Caesar Cipher in Cryptography

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. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

Cryptography Algorithm For the Caesar Cipher

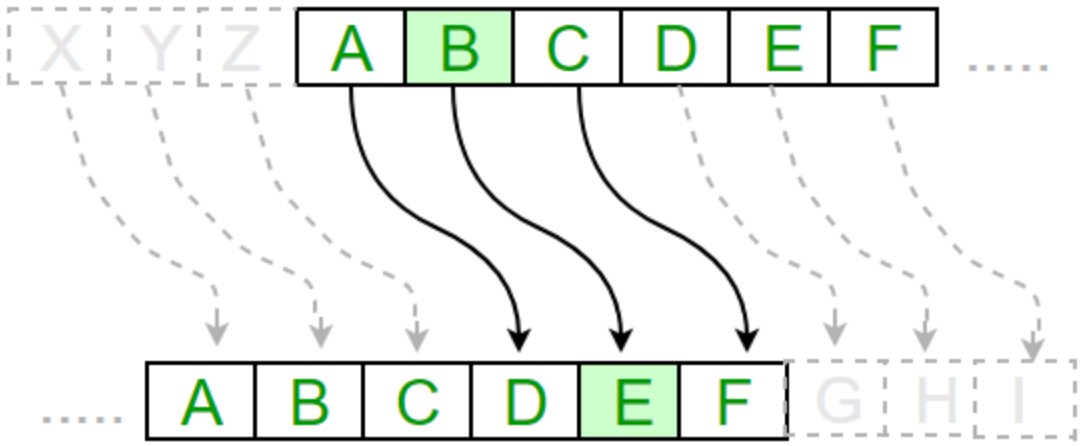
1. Write down the plaintext message.
2. Choose a shift value. In this case, we will use a shift of 3.
3. Replace each letter in the plaintext message with the letter that is three positions to the right in the alphabet.

For Example , HELLO -> KHOOR

H becomes K (shift 3 from H)
E becomes H (shift 3 from E)
L becomes O (shift 3 from L)
L becomes O (shift 3 from L)
O becomes R (shift 3 from O

$E_n(x)=(x+n) \mod 26$
(Encryption Phase with shift n)

$D_n(x)=(x-n) \mod 26$
(Decryption Phase with shift n)



Implementation of Caesar Cipher :-

```
# caesar cipher

def caesar_cipher(p,k):
    res=""
    for i in range(len(p)):
        c=p[i]
        if(c.isupper()):
            res+=chr((ord(c)+k-65)%26+65)
        else:
            res+=chr((ord(c)+k-97)%26+97)
    return res
```

O/P:

```
┌──(kali㉿kali)-[~]
└─$ python lab3.py
The Caesar Cipher: KhoorqZruog
```