

FACULTY OF ENGINEERING AND TECHNOLOGY BACHELOR OF TECHNOLOGY

Information and Network Security(INS) (203105310)

VII SEMESTER

Computer Science & Engineering Department



Logo

Description automatically generated

CERTIFICATE

*This is to certify that*

*Mr.* **LUCKY PATHAN** *with Enrollment No.* **210303105790** has *successfully completed her laboratory experiments in the subject (with Code)* **Information and Network Security (203105310)** *from the department of* **Computer Science and Engineering** *during the academic year* ***2023-2024.***



**Date of Submission …..…………. Staff In charge …..……………**

**Head of Department ……………..**

**TABLE OF CONTENT:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **SR NO.** | **PRACTICAL LIST** | **START DATE** | **END DATE** | **SIGN** | **MARKS** |
| 1 | Implement Caesar cipher encryption-decryption |  |  |  |  |
| 2 | Implement Monoalphabetic cipher encryption-decryption |  |  |  |  |
| 3 | Implement Playfair cipher encryption-decryption |  |  |  |  |
| 4 | Implement Polyalphabetic cipher encryption-decryption |  |  |  |  |
| 5 | Implement Hill cipher encryption-decryption |  |  |  |  |
| 6 | Implement Simple Transposition encryption-decryption. |  |  |  |  |
| 7 | Implement One time pad encryption-decryption |  |  |  |  |
| 8 | Implement Diffi-Hellmen Key exchange Method |  |  |  |  |
| 9 | Implement RSA encryption-decryption algorithm |  |  |  |  |
| 10 | Demonstrate working of Digital Signature using Cryptool |  |  |  |  |

# PRACTICAL- 1

AIM: **Implement Caesar Cipher Encryption Decryption.**

**Theory:**

Julius Caesar employed the Caesar cipher, a basic encryption method, to communicate with his friends in secret. The "shift" or "key" is used to change the plaintext message's letters by a certain number of places. One of the earliest and most basic encryption techniques is the Caesar Cypher. It is merely a type of substitution cypher in which each letter of a given text is substituted with a letter that is located a certain number of positions farther down the alphabet. As an illustration, if there was a shift of 1, A would be replaced by B, B by C, and so on. Julius Caesar, who reportedly employed it to communicate with his officials, is said to be the inspiration for the method's moniker.

Therefore, in order to cypher a given text, we require an integer value, or "shift," that represents the number of positions down which each letter in the text has been moved. Modular arithmetic can be used to express the encryption by first converting the letters' letters into numbers, where A = 0, B = 1,..., Z = 25. Mathematically, encrypting a letter with a shift n is expressed as. For instance, if the shift is 3, the letter A would be changed to the letter D, B would be changed to the letter E, C would be changed to the letter F, and so on. After Z, the alphabet turns around and recursively begins at A.



(Encryption Phase with shift n)

 (Decryption Phase with shift n)

**Code :**

#include<iostream>

using namespace std;

void encrypt(char plainText[],int len,int key){

for(int i = 0;i<len;i++){

plainText[i] = (((plainText[i]+key)-65)%26)+65;

}

for(int i = 0;i<len;i++){

cout<<plainText[i];

}

}

void decrypt(char plainText[],int len,int key){

for(int i = 0;i<len;i++){

plainText[i] = ((((plainText[i]-key)-65)+26)%26)+65;

}

for(int i = 0;i<len;i++){

cout<<plainText[i];

}

}

int main(){

int key,len;

cout<<"Enter number of letter :";

cin>>len;

cout<<"Enter key :";

cin>>key;

cout<<"Enter word :";

char text[len];

for (int i = 0; i < len; i++)

{

cin>>text[i];

}

cout<<endl<<"encrypt: ";

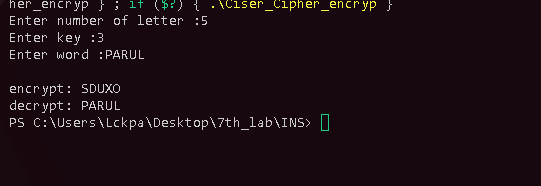
encrypt(text,len,key);

cout<<endl<<"decrypt: ";

decrypt(text,len,key);

return 0;

}

**Output :**

**Analysis:**

Breaking of Caesar cipher through brute force is possible with powerful computers, the complexity can be represented as **O(26)** or more simply **O(1)** suggesting that it can be deciphered within a constant time.

**Suggestion:**

The complexity of cracking the Caesar cipher four times over the output of each cipher is **O(264)**  or **O(26n)**[n can be defined by user], which can also be expressed as **O(456976)**. This means that the number of possible combinations an attacker would need to try to crack the cipher increases to 4,56,976, making it significantly more difficult compared to a single application of the Caesar cipher.

# PRACTICAL- 2

AIM: **Implement Monoalphabetic cipher encryption-decryption.**

**Theory:**