**Name: Drishti Bhatia** **Roll Number: 07**
**FYMCA** **Block Chain Lab**

# Practical No: 01

## Aim: To implement Caesar Cipher (Symmetric Encryption) and show the encryption as well as decryption process.

**Theory:**

❖ **What is Cryptography?**

- Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.

- **Cryptography focuses on four different objectives:**

**1. Confidentiality:** Confidentiality ensures that only the intended recipient can decrypt the message and read its contents.

**2. Non-repudiation:** Non-repudiation means the sender of the message cannot backtrack in the future and deny their reasons for sending or creating the message.

**3. Integrity:** Integrity focuses on the ability to be certain that the information contained within the message cannot be modified while in storage or transit.

**4. Authenticity:** Authenticity ensures the sender and recipient can verify each other’s identities and the destination of the message.

- In addition, cryptography also covers the obfuscation of information in images using techniques such as microdots or merging.
- Ancient Egyptians were known to use these methods in complex hieroglyphics, and Roman Emperor Julius Caesar is credited with using one of the first modern ciphers.
- When transmitting electronic data, the most common use of cryptography is to encrypt and decrypt email and other plain-text messages.
- The simplest method uses the symmetric or "secret key" system. Here, data is encrypted using a secret key, and then both the encoded message and secret key are sent to the recipient for decryption.
- The problem? If the message is intercepted, a third party has everything they need to decrypt and read the message.
- To address this issue, cryptologists devised the asymmetric or "public key" system. In this case, every user has two keys: one public and one private.
- Senders request the public key of their intended recipient, encrypt the message and send it along.
- When the message arrives, only the recipient's private key will decode it — meaning theft is of no use without the corresponding private key.

### ❖ What is Symmetric Encryption.

- Encryption is a process to change the form of any message in order to protect it from reading by anyone.
- Symmetric Key Cryptography also known as Symmetric Encryption is when a secret key is leveraged for both encryption and decryption functions.
- This method is the opposite of Asymmetric Encryption where one key is used to encrypt and another is used to decrypt.
- During this process, data is converted to a format that cannot be read or inspected by anyone who does not have the secret key that was used to encrypt it.
- The success of this approach depends on the strength of the random number generator that is used to create the secret key.
- Symmetric Key Cryptography is widely used in today's Internet and primarily consists of two types of algorithms, Block and Stream. Some common encryption algorithms include the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES).
- This form of encryption is traditionally much faster than Asymmetric however it requires both the sender and the recipient of the data to have the secret key.

### ❖ Explanation about Caesar cipher

- 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.

**Formula:**

$E(x) = (x+n) \bmod 26$ (Encryption Phase with shift n)

$D(x) = (x-n) \bmod 26$ (Decryption Phase with shift n)

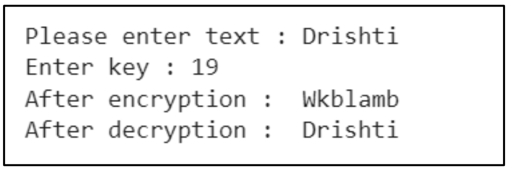
- The Caesar cipher is a kind of replacement (substitution) cipher, where all letter of plain text is replaced by another letter.
- Caesar ciphers is a weak method of cryptography. It can be easily hacked. It means the message encrypted by this method can be easily decrypted.

**Name: Drishti Bhatia** **Roll Number: 07**
**FYMCA** **Block Chain Lab**

**Code:**

```
def ceaser_cipher(text, shift, texttype):
 cipher = ''
 for char in text:
   if char == ' ':
     cipher = cipher + char
   elif char.isupper():
    if texttype=='encrypt':
      cipher = cipher + chr((ord(char) + shift - 65) % 26 + 65)
    else:
      cipher = cipher + chr((ord(char) - shift - 65) % 26 + 65)
   else:
      if texttype=='encrypt':
        cipher = cipher + chr((ord(char) + shift - 97) % 26 + 97)
      else:
        cipher = cipher + chr((ord(char) - shift - 97) % 26 + 97)
 return cipher
plainText= input("Please enter text : ")
key= int(input("Enter key : "))
encrypted= ceaser_cipher(plainText, key, 'encrypt')
decrypted= ceaser_cipher(encrypted, key, 'decrypt')
print("After encryption : ", encrypted)
print("After decryption : ", decrypted)
```

**Output:**



```
Please enter text : Drishti
Enter key : 19
After encryption :  Wkblamb
After decryption :  Drishti
```

**Conclusion:** We have successfully implemented Caesar Cipher (Symmetric Encryption) and shown the encryption as well as decryption process.