

**COMPUTER EXPERIMENTATION #2 – MATH 5405
SPRING 2016**

DUE: TUESDAY FEBRUARY 2ND

Let's functions for encrypting and decrypting with the Vigenère cipher. You may turn in individual assignments or you can work in a group of 2 people.

Step 1 Open up a terminal.

Step 2 Make a new file that will hold the functions procedures you will write. The file should end with “.py”. For instance you could do

```
gedit Vigenere.py &
```

which will open an editor and edit a file.

Step 3 Run python.

Step 4 Next let's learn how to manipulate strings in python. One thing that will be critical is turning a string (a bit of text) into the corresponding numerical codes. Try the following commands and think about what they are doing.

```
>>> import string
>>> s = 'Hello World'
>>> len(s)
>>> s = s.lower()
>>> s
>>> s = s.upper()
>>> s
>>> s = s.replace(' ', '')
>>> s
>>> range(0,3)
>>> for i in range(0,3):
...     print i
...
>>> [c for c in s]
>>> numList = [ord(c) for c in s]
>>> numList
>>> charList = [chr(i) for i in numList]
>>> charList
>>> newS = ''.join(charList)
>>> newS
>>> numList = [j-ord('A') for j in numList]
>>> numList = [(j+3)%26 + ord('A') for j in numList]
>>> newS2 = ''.join([chr(i) for i in numList])
>>> newS2
```

Step 5 At this point, I think you actually have the necessary tools in order to implement a Vigenère cipher. But let me get you started. I'd make a function in your Vigenere.py file. Here's the start of my function. Note my function only works for strings made up of letters.

```
def Encrypt(code, plaintext):
    import string
    code = code.upper()
    codeList = [ord(c)-ord('A') for c in code]
    codeLen = len(code)
    plaintext = plaintext.upper()
    plainlist = [ord(c) - ord('A') for c in plaintext]
```

After that, I made a for loop that shifted letters appropriately and then returned the ciphertext string.

Step 6 Now make a function that decrypts. Finally, check that your decryption undoes your encryption at least

Step 7 Improve your code, perhaps strip non-letters from your code word or ciphertext.

Step 8 Write a function that does autocorrelation. In other words, suppose *s* is a string. Write a function that counts how many letters of *s* and (*s* shifted right by *n*) line up. For instance 'CATS' shifted by 1 should become 'SCAT' and shifted by 2 should become 'TSCA'. Now create a loop that computes this number for various *n* (in a loop). See section 2.3.1 in Trappe and Washington for additional discussion of this method.

Step 9 Write a function that tries to do automated Vigenère decryption. Look up letter frequency tables on the internet. Include a writeup explaining what you did (you can probably do better than just looking for the most frequent letter which might or might not be 'e'). This is hard, so I don't expect you to do it perfectly. Just try your best.

Step 10 After this is turned in, we will have a competition to see which algorithm works best! (Just for fun)