CS2107 Self-Exploration Activity 2

Notes:

For Activity 2, you can perform the following:

1. To try out some Python scripts and online tools that allow you to implement the **Shift/Caesar cipher**, **Vigenere cipher**, and **One-Time Pad**;
2. To try out some Python scripts that allow you to **attack** the Shift/Caesar cipher and Vigenere cipher.

Task 1: Implementing and Attacking Shift/Caesar Cipher

The book by Al Sweigart, "*Cracking Codes with Python: An Introduction to Building and Breaking Ciphers*", No Starch Press, 2018 (available freely online) also provides Python scripts to implement and attack **the Shift/Caesar cipher**:

- Chapter 5 (The Caesar Cipher): https://inventwithpython.com/cracking/chapter5.html;
- Chapter 6 (Hacking the Caesar Cipher with Brute Force): https://inventwithpython.com/cracking/chapter6.html.

Additionally, there are many online tools that allow you to perform the encryption and decryption operations of the Shift/Caesar cipher, such as:

- https://cryptii.com/pipes/caesar-cipher.

Task 2: Implementing and Attacking Vigenere Cipher

The book "*Cracking Codes with Python: An Introduction to Building and Breaking Ciphers*", No Starch Press, 2018 also provides Python scripts to implement and attack **the Vigenere cipher**:

- Chapter 18 (Programming the Vigenere Cipher): https://inventwithpython.com/cracking/chapter18.html;
- Chapter 20 (Hacking the Vigenere Cipher): https://inventwithpython.com/cracking/chapter20.html.

Likewise, there are many online tools that allow you to perform the encryption and decryption operations of the Vigenere cipher, such as:

- https://cryptii.com/pipes/vigenere-cipher.

Task 3: Implementing One-Time Pad

The book "*Cracking Codes with Python: An Introduction to Building and Breaking Ciphers*", No Starch Press, 2018 provides a script to implement **the One-Time Pad** as well:

- Chapter 21 (The One Time Pad Cipher): https://inventwithpython.com/cracking/chapter21.html.

The book author implements the One-Time Pad as a (trivial) extension of the Vigenere cipher, whereby now the key is as long as the plaintext to encrypt.

Note that the script to *attack* the One-Time Pad is, however, *not* found in the book. You may want to check the uploaded Lecture 1 (part 2) slide deck to see why the book chooses to omit including an attack on the One-Time Pad.

Yet, if you want, you can try to attack the cipher. *And good luck with it!* 😊