Assignment 2

Aim:- Cryptanalysis or decoding of polyalphabetic ciphers: Playfair, Vigenere cipher.

Lo Mapped:- Lo 1

Theory:-

Playfair Cipher:

• The Playfair Cipher is a polygraphic substitution cipher that operates on pairs of letters (digraphs) instead of individual letters.

• It uses a 5x5 matrix (usually called a key square) containing a keyword's unique letters followed by the remaining letters of the alphabet (excluding duplicates).

• The matrix is used to encrypt and decrypt letters in pairs.

• Encryption Steps:

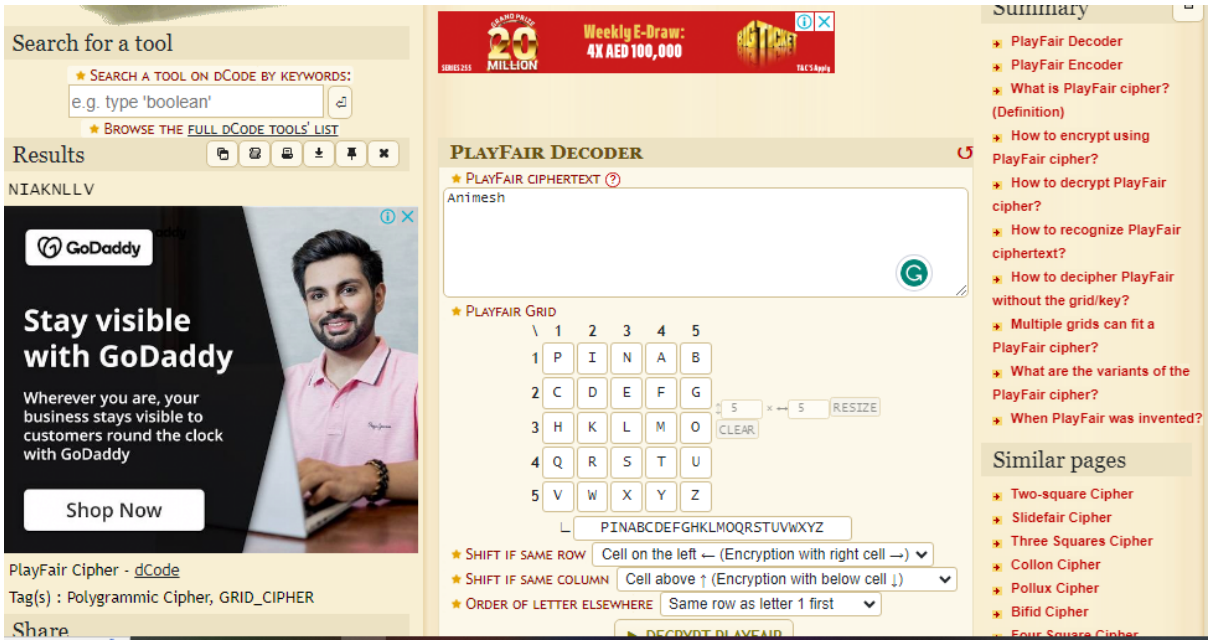
1. Break the plaintext into pairs (digraphs) of letters.

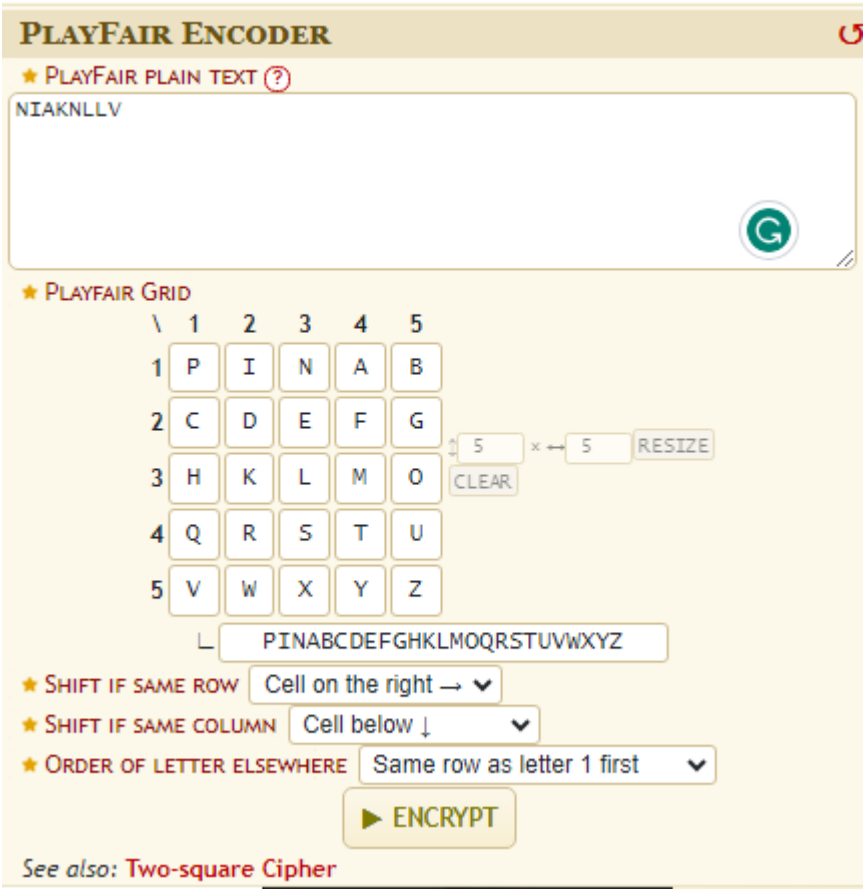
2. If a pair has identical letters, insert a filler letter (like X) between them.

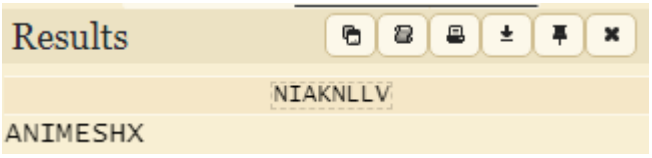
3. For each digraph, find the positions of its letters in the key square.

4. Apply specific rules to determine the ciphertext letters based on the positions.

• Decryption is essentially the reverse process of encryption.







Vigenère Cipher:

• The Vigenère Cipher is a polyalphabetic substitution cipher that uses a keyword to determine different shift values for each letter.

• It's an improvement over the Caesar Cipher, where each letter can be shifted by a different amount.

• Encryption Steps:

1. Repeatedly write the keyword above the plaintext.

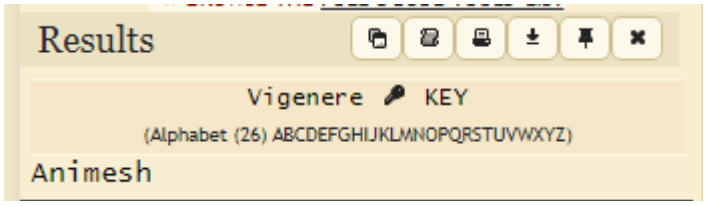
2. Convert both the keyword and the plaintext into numbers using a key-to-number mapping.

3. Add the numbers of the keyword and the plaintext modulo the size of the alphabet to get the ciphertext numbers.

4. Convert the ciphertext numbers back to letters using a number-to-key mapping.

• The keyword's length determines the periodicity of the cipher's key. Longer keywords increase security.

• Decryption requires subtracting the keyword values from the ciphertext values and then converting back to plaintext letters.



Conclusion:
We conclude that both the Playfair Cipher and the Vigenère Cipher offer improvements over basic substitution ciphers, adding complexity and making frequency analysis more difficult. However, they can still be vulnerable to more sophisticated attacks, and modern cryptographic methods like the Advanced Encryption Standard (AES) have replaced them in secure communication.