## EXPERIMENT NUMBER: 2

**Date of Performance :**

**Date of Submission :**

**AIM**: Design and Implement a product cipher using Substitution ciphers.

**THEORY:**

- 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.
- Thus to cipher a given text we need an integer value, known as a shift which indicates the number of positions each letter of the text has been moved down.
  The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.
- For example, if the shift is 3, then the letter A would be replaced by the letter D, B would become E, C would become F, and so on. The alphabet is wrapped around so that after Z, it starts back at A.
- Here is an example of how to use the Caesar cipher to encrypt the message "HELLO" with a shift of 3:

1. Write down the plaintext message: HELLO
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.

   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)

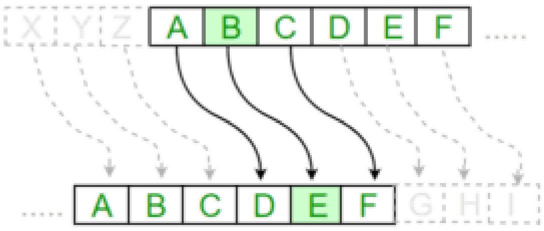
*Algorithm of Caesar Cipher*

The algorithm of Caesar cipher holds the following features −

- Caesar Cipher Technique is the simple and easy method of encryption technique.
- It is simple type of substitution cipher.
- Each letter of plain text is replaced by a letter with some fixed number of positions down with alphabet.

.

## EXAMPLE:



### Examples:

**Plain Text:** I am studying Data Encryption
**Key:** 4
**Output:** M eqwxyhCmrkHexeIrgvCtxmsr

**Plain Text:** ABCDEFGHIJKLMNOPQRSTUVWXYZ
**Key:** 4
**Output:**EFGHIJKLMNOPQRSTUVWXYZabcd

**Caesar Cipher**

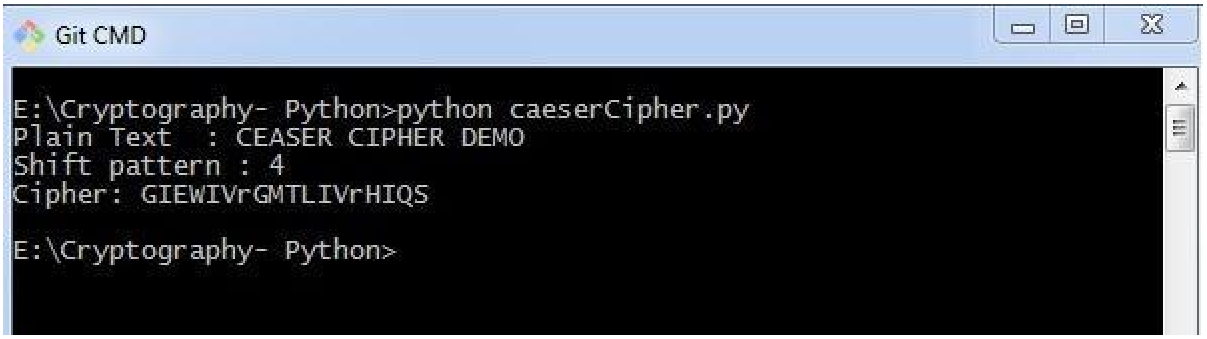
The program implementation of Caesar cipher algorithm is as follows –

```
def encrypt(text,s):
result =""
# transverse the plain text
for i in range(len(text)):
char= text[i]
# Encrypt uppercase characters in plain text

if(char.isupper()):
result+=chr((ord(char)+ s-65)%26+65)
# Encrypt lowercase characters in plain text
else:
result+=chr((ord(char)+ s -97)%26+97)
return result
```

```
#check the above function
text="CEASER CIPHER DEMO"
s =4

print"Plain Text : "+ text
print"Shift pattern : "+str(s)
print"Cipher: "+ encrypt(text,s)
```

Output

You can see the Caesar cipher, that is the output as shown in the following image −



```
E:\Cryptography- Python>python caeserCipher.py
Plain Text  : CEASER CIPHER DEMO
Shift pattern : 4
Cipher: GIEWIVrGMTLIVrHIQS

E:\Cryptography- Python>
```

## CONCLUSION/ Outcome:

we successfully product cipher using Substitution ciphers.

**Marks & Signature:**

| R1<br>(5 Marks) | R2<br>(5 Marks) | R3<br>(5 Marks) | Total<br>(15 Marks) | Signature |
|---|---|---|---|---|
| | | | | |