**EXPERIMENT NO :- 02**

**ROLL NO: DATE:**

**Aim :** To study and implement Caeser Cipher algorithm.

**Theory:**

**Introduction:**

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 technique. 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.

Example:-

Here is an example of how to use the Caesar cipher to encrypt the message “HELLO” with a shift of 3:

Write down the plaintext message: HELLO

Choose a shift value. In this case, we will use a shift of 3.

Replace each letter in the plaintext message with the letter that is three positions to the right in the alphabet.

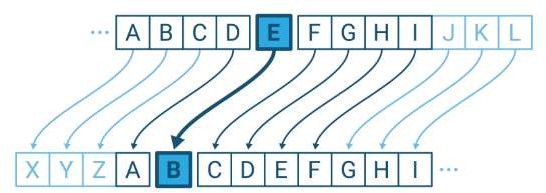
H becomes K (shift 3 from H) E becomes H (shift 3 from E) L becomes O (shift 3 from L) L becomes O (shift 3 from L) O becomes R (shift 3 from O)

4.The encrypted message is now “KHOOR”.

To decrypt the message, you simply need to shift each letter back by the same number of positions. In this case, you would shift each letter in “KHOOR” back by 3 positions to get the original message, “HELLO”.

**E\_n(x)=(x+n)mod\ 26 (Encryption Phase with shift n)**

**D\_n(x)=(x-n)mod\ 26 (Decryption Phase with shift n)**



**Fig: Caeser Cipher Algorithm**

**Algorithm for Caesar Cipher:**

Input:

Choose a shift value between 1 and 25.

Write down the alphabet in order from A to Z.

Create a new alphabet by shifting each letter of the original alphabet by the shift value. For example, if the shift value is 3, the new alphabet would be:

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

Replace each letter of the message with the corresponding letter from the new alphabet. For example, if the shift value is 3, the word “hello” would become “khoor”.

To decrypt the message, shift each letter back by the same amount. For example, if the shift value is 3, the encrypted message “khoor” would become “hello”.

Procedure:

Traverse the given text one character at a time .

For each character, transform the given character as per the rule, depending on whether we’re encrypting or decrypting the text.

Return the new string generated.

A program that receives a Text (string) and Shift value( integer) and returns the encrypted text.

**Implementation Code:- (Using Python)**

encrypt = []

decrypt = []

alphabet\_dict = {chr(i + 97): i for i in range(26)}

print(alphabet\_dict)

text = "ADVAIT"

key = 77

new\_text = list(text.lower())

string = ''.join(new\_text)

print("Text is :", string)

inverse\_dict = dict(zip(alphabet\_dict.values(), alphabet\_dict.keys()))

# Encrypt

for i in range(len(new\_text)):

val = new\_text[i]

new\_val = alphabet\_dict[val]

mod = (new\_val + key) % 26

enc = inverse\_dict.get(mod)

encrypt.append(enc)

string1 = ''.join(encrypt)

print("Encrypted text : ", string1)

# decrypt

for i in range(len(string1)):

val = string1[i]

new\_val = alphabet\_dict[val]

mod = (new\_val - key) % 26

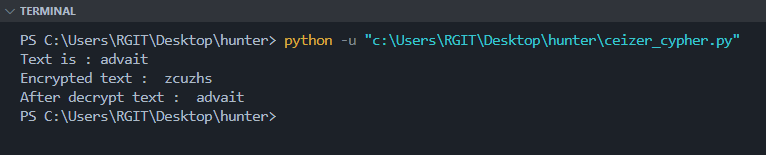
enc = inverse\_dict.get(mod)

decrypt.append(enc)

string2 = ''.join(decrypt)

print("After decrypt text : ", string2)

**Output:-**

****

**Conclusion:-**

We have studied and implemented Caeser Cipher algorithm in cryptography and system security