**Caesar Cipher** **in Cryptography**

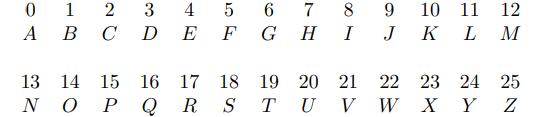
The **Caesar Cipher** is one of the simplest and oldest methods of encrypting messages, named after Julius Caesar, who reportedly used it to protect his military communications. This technique involves shifting the letters of the alphabet by a fixed number of places. For example, with a shift of three, the letter ‘A’ becomes ‘D’, ‘B’ becomes ‘E’, and so on. Despite its simplicity, the Caesar Cipher formed the groundwork for modern cryptographic techniques.

**What is Caesar Cipher Technique?**

The Caesar cipher is a simple encryption technique that was used by Julius Caesar to send secret messages to his allies. It works by shifting the letters in the plaintext message by a certain number of positions, known as the “shift” or “key”. The Caesar Cipher technique is one of the earliest and simplest methods of encryption techniques.

It’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet. For example, with a shift of 1, A would be replaced by B, B would become C, and so on.

To make all of this more mathematical, consider the following conversion table for the English alphabet:



* Using the table, we can represent the letters in our message “cookie” with their corresponding numbers: 2 14 14 10 8 4.
* Now add 3 (the encryption key) to each number to get: 5 17 17 13 11 7.
* Now use the table to replace these numbers with their corresponding letters: FRRNLH.

Formula :

a ≡ b (mod m) means m is a divisor of a – b

In our situation, we take the number m (the modulus), to be equal to the size of our character set, so m = 26. Now take each number x from the representation of the message and perform the following arithmetic: add 3 to x, and if the result is between 0 and 25, stop; otherwise, replace x + 3 with the integer y between 0 and 25 that satisfies y ≡ x + 3 (mod 26).

Encryption of the message “pizza” using a shift cipher with encryption key 3 looks like this:

p 🡪 15 🡪 15 + 3 ≡ 18 (mod 26) 🡪 S

i 🡪 8 🡪 8 + 3 ≡ 11 (mod 26) 🡪 L

z 🡪 25 🡪 25 + 3 ≡ 2 (mod 26) 🡪 C

z 🡪 25 🡪 25 + 3 ≡ 2 (mod 26) 🡪 C

a 🡪 0 🡪 0 + 3 ≡ 3 (mod 26) 🡪 D

Now let’s decrypt the message, given ciphertext is: LQXLXUJCN, key = 9, to decrypt it we need to add 17 or subtract 9 to each of the numbers representing the ciphertext letters.

L 🡪 11 🡪 11 + 17 ≡ 2 (mod 26) 🡪 c

Q 🡪 16 🡪 16 + 17 ≡ 7 (mod 26) 🡪 h

X 🡪 23 🡪 23 + 17 ≡ 14 (mod 26) 🡪 o

L 🡪 11 🡪 11 + 17 ≡ 2 (mod 26) 🡪 c

X 🡪 23 🡪 23 + 17 ≡ 14 (mod 26) 🡪 o

U 🡪 20 🡪 20 + 17 ≡ 11 (mod 26) 🡪 l

J 🡪 9 🡪 9 + 17 ≡ 0 (mod 26) 🡪 a

C 🡪 2 🡪 2 + 17 ≡ 19 (mod 26) 🡪 t

N 🡪 13 🡪 13 + 17 ≡ 4 (mod 26) 🡪 e

Plaintext : chocolate