CSCE4013/5013 Homework 1 (Programming)

Due date: August 31, 2018

Full Grade: 100 pts

In this assignment, you need to implement the Enhanced Caesar Cipher (see Module 2 slides).

Part 1: Implement both encryption and decryption. For encryption, given a plaintext and the key *n*, your program should be able generate its ciphertext. For decryption, given a ciphertext and the key *n*, your program should be able to decrypt it and get the plaintext.

Part 2: Implement a brute-force attack that can decipher any ciphertext encrypted using the Enhanced Caesar Cipher where the plaintext is from a certain vocabulary specified in a text file. Specifically, given a particular ciphertext and the vocabulary text file, your program should be able to find the key *n* and the plaintext. For your convenience, a sample vocabulary text file *sample.txt* is attached. Note that your algorithm should work for other vocabulary file as well.

Other instructions

- Any programming language is fine.
- Submit your code as a .zip file named in this format: HW1.YourLastName.YourFirstName.zip.