

## 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.

The screenshot shows a web-based Playfair Decoder tool. On the left, there is a search bar with the text 'Search for a tool' and a search button. Below it, a results section displays a GoDaddy advertisement. The main section is titled 'PLAYFAIR DECODER' and contains a text input field for the ciphertext, which currently contains 'Animesh'. Below the input field is a 5x5 grid for the key, with the letters P, I, N, A, B in the first row, C, D, E, F, G in the second row, H, K, L, M, O in the third row, Q, R, S, T, U in the fourth row, and V, W, X, Y, Z in the fifth row. To the right of the grid is a 'RESIZE' button. Below the grid is a dropdown menu for the 'PLAYFAIR CIPHERTEXT' type, currently set to 'PINABCEFGHKLMOQRSTUVWXYZ'. There are also buttons for 'SHIFT IF SAME ROW', 'SHIFT IF SAME COLUMN', and 'ORDER OF LETTER ELSEWHERE'. The bottom of the interface has a 'DECRYPT PLAYFAIR' button. On the right side, there is a 'Summary' section with a list of links related to the Playfair cipher, and a 'Similar pages' section with links to other cipher tools.

# PLAYFAIR ENCODER

★ PLAYFAIR PLAIN TEXT (?)

NIAKNLLV

★ PLAYFAIR GRID

\	1	2	3	4	5
1	P	I	N	A	B
2	C	D	E	F	G
3	H	K	L	M	O
4	Q	R	S	T	U
5	V	W	X	Y	Z

5

×

5

RESIZE

CLEAR

L

PINABCDEFGHIJKLMOQRSTUVWXYZ

★ SHIFT IF SAME ROW

Cell on the right →

★ SHIFT IF SAME COLUMN

Cell below ↓

★ ORDER OF LETTER ELSEWHERE

Same row as letter 1 first

▶ ENCRYPT

See also: [Two-square Cipher](#)

## Results

NIAKNLLV

ANIMESHX

## 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.

Search for a tool

★ SEARCH A TOOL ON dCode BY KEYWORDS:  
e.g. type 'boolean'

★ BROWSE THE FULL dCODE TOOLS' LIST

Results

Vigenere KEY  
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

Qjkcaux



### VIGENERE DECODER

★ VIGENERE CIPHERTEXT ?

Animesh

**PARAMETERS**

★ PLAINTEXT LANGUAGE English

★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

▶ AUTOMATIC DECRYPTION

**DECRYPTION METHOD**

☒ KNOWING THE KEY/PASSWORD: KEY

☐ KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3

☐ KNOWING ONLY A PARTIAL KEY: KE?

☐ KNOWING A PLAINTEXT WORD: CODE

☐ VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

▶ DECRYPT

See also: Beaufort Cipher – Caesar Cipher

- ★ Vigenere Decoder
- ★ Vigenere Encoder
- ★ What is the Vigenere cipher? (Definition)
- ★ How to encrypt using Vigenere cipher?
- ★ How to decrypt Vigenere cipher?
- ★ How to recognize Vigenere ciphertext?
- ★ How to decipher Vigenere without knowing the key?
- ★ How to find the key when having both cipher and plaintext?
- ★ What are the variants of the Vigenere cipher?
- ★ How to choose the encryption key?
- ★ What is the running key vigenere cipher?
- ★ What is the keyed vigenere

### VIGENERE ENCODER

★ VIGENERE PLAIN TEXT ?

Qjkcaux

★ CIPHER KEY KEY

★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

★ PRESERVE PUNCTUATION ☒

▶ ENCRYPT

See also: Beaufort Cipher – Autoclave Cipher – Caesar Cipher

Results

Vigenere KEY  
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

Animesh

### 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.