**Substitution techniques : CAESAR CIPHER**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

**Text** : ABCDEFGHIJKLMNOPQRSTUVWXYZ

**Shift**: 7

**Cipher**: HIJKLMNOPQRSTUVWXYZABCDEFG

**Text** : ABCDEFGHIJKLMNOPQRSTUVWXYZ

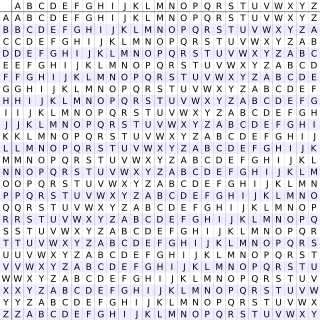
**Shift**: 21

**Cipher**: VWXYZABCDEFGHIJKLMNOPQRSTU

ERMHJEJAMQRWR9VIDYAVARDHINI

**Vigenere Cipher:** Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of [polyalphabetic substitution](https://en.wikipedia.org/wiki/Polyalphabetic_cipher). A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the [Vigenère square or Vigenère table](https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher#/media/File:Vigen%C3%A8re_square_shading.svg).

* The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible[Caesar Ciphers](https://www.geeksforgeeks.org/caesar-cipher/).
* At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
* The alphabet used at each point depends on a repeating keyword.



**Ex1. Ciphertext : QIVYIQAJDPDNA**

**Original/Decrypted Text : VIDYAVARDHINI**

**Ex2. Ciphertext : SMFPBZMYLWHMZYRAKPZI**

**Original/Decrypted Text : LIFEISFULLOFSURPRISE**

**--------------------------------**

**Playfair Cipher Encryption**

Algorithm steps:   
 **Generate the key Square(5×5):**

* + The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.
  + The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

1. **Algorithm to encrypt the plain text:** The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.   
   **For example:**

**PlainText**: "information"

**After Split:** 'in' 'fo' 'rm' 'at' 'io' 'nz'

**Playfair Cipher Encryption**

**Ex1.**

**Key text: Vidyavardhini**

**Plain text: InformationTechnology**

**Cipher text: dhouetvzhurwlrnbsfpfax**

**Ex2.**

**Key text: Vidyavardhini**

**Plain text: dhouetvzhurwlrnbsfpfax**

**Deciphered text: informationtechnologyz**

**Ex3.**

**Key text: VASAI**

**Plain text: VIDYAVARDHINI**

**Cipher text: abfwsaipckbmby**

**IN FO RM AT IO NT EC HN OL OG YX**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **I** | **N** | **F** | **O** | **R** |
| **M** | **A** | **T** | **B** | **C** |
| **D** | **E** | **G** | **H** | **K** |
| **L** | **P** | **Q** | **S** | **U** |
| **V** | **W** | **X** | **Y** | **Z** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **I** | **N** | **F** | **O** | **R** |
| **M** | **A** | **T** | **B** | **C** |
| **D** | **E** | **G** | **H** | **K** |
| **L** | **P** | **Q** | **S** | **U** |
| **V** | **W** | **X** | **Y** | **Z** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **I** | **N** | **F** | **O** | **R** |
| **M** | **A** | **T** | **B** | **C** |
| **D** | **E** | **G** | **H** | **K** |
| **L** | **P** | **Q** | **S** | **U** |
| **V** | **W** | **X** | **Y** | **Z** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **I** | **N** | **F** | **O** | **R** |
| **M** | **A** | **T** | **B** | **C** |
| **D** | **E** | **G** | **H** | **K** |
| **L** | **P** | **Q** | **S** | **U** |
| **V** | **W** | **X** | **Y** | **Z** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **I** | **N** | **F** | **O** | **R** |
| **M** | **A** | **T** | **B** | **C** |
| **D** | **E** | **G** | **H** | **K** |
| **L** | **P** | **Q** | **S** | **U** |
| **V** | **W** | **X** | **Y** | **Z** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **I** | **N** | **F** | **O** | **R** |
| **M** | **A** | **T** | **B** | **C** |
| **D** | **E** | **G** | **H** | **K** |
| **L** | **P** | **Q** | **S** | **U** |
| **V** | **W** | **X** | **Y** | **Z** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **I** | **N** | **F** | **O** | **R** |
| **M** | **A** | **T** | **B** | **C** |
| **D** | **E** | **G** | **H** | **K** |
| **L** | **P** | **Q** | **S** | **U** |
| **V** | **W** | **X** | **Y** | **Z** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **I** | **N** | **F** | **O** | **R** |
| **M** | **A** | **T** | **B** | **C** |
| **D** | **E** | **G** | **H** | **K** |
| **L** | **P** | **Q** | **S** | **U** |
| **V** | **W** | **X** | **Y** | **Z** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **I** | **N** | **F** | **O** | **R** |
| **M** | **A** | **T** | **B** | **C** |
| **D** | **E** | **G** | **H** | **K** |
| **L** | **P** | **Q** | **S** | **U** |
| **V** | **W** | **X** | **Y** | **Z** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **I** | **N** | **F** | **O** | **R** |
| **M** | **A** | **T** | **B** | **C** |
| **D** | **E** | **G** | **H** | **K** |
| **L** | **P** | **Q** | **S** | **U** |
| **V** | **W** | **X** | **Y** | **Z** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **I** | **N** | **F** | **O** | **R** |
| **M** | **A** | **T** | **B** | **C** |
| **D** | **E** | **G** | **H** | **K** |
| **L** | **P** | **Q** | **S** | **U** |
| **V** | **W** | **X** | **Y** | **Z** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **I** | **N** | **F** | **O** | **R** |
| **M** | **A** | **T** | **B** | **C** |
| **D** | **E** | **G** | **H** | **K** |
| **L** | **P** | **Q** | **S** | **U** |
| **V** | **W** | **X** | **Y** | **Z** |