**Lee\_Report\_PA2**

**Cryptography Section W01 Summer Semester 2024 CO**

**Raehyeong Lee**

**2024-06-23**

**Overview**

This program implements the Playfair cipher, an encryption technique that uses a 5x5 matrix of letters constructed from a keyword. The main components of the program include the generation of the key matrix, the preparation of plaintext for encryption, and the encryption and decryption processes. The program also includes a test function to demonstrate the encryption and decryption using user inputs.

**Functions**

**1. generate\_key\_matrix(k)**

This function generates a 5x5 matrix used for encryption and decryption based on a given keyword.

**Details:**

* Converts the key to uppercase.
* Initializes an empty 5x5 matrix and a list to keep track of inserted alphabets.
* Populates the matrix with unique characters from the key.
* Fills in the remaining spaces with the rest of the alphabet, skipping 'J' (considered the same as 'I').

**2. x\_generater(str)**

This function works with the plaintext by inserting 'X' between identical consecutive letters and at the end if necessary.

Details:

* Iterates through the text, checking for identical consecutive letters.
* If found, inserts 'X' between them.
* Adds 'X' at the end if the text length is odd.

**3. find\_position(alphabet, mat)**

This function finds the position (row, column) of a letter in the 5x5 matrix.

Details:

* Iterates through the matrix rows.
* Returns the (row, column) tuple for the first occurrence of the letter.:

**4. Encrypt (Plaintext, mat)**

This function changes the plaintext using the Playfair cipher encryption rules.

Details:

* Converts plaintext to uppercase and removes spaces.
* Processes the plaintext with x\_generater.
* Splits the text in pairs and converts following encryption rule:
  + If the letters are in the same row, they are replaced by the letters to their immediate right.
  + If they are in the same column, they are replaced by the letters immediately below.
  + Otherwise, they are replaced by the letters in the same row but in the columns of the other letter.

**5. Decrypt (Ciphertext, key)**

This function changes Decrypts the ciphertext using the Playfair cipher rules.

Details:

* Generates the key matrix using generate\_key\_matrix.
* Converts ciphertext to uppercase and removes spaces.
* Processes the ciphertext with x\_generater.
* Splits the text in pairs and converts following decryption rule:
  + If the letters are in the same row, they are replaced by the letters to their immediate left.
  + If they are in the same column, they are replaced by the letters immediately above.
  + Otherwise, they are replaced by the letters in the same row but in the columns of the other letter.

**6. test\_playfiar()**

This function tests the Playfair cipher by prompting the user for inputs and displaying the results.

Details:

* Prompts the user for a keyword to generate the key matrix.
* Displays the key matrix.
* Prompts the user for plaintext and encrypts it.
* Prompts the user for ciphertext and decrypts it.

**Conclusion**

The program effectively implements the Playfair cipher, allowing users to encrypt and decrypt messages based on a given keyword. The key matrix generation and text preparation functions ensure that the Playfair rules are correctly applied during the encryption and decryption processes. The test\_playfiar function provides a simple interface for testing the cipher with user inputs.

**Project Code**

**텍스트, 스크린샷, 소프트웨어, 멀티미디어 소프트웨어이(가) 표시된 사진

자동 생성된 설명텍스트, 스크린샷이(가) 표시된 사진

자동 생성된 설명텍스트, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명**

**Output**

**텍스트, 스크린샷, 폰트, 디자인이(가) 표시된 사진

자동 생성된 설명**