COE817 - Lab 1

Objectives

- In this lab, you will work on Caesar Cipher and an implementation of the Vigenère Cipher, the system for encoding and decoding text messages that was discussed in class. You will program with Java or Python. Netbeans is the IDE for Java and Anaconda is the IDE for Python.

Exercise 1

(a) Choose a secret sentence (Plaintext) of about 20 words and encrypt using Caesar Cipher with your own secret key. Fill the table 1 by using your plain text, secret key and corresponding ciphertext.

Plaintext	Yesterday was excellent! Let's meet again Tuesday at noon
Your secret Key	A shift of +3, i.e. A -> D
Ciphertext	Bhvwhugdb zdv hafhoohqw! Ohw'v phhw djdlq Wxhvgdb dw qrrq

Table 1: Encryption

(b) Break the given Ciphertext encrypted by Caesar Cipher

Ciphertext	Glzkx g cnork, Rozzrk Jaiqrotm cgy zoxkj ul vrgeotm. Ynk yixgshrkj av utzu znk mxgyye hgtq gtj lrallkj uaz nkx lkgznkxy zu jxe. Gxuatj nkx znk cotj cnoyvkxkj ot znk mxgyy. Znk rkgbky xayzrkj gtj ubkxnkgj znk yqe mxkc jgxq. Rozzrk Jaiqrotm xkgrofkj ynk cgy grr grutk.
Plaintext	
Explain how you break the Ciphertext, provide details. Plaintext: After a while, Little Duckling was tired of playing. She scrambled up onto the grassy bank and fluffed out her feathers to dry. Around her the wind whispered in the grass. The leaves rustled and overhead the sky grew dark. Little Duckling realized she was all alone. To break the ciphertext, I used the brute force method. I wrote a Python script that would use all 26 keys from range 0 to 25 and print them all in an output file. I then simply parsed through the file to find the sentence that was in plain English.	

Table 2: Decryption

Exercise 2:

Part A: Use Java or Python to solve this exercise. In Java name your class as “Vigenere**”**. In Python name your program as “Vigenere”. Here are the requirements for the methods/functions. You may include other methods if needed

- Create a method/function in the class Vigenere that will **encrypt** a message using a specified key.
- Create a method/function in the class Vigenere that will **decrypt** a message using a specified key.

Part B: Write a main method/function in class Vigenere to do the following:

1. Ask the user to enter the message "TO BE OR NOT TO BE THAT IS THE QUESTION".
2. Ask the user for the Vigenère key "RELATIONS".
3. Encode the message using the Vigenère cipher.
4. Print the encrypted text.
5. Decode the message using the Vigenère cipher.
6. Print the result of decrying the encrypted text (which should be the original text).

Submitting your lab

You must submit your assignment in the D2L and demonstrate in the lab session before the deadline. For Exercise 1 you need to submit lab report and for Exercise 2 you need to submit source code. Code should be well documented. Zip the lab1 folder (remember to do this recursively so that all sub-folders are included), then submit in the D2L.