

Aim:

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

LO Mapping: LO1**Theory & Output:****Playfair Cipher**

The Playfair cipher is a manual symmetric encryption technique and was the first digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but it was named after Lord Playfair who promoted its use. It encrypts pairs of letters (digraphs) instead of single letters, which makes it significantly harder to break than simpler substitution ciphers.

Features:**1. Key Square:**

- The Playfair cipher uses a 5x5 grid filled with letters of the alphabet. Normally, the letters "I" and "J" are combined, so the 26-letter alphabet fits into the 25 spaces of the square.
- The key square is filled with a keyword first, omitting any duplicate letters, and then the remaining letters of the alphabet.

2. Encryption Process:

- The plaintext message is split into pairs of letters. If there are any repeated letters in a pair or if there's a single remaining letter, an 'X' is added to adjust.
- Each pair of letters is encrypted according to their position in the key square:
 - If both letters are in the same row, each letter is replaced with the letter immediately to its right (wrapping around to the beginning of the row if necessary).
 - If both letters are in the same column, each letter is replaced with the letter immediately below it (wrapping around to the top of the column if necessary).
 - If the letters form a rectangle, each letter is replaced by the letter on the same row but at the column of the other letter in the pair.

PLAYFAIR ENCODER

★ PLAYFAIR PLAIN TEXT ?
thadomaTshahani

★ PLAYFAIR GRID

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

CIPHER A B D F G K L M N O Q S T U V W X Y Z

★ 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

Results

THADOMALSHAHANI

YDBFTGBKTPDIFKPW

3. Decryption Process:

- Decryption is the reverse of encryption:
 - If both letters are in the same row, each letter is replaced with the letter immediately to its left.
 - If both letters are in the same column, each letter is replaced with the letter immediately above.
 - If the letters form a rectangle, each letter is replaced by the letter on the same row but at the column of the other letter in the pair.

PLAYFAIR CIPHER

Cryptography · Polygrammic Cipher · PlayFair Cipher

PLAYFAIR DECODER

★ PLAYFAIR CIPHERTEXT ?

YDBFTGBKTPDIFKPW

★ PLAYFAIR GRID

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

5 × 5 RESIZE

CLEAR

CIPHERABDFGKLMNOQSTUVWXYZ

★ SHIFT IF SAME ROW Cell on the left ← (Encryption with right cell →) ▾

★ SHIFT IF SAME COLUMN Cell above ↑ (Encryption with below cell ↓) ▾

★ ORDER OF LETTER ELSEWHERE Same row as letter 1 first ▾

▶ DECRYPT PLAYFAIR

▶ BRUTEFORCE DECRYPTION ATTACK WITH THE GRID

WITHOUT KNOWING KEY

★ KNOWN PLAINTEXT

▶ KNOWN PLAINTEXT ATTACK

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

THADOMALSHAHANIX

Vigenère Cipher

The Vigenère cipher is a method of encrypting alphabetic text by using a simple form of polyalphabetic substitution. A keyword is repeated until it matches the length of the plaintext. Each letter of the plaintext is then shifted along some number of places defined by the corresponding letter of the key.

Key Features:

1. **Key:**
 - The Vigenère cipher uses a keyword, where each letter of the keyword specifies a shift for the corresponding letter of the plaintext.
2. **Encryption Process:**
 - The plaintext is written out, and the keyword is repeated until it matches the length of the plaintext.

- Each letter of the plaintext is shifted along the alphabet by the number of positions defined by the corresponding letter of the keyword (where A = 0, B = 1, ..., Z = 25).

The screenshot shows the 'VIGENERE ENCODER' web application. It has a title bar with a refresh icon. Below the title, there are four input fields: 'VIGENERE PLAIN TEXT' containing 'pankajparihar', 'CIPHER KEY' containing 'PANKAJ', 'ALPHABET' containing 'ABCDEFGHIJKLMNOPQRSTUVWXYZ', and 'PRESERVE PUNCTUATION' which is checked. An 'ENCRYPT' button is located below these fields. At the bottom, there is a link that says 'See also: Beaufort Cipher – Autoclave Cipher – Caesar Cipher'.

The screenshot shows the search results for the 'Vigenere' tool. The search bar contains 'e.g. type \'boolean\''. Below the search bar, there is a link 'BROWSE THE FULL DCODE TOOLS\' LIST'. The results section shows 'Vigenere' with a key 'PANKAJ' and the alphabet '(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)'. The resulting ciphertext is 'eaauaseaeshjg'.

3. Decryption Process:

- The cipher text is written out, and the keyword is repeated until it matches the length of the cipher text.
- Each letter of the cipher text is shifted backwards by the number of positions defined by the corresponding letter of the keyword.

VIGENERE DECODER

★ VIGENERE CIPHERTEXT ?
 eaauaseaeshjg

PARAMETERS

★ PLAINTEXT LANGUAGE English

★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

▶ AUTOMATIC DECRYPTION

DECRYPTION METHOD

☒ KNOWING THE KEY/PASSWORD: PANKAJ

☐ 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](#)

★ [BROWSE THE FULL DCODE TOOLS LIST](#)

Results

Vigenere PANKAJ

(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

pankajparihar

Conclusion:

In conclusion, while polyalphabetic ciphers like the Playfair and Vigenere ciphers offer more security than mono-alphabetic ciphers by using multiple alphabets, they are still vulnerable to cryptanalysis. Techniques such as Kasiski examination and frequency analysis adapted for polyalphabetic ciphers can break these encryption methods. Despite their increased complexity, they are not immune to systematic cryptanalysis, which can reveal the key or plaintext under certain conditions.