Caesar Cipher

Caesar Cipher is one of the oldest and simplest classical encryption methods. It is named after Julius Caesar who used this method to secure his military messages. Caesar Cipher encryption is based on replacing each letter in the original text with another letter located after it in the alphabet by a fixed number of steps.

**Working Principles:**

1. Original text: The plain text to be encrypted.

2. Key: The number of steps or shifts by which the letters are replaced.

3. Encrypted text: The text resulting from applying the Caesar Cipher to the original text using the key.

**Example:**

If the original text is: "HELLO".

And the key is 3.

The encrypted text becomes: "KHOOR", where each letter is replaced by the third letter after it in the alphabet.

**Features:**

Simple and easy to implement.

Suitable for learning the basics of encryption.

**Disadvantages:**

Weak in security, as it can be easily broken using statistical analysis or trial and error, due to the limited number of possible keys (the number of letters in the alphabet).

**Uses:**

The Caesar cipher is used today for educational purposes to illustrate basic concepts in cryptography, but it is impractical in modern cryptography due to its ease of cracking.

**Conclusion:**

The Caesar cipher is one of the first building blocks of cryptography. Despite its simplicity, it was of great importance in ancient times.

Algorithm

Caesar\_Cipher(Texte, Clé, Mode):

Début

Résultat ← chaîne vide ( Initialisation de la chaîne de résultat)

Si Mode = "chiffrement" alors

Clé ← Clé ( Utilisation de la clé telle quelle)

Sinon

Clé ← -Clé ( Inverse la clé pour le déchiffrement)

Pour chaque caractère char dans Texte:

Si char est une lettre alors

Si char est une lettre majuscule alors

Début

start ← valeur ASCII de 'A' (65)

Fin

Sinon

Début

start ← valeur ASCII de 'a' (97)

Fin

FinSi

nouveau\_caractère ← (valeur ASCII de char - start + Clé) % 26 + start

Ajouter nouveau\_caractère à Résultat

Sinon

Ajouter char à Résultat

FinPour

Retourner Résultat ( Le texte chiffré ou déchiffré)

Fin