Cypher Canvas

Learn PlayFair Cipher

The Playfair cipher is a classical substitution cipher invented in the 19th century by Charles Wheatstone and later promoted by Lord Playfair. It is a digraphic substitution cipher, meaning it encrypts pairs of letters rather than individual letters like the simpler Caesar cipher. Here's a detailed explanation of how the Playfair cipher works along with its rules and points:

Rules of the Playfair Cipher:

- Key Preparation: A key (often a keyword) is chosen, and the letters of the key are arranged in a 5x5 grid known as the "Playfair Square." The remaining letters of the alphabet are then filled in the grid, omitting any repeated letters from the key.
- Alphabet Pairing: The letters of the plaintext are paired up into digraphs (groups of two letters). If there's an odd number of letters, a dummy letter like 'X' or 'Q' is appended at the end.
- Handling Repeated Letters: If a pair contains the same letter twice, a dummy letter (usually 'X') is inserted between them. For example, "hello" becomes "HE LX LO".
- Encryption: Each pair of letters is encrypted using the following rules:
- If the letters are in the same row of the Playfair Square, replace them with the letters to their immediate right, wrapping around if necessary.
- If the letters are in the same column of the Playfair Square, replace them with the letters immediately below, wrapping around if necessary.
- If the letters form a rectangle, replace them with the letters on the same row but at the opposite corners of the rectangle.

Decryption: The decryption process is the reverse of encryption. It follows the same rules but in reverse order.

Points to Note:

- Playfair Square: The key determines the arrangement of the Playfair Square. It's usually a 5x5 grid with the 26 letters of the alphabet, excluding one letter (usually 'J' which is often replaced with 'I').
- Letter Pairing: The plaintext is divided into pairs of letters (digraphs). Each pair is then encrypted separately.
- Handling Odd Letters: If there's an odd number of letters, a dummy letter is added to the end to form pairs.
- Dummy Letters: 'X' or 'Q' is commonly used as a dummy letter when necessary, but any letter can be used.
- Row and Column Wrapping: When a letter is at the edge of the Playfair Square, wrapping around occurs to find the replacement letter.
- Rectangular Rule: If the two letters being encrypted form a rectangle on the Playfair Square, the letters on the same row but at the opposite corners of the rectangle are used for encryption.
- Letter 'J': Traditionally, 'J' and 'I' are treated as the same letter in the Playfair Square, or 'J' is omitted altogether.

Example:
Plain Text: "instrumentsz"
Encrypted Text: gatlmzclrqtx

- Encryption:
- i -> g
- n -> a
- s -> t
- t -> l
- r -> m
- u -> z
- m -> c
- e -> l
- n -> r
- t -> q
- s -> t
- z -> x