CMPSC 443 Homework 1

Name: Adam Robertson PSU Username: abr5598

Format Requirement

- Do NOT change the template except the answer portion.
- Use Markdown to complete the answers.
- You can use your favorite Markdown editor.
- In your answers, if code is included, all code should be placed in code blocks/fences. For example:

```
def somefunc(param1='', param2=0):
    '''A docstring'''
    if param1 > param2: # interesting
        print 'Greater'
    return (param2 - param1 + 1) or None
```

- Export your work to a **pdf** file for submission

Problem Set

Problem 1

Please use your own words to describe **Vigenère cipher**, and how to break it.

Answer

A Vigenère cipher is when a key is used to shift the characters of a plaintext differently character by character.

If the key is shorter than the plaintext, the key is the applied repeatedly to the the rest of the plaintext.

Problem 2

The following word is encrypted using **Caesar cipher**. Please figure out the offset used in this encryption and what the original word is.

`xqluvkd`

Answer

The offset of the Ceasar cipher is 10. The orignial word is `havefun`.

```
# Shift a lowercase letter by the specified 'shift'
def shiftLetter(character, shift):
```

```
    character = chr(ord(character) + shift) # Add shift
    if ord(character) > ord('z'): # If exceeded the alphabet
        # Add the remainder to the start of the alphabet
        character = chr(ord('a') + (ord(character) % (ord('z') + 1)))
    return character

if __name__ =='__main__':

    message = 'xqluvkd'

    for shifting in range(0, 23): # Test every shift 0-22
        newMess = ''
        for character in range(0, len(message)): # Shift every character
            newMess += shiftLetter(message[character], shifting)
        print("Shift: " + str(shifting) + " -> " + str(newMess))
```
