private correspondence.

Clean Text:
incryptographyacaesarcipheralsoknownascaesarsciphertheshiftciphercaesarscodeo
rcaesarshiftisoneofthesimplestandmostwidelyknownencryptiontechniquesitisatype
ofsubstitutioncipherinwhicheachletterintheplaintextisreplacedbyalettersomefix
ednumberofpositionsdownthealphabetforexamplewithaleftshiftofthreedwouldberepl
acedbyaewouldbecomebandsoonthemethodisnamedafterjuliuscaesarwhouseditinhispri
vatecorrespondence

Encrypted Text:
zetipgkfxirgyprtrvjritzgyvircjfbefnerjtrvjrijtzgyvikyvjyzwktzgyvitrvjrijtfuvf
itrvjrijyzwkzjfevfwkyvjzdgcvjkreudfjknzuvcpbefnevetipgkzfekvtyezhlvjzkzjrkpgv
fwjlsjkzklkzfetzgyvizenyztyvrtycvkkvizekyvgcrzekvokzjivgcrtvusprcvkkvijfdvwzo
vueldsvifwgfjzkzfejufnekyvrcgyrsvkwfivordgcvnzkyrcvwkjyzwkfwkyivvunflcusvivgc
rtvusprvnflcusvtfdvsreujffekyvdvkyfuzjerdvurwkvialczljtrvjrinyfljvuzkzeyzjgiz
mrkvtfiivjgfeuvetvi

Predicted Shift is 17 and actual shift is 17

Results of breaking the cipher:
incryptographyacaesarcipheralsoknownascaesarsciphertheshiftciphercaesarscodeo
rcaesarshiftisoneofthesimplestandmostwidelyknownencryptiontechniquesitisatype
ofsubstitutioncipherinwhicheachletterintheplaintextisreplacedbyalettersomefix
ednumberofpositionsdownthealphabetforexamplewithaleftshiftofthreedwouldberepl
acedbyaewouldbecomebandsoonthemethodisnamedafterjuliuscaesarwhouseditinhispri
vatecorrespondencer
```

Hints

String functions

See the following links:

https://docs.python.org/2/library/string.html

http://www.pythonforbeginners.com/basics/string-manipulation-in-python

Filing

See: https://docs.python.org/2/tutorial/inputoutput.html