CIIC5018 / ICOM5018
Network Security and Cryptography

Project 2: Playfair Cipher and Vigenere Cipher

Overview

In this exercise, you will need to design and implement Playfair cipher and Vigenere cipher, and then compare the relative frequency of letters in the plaintext and cyphertext. The programming language is Python.

Document requirements

To work on the exercise, you will need to prepare **three** documents following the guidelines below.

1. A design document
    a. Cover page
        i. It shall include the title of the document, your name, student ID, department and university information, etc.
    b. Table of content
    c. Section 1: The Playfair cipher (encryption and decryption)
        i. The input of encryption is a plaintext and a key
            1. The plaintext must be the output of the procedure described in section 1 of Project 1
        ii. The return of encryption is a ciphertext
        iii. The input of decryption is a cyphertext and a key
        iv. The return of decryption is a plaintext
        v. Explain your design to deal with the situation that two input letters are the same
        vi. Explain your design to deal with the situation that the last plaintext is a single letter
    d. Section 2: The Vigenere cipher (encryption and decryption)
        i. The input of encryption is a plaintext and a key
            1. The plaintext must be the output of the procedure described in section 1 of Project 1
        ii. The return of encryption is a ciphertext
        iii. The input of decryption is a cyphertext and a key
        iv. The return of decryption is a plaintext
    e. Section 3: The relative frequencies of letters in a string
        i. The input is a string that contains only capitalized English letters
        ii. The output is a sorted (decreasing order) array of relative frequencies of letters
    f. References

i. Cite **at least 5 references**
ii. **The link to your YouTube video must be included here**

2. A Python program saved in a Jupyter notebook
    a. The following functions shall be implemented based on the pseudo codes in the design document:
        i. The Playfair encryption function.
        ii. The Playfair decryption function.
        iii. The Vigenere encryption function.
        iv. The Vigenere decryption function.
        v. The relative frequency function.
        vi. Some test functions.
    b. To verify your encryption and decryption functions, you must show that the plaintext can be accurately recovered after you used the same key to encrypt and decrypt
    c. To test the Playfair cipher, you shall use key “MAXFRESH”.
    d. To test the Vigenere cipher, you shall use repeated key “MAXFRESH”.
    e. To show the result of the relative frequency function. You must
        i. use all the text in this Word document as the input of the text processing procedure and generate the plaintext, then
        ii. encrypt the plaintext using the Playfair cipher to generate ciphertext 1, then
        iii. encrypt the plaintext using the Vigenere cipher to generate ciphertext 2, then
        iv. generate the relative frequencies for plaintext, ciphertext 1 and ciphertext 2, and finally
        v. plot a figure to compare relative frequencies (**similar to Figure 2.6 in the textbook**).
3. A YouTube video to walk through your code
    a. In the video, you shall go through Step 2.c to verify your encryption and decryption functions of the Playfair cipher.
    b. In the video, you shall go through Step 2.d to verify your encryption and decryption functions of the Vigenere cipher.
    c. In the video, you shall go through Step 2.e and show the figure of relative frequencies.
    d. Upload the video to YouTube, set the video as private, then share it to me (Kejie.lu@upr.edu)

Submission

Submit a single zip file that includes:

1. the design document
2. the Jupyter notebook

Evaluation

1. Rubrics are used in the evaluation.
2. You must carefully review all rubrics before preparing for the documents.