NAME	Nishant Baruah
ROLL NO	A053
BATCH	2

THEORY :-

The Caesar cipher is a classic method of encryption that is named after Julius Caesar, who is reputed to have used it to communicate with his generals. It belongs to the category of substitution ciphers, specifically a type of monoalphabetic cipher, where each letter in the plaintext is replaced by a letter some fixed number of positions down or up the alphabet. The "shift" or "key" is the number of positions each letter in the plaintext is moved to create the ciphertext.

Properties

1. Simplicity: The Caesar cipher is straightforward to understand and implement, making it a good introductory example of encryption techniques.
2. Symmetry: The same algorithm can be used for both encryption and decryption, provided the shift direction is reversed.
3. Vulnerability: Due to its simplicity, the Caesar cipher is very vulnerable to various forms of cryptanalysis, such as frequency analysis, brute force attacks, and known-plaintext attacks. In frequency analysis, for example, an attacker can analyze the frequency of characters in the ciphertext and compare them to known frequencies in the language of the plaintext, effectively determining the shift used.

Modern Use

While the Caesar cipher is not secure by today's standards and thus not suitable for protecting sensitive information, it remains a popular educational tool. It introduces concepts fundamental to the study of cryptography and the development of more complex encryption methods.

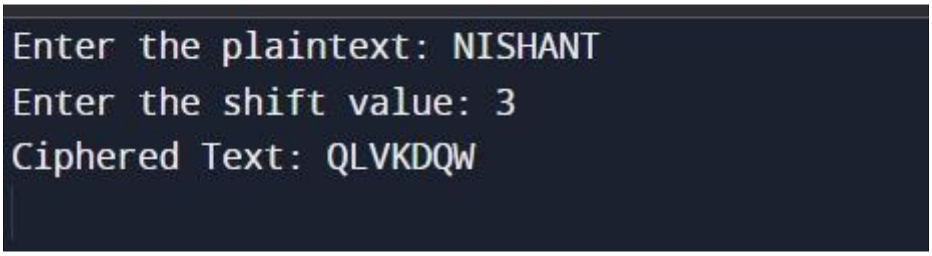
In modern cryptographic applications, more sophisticated algorithms, such as AES (Advanced Encryption Standard) and RSA, are used to ensure secure communication.

CODE:-

```
def caesar_cipher(plaintext, shift):
    alphabet = 'abcdefghijklmnopqrstuvwxyz'
    ciphered_text = ''
        for char in plaintext:
        if char.lower() in alphabet:
            pos = alphabet.find(char.lower())
            new_pos = (pos + shift) % 26
            if char.isupper():
                ciphered_text += alphabet[new_pos].upper()
            else:
                ciphered_text += alphabet[new_pos]
        else:
            ciphered_text += char

    return ciphered_text
plaintext = input("Enter the plaintext: ") shift
= int(input("Enter the shift value: "))
ciphered_text = caesar_cipher(plaintext, shift)print(f"Ciphered
Text: {ciphered_text}")
```

OUTPUT :-



```
Enter the plaintext: NISHANT
Enter the shift value: 3
Ciphered Text: QLVKDQW
```