# PRACTICAL 1

**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.
* The term is derived from the Greek word *kryptos,* which means hidden. It is closely associated to encryption, which is the act of scrambling ordinary text into what's known as ciphertext and then back again upon arrival.
* 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.
* In Symmetric-key encryption the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure.
* It also requires a safe method to transfer the key from one party to another.
* Traditional private/secret/single key cryptography uses one key
* Both parties share the same key (which is kept secret).
* Before communications begin, both parties must exchange the shared secret key.
* Each pair of communicating entities requires a unique shared key.
* The key is not shared with other communication partners.
* If this key is disclosed communications are compromised
* Also is symmetric, parties are equal. Hence does not protect sender from receiver forging a message & claiming is sent by sender.

# 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.

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

D(x) = (x-n) mod 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.

# 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:**



**Conclusion:**

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