

# Lab Report 01

## **Experiment Name:** Implementation of Caesar Cipher

### **Theory:**

The Caesar Cipher is one of the oldest and simplest encryption techniques, named after Julius Caesar who is historically credited with its use. It is a substitution cipher where each letter in the plaintext is shifted a certain number of places down or up the alphabet. The key determines the number of positions each letter is shifted.

### **History:**

The Caesar Cipher has its origins in ancient Rome, where Julius Caesar used it to encrypt his messages. The method provided a basic level of security against casual eavesdropping but is relatively easy to break with modern cryptographic analysis.

### **Applications of Cryptography:**

1. Secure Communication
2. Online Banking and Transactions
3. E-commerce Security
4. Password Protection
5. Virtual Private Networks
6. Digital Signatures
7. Secure Email Communication
8. Blockchain Technology
9. Software and Firmware Integrity
10. Military and Government Communications

## Code:

```
#include <iostream>
#include <string>
using namespace std;

string encrypt(string text, int key) {
    for (char& c : text) {
        if (isalpha(c)) {
            c = 'a' + (c - 'a' + key) % 26;
        }
    }
    return text;
}

string decrypt(string text, int key) {
    return encrypt(text, 26 - key);
}

int main() {

    cout << "Enter the string to encrypt: ";
    string originalText;
    getline(cin, originalText);

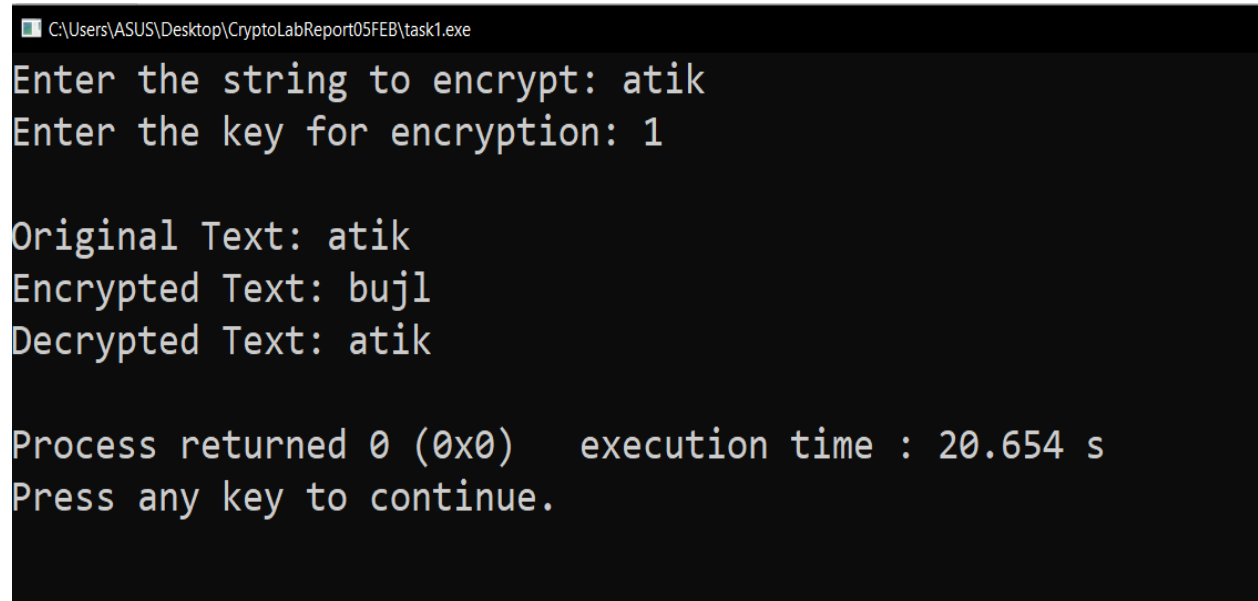
    cout << "Enter the key for encryption: ";
    int key;
    cin >> key;

    for (char& c : originalText) {
        c = tolower(c);
    }

    string encryptedText = encrypt(originalText, key);
    string decryptedText = decrypt(encryptedText, key);
    cout << "\nOriginal Text: " << originalText << endl;
    cout << "Encrypted Text: " << encryptedText << endl;
```

```
cout << "Decrypted Text: " << decryptedText << endl;  
return 0;  
}
```

## Output:



```
C:\Users\ASUS\Desktop\CryptoLabReport05FEB\task1.exe  
Enter the string to encrypt: atik  
Enter the key for encryption: 1  
  
Original Text: atik  
Encrypted Text: bujl  
Decrypted Text: atik  
  
Process returned 0 (0x0)   execution time : 20.654 s  
Press any key to continue.
```

## Result and Discussion:

After implementing the Caesar Cipher algorithm in the lab, the results demonstrate a successful encryption and decryption process. The encrypted text is produced by shifting each letter in the plaintext according to the specified key, and decryption is achieved by shifting the letters back. We can use this algorithm for Educational Purposes, Puzzles, and Games.

## Conclusion:

In conclusion, the Caesar Cipher is a historic encryption technique that laid the foundation for more advanced cryptographic methods. While it is no longer suitable for secure communication due to its vulnerability, studying the Caesar Cipher provides valuable insights into the principles of encryption and the importance of key management.