Name: Harsh Mishra
Roll no: 64
Batch: T21

Aim: To perform Cryptanalysis or decoding of polyalphabetic ciphers: Playfair & Vigenere cipher.

Theory:

Playfair Cipher :

The Playfair cipher is a classical encryption algorithm that uses a digraph (pair of letters) substitution technique to encode plaintext. It was invented by Charles Wheatstone in 1854 but is named after Lord Playfair, who promoted its use.

Key Preparation

1. **Key Square Creation:**
    - **Choose a keyword or phrase (e.g., "KEYWORD").**
    - **Remove duplicates and combine the letters with the remaining letters of the alphabet (excluding 'J', which is usually combined with 'I').**
    - **Construct a 5x5 grid with these letters.**

For example, with the keyword "KEYWORD":

K E Y W O

R D A B C

F G H I/J L

M N P Q S

T U V X Z

Name: Harsh Mishra
Roll no: 64
Batch: T21

Encryption Process

1. **Pairing Letters:**
    - **Split the plaintext into digraphs (pairs of two letters). If there's an odd number of letters, add an extra letter (usually 'X') to the last pair.**
    - **If a pair consists of the same letter (like "LL"), replace one letter with a different letter (e.g., "LX" or "YL").**
2. **Encryption Rules:**
    - **Same Row: If both letters are in the same row of the grid, replace them with the letters immediately to their right. Wrap around to the beginning of the row if needed.**
    - **Same Column: If both letters are in the same column, replace them with the letters immediately below. Wrap around to the top if needed.**
    - **Rectangle: If the letters form a rectangle, replace each letter with the letter in its own row but in the column of the other letter of the pair.**

Decryption Process

1. **Pairing Letters:**
    - **Similar to encryption, but the rules for substitution are reversed.**
2. **Decryption Rules:**
    - **Same Row: Replace each letter with the letter immediately to its left. Wrap around to the end of the row if needed.**
    - **Same Column: Replace each letter with the letter immediately above. Wrap around to the bottom if needed.**
    - **Rectangle: Replace each letter with the letter in its own row but in the column of the other letter of the pair.**

The Playfair cipher is more secure than simple substitution ciphers because it encrypts pairs of letters and provides more complexity, but it’s still vulnerable to more advanced cryptanalysis techniques.

Name: Harsh Mishra
Roll no: 64
Batch: T21

Vigenere Cipher :

The Vigenère cipher is a method of encrypting alphabetic text using a series of different Caesar ciphers based on the letters of a keyword. It is a polyalphabetic substitution cipher. Here's a basic overview of how it works:

Encryption

1. **Choose a Keyword: Select a keyword (e.g., "KEYWORD").**
2. **Prepare the Text: Write the plaintext (the text you want to encrypt) and repeat the keyword to match the length of the plaintext.**

Example:

- **Plaintext: HELLO**
- **Keyword: KEYKE (repeated to match length)**

3. **Encrypt Using the Vigenère Square:**
    - **The Vigenère square is a table of 26 x 26 letters, where each row is a Caesar cipher shifted by one position more than the previous row.**

To encrypt:

- **Locate the letter of the plaintext in the column of the keyword letter in the Vigenère square.**
- **The intersecting letter in the row of the keyword letter is the ciphertext letter.**

For example, if the plaintext letter is H and the keyword letter is K, you find H in the K column and the intersection gives you the ciphertext letter.

Decryption

To decrypt, you essentially reverse the process:

1. **Prepare the Text: Write the ciphertext and repeat the keyword to match the length.**
2. **Decrypt Using the Vigenère Square:**
    - **Find the ciphertext letter in the row corresponding to the keyword letter in the Vigenère square.**
    - **The column intersection gives you the plaintext letter.**

Name: Harsh Mishra
Roll no: 64
Batch: T21

Output:

Playfair Cipher:

Encryption:

Name: Harsh Mishra
Roll no: 64
Batch: T21

Decryption:

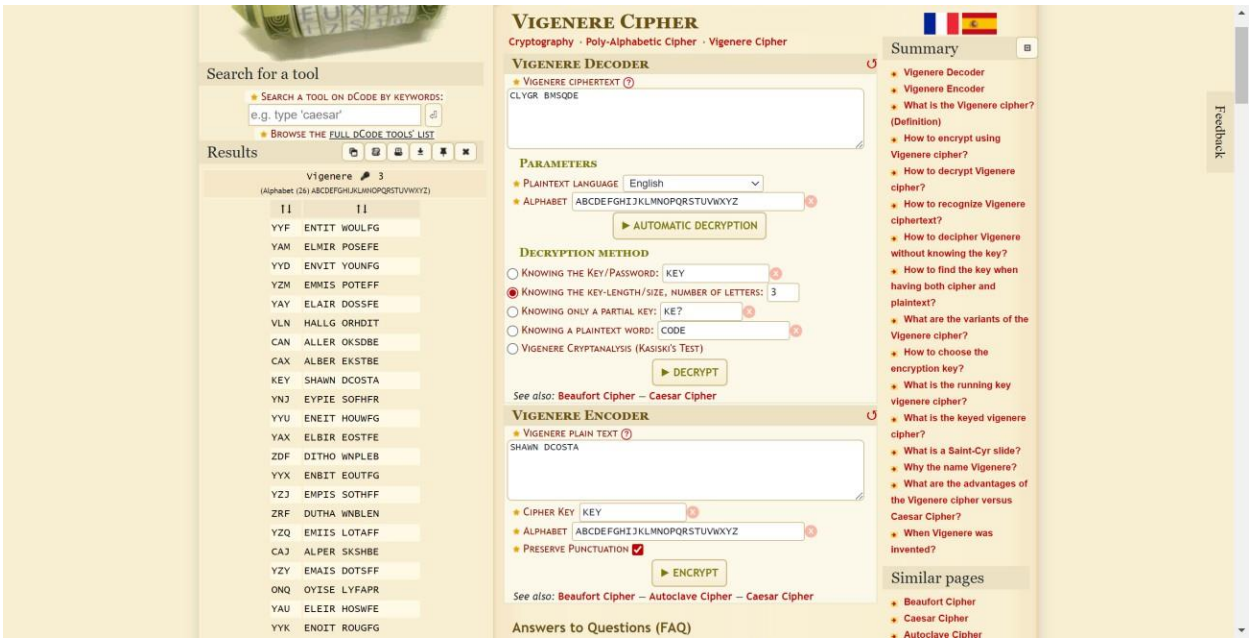
Name: Harsh Mishra
Roll no: 64
Batch: T21

Vigenere Cipher:

Encryption:

Decryption:

Name: Harsh Mishra
Roll no: 64
Batch: T21



Name: Harsh Mishra
Roll no: 64
Batch: T21

Conclusion: Illustration of symmetric cryptography by implementing classical ciphers (Shift and Mono-alphabetic) is achieved (LO1 is achieved).