Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY | PUNE
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

T.Y.B.Tech (CSE)

Information Security

Lab Assignment No – A1

Name: Aniruddha Shende

Roll number: PE04

Batch: E1

Panel: E

PE-04 Aniruddha Shende

Name :- Aniruddha Arun Shende
Roll no :- PE04
Batch :- E1
Panel :- E

Subject :- INFORMATION SECURITY

LAB ASSIGNMENT - A1

Implement Any Classical Cryptographic techniqu using Java / Python / C++.

Aim :- Implement any classic cryptographic technique using Java or Python or C++.

Objective :-
Conceal the context of some message from al except the sender & receipient (privacy or secrecy

Theory :-

* Caeser Cipher in Classical Cryptography

The Caeser Cipher technique is one of the earliest & simplest method of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. for eg :- A shift of 1, A would be replaced by B, B would become C & so on.

For eg:- If we replace each letter of a message by a letter which is fixed distance away. Each letter is replaced by a letter three positions further down the object i.e. alphabet.

Eg:- mit pune → plw sxqh.

General Caeser Cipher can be :-

$$c = E_K(p) = (p+k) \bmod 26$$

$$p = D_K(c) = (c-k) \bmod 26$$

Algorithm for Caeser Cipher.

Input :- ① String of lowercase letters called Text.

② An integer between 0-25 ~~denote~~ denoting shift

Procedure :-

① Traverse the given text one character at a time

② For each character, transform the given character as per the rule, depending on whether we are decrypting / encrypting the text.

③ Return New String generated

* Monoalphabetic Cipher :-

A Monoalphabetic cipher is any cipher in which the letters of the plain text are mapped to cipher text letters based on a single alphabetic key.

The relationship between a character in plain text & a character in cipher text is one-to-one.

For eg:-

Plain letters : a b c d e f

Cipher letters : D K V Q F I

Conclusion:-

Thus we have successfully implemented a classical cryptographic technique using C++.

FAQs:-

1) What are various classical ciphers.

Ans 1) Following are the various classical ciphers:-

(a) Atbash Cipher.
(b) ~~Caes~~ Caesar Cipher
(c) Baconian Cipher
(d) Simple Substitution Ciphers
(e) Affine Cipher.

2) Compare steganography & Cryptography.

Ans 2)

Steganography	Cryptography
a) It means covered writing	a) It means secret writing.
b) It is less popular than cryptography	b) It is more popular than steganography.
c) Attack's name in steganography is Steganalysis	c) Attack's name in cryptography is cryptanalysis.

3) State the reasons why classical ciphers are obsolete.

Ans 3) For classical ciphers an attacker should not be able to find the key even if he knows any amount of plaintext & corresponding ciphertext even he could select plaintext or ciphertext himself.

Classical ciphers do not satisfy these much stronger criteria & hence are no longer of interest for serious applications.

4) How to carry out cryptanalysis of classical cryptography?

Ans 4) Cryptanalysis is the study of methods for obtaining the meaning of encrypted information, without knowing access to secret information that is typically required to do so.

Thus, in cryptanalysis, we find how the system works & find a secret key. It is also called as code breaking.

Depending on what information is available & what type of cipher is being analyzed, cryptanalysts can follow one or more attack models to crack a cipher.

5) Write how different disciplines of art, science & engineering have contributed for information security.

Ans 5) From early ages, people have thought & attempted to secure things so as other people cannot aquire information about those things. We can see many secret codes which earlier people used & how they made their systems secure.

Computer Engineers & Scientists have learnt a lot from Arts, Siene & engineering, by developing the technology which makes information security a science.

Program code :

```
// Name : Aniruddha Shende
// Roll no : PE04
// Batch : E1
// Panel : E
#include <iostream>
using namespace std;

// This function receives str and shift and
// returns the encrypted str
string encrypt(string str, int s)
{
    string encrypted_string = "";
    for (int i = 0; i < str.length(); i++)
    {
        if ((str[i]) >= 'A' && (str[i]) <= 'Z')
            encrypted_string += char(int(str[i] + s -
65) % 26 + 97);
        else
            encrypted_string += char(int(str[i] + s -
97) % 26 + 65);
    }
    return encrypted_string;
}

string decrpyt(string str, int s)
{
    string decrypted_string = "";
    for (int i = 0; i < str.length(); i++)
    {
        if ((str[i]) >= 'A' && (str[i]) <= 'Z')
            decrypted_string += char(int(str[i] - s -
65) % 26 + 97);
```

```
        else
            decrypted_string += char(int(str[i] - s -
97) % 26 + 65);
    }
    return decrypted_string;
}

// Driver program to test the above function
int main()
{
    char ch = true;
    while (ch == true)
    {
        string str;
        cout << "Enter the string you want to Encrypt
or Decrypt : ";
        cin >> str;
        int s;
        cout << "Enter Key : ";
        cin >> s;
        cout << "1. Encrypt \n2. Decrypt \n\nEnter
your choice\n";
        int n;
        cin >> n;
        if (n == 1)
        {
            cout << "\nEncrypted str is: " <<
encrypt(str, s);
        }
        else if (n == 2)
        {
            cout << "\nDecrypted str is: " <<
decrpyt(str, s);
        }
```

```
        else
        {
            return 0;
        }
        cout << "\n\nDo you want to continue ?? (1->yes)";
        int choice;
        cin >> choice;
        (choice == 1) ? ch = true : ch = false;
    }
    return 0;
}
```

Output :

```
ani@Aniruddhas-MacBook-Pro IS LAbs % cd "/Users/ani/Desktop/Tri-8/IS LAbs/p1/" && g++ --std=c++17 a.cpp -o a && "/Users/ani/Desktop/Tri-8/IS LAbs/p1/"a
Enter the string you want to Encrypt or Decrypt : MITWPU
Enter Key : 3
1. Encrypt
2. Decrypt

Enter your choice
1

Encrypted str is: plwzsx

Do you want to continue ?? (1->yes)1
Enter the string you want to Encrypt or Decrypt : plwzsx
Enter Key : 3
1. Encrypt
2. Decrypt

Enter your choice
2

Decrypted str is: MITWPU

Do you want to continue ?? (1->yes)0
ani@Aniruddhas-MacBook-Pro p1 %
```