LAB Manual

PART A

(PART A : TO BE REFFERED BY STUDENTS)

**Experiment No.01**

**A.1 Aim:**

To implement a simple substitution cipher and a transposition cipher

**A.2 Prerequisite:**

Fundamentals of encryption and decryption process

**A.3 Outcome:**

**After successful completion of this experiment students will be able to** 1. Learn and appreciate the operation of classical ciphers

2. Understand the shortcomings of these ciphers

**A.4 Theory:**

The art and science of keeping messages secure is **cryptography.** A message is **plaintext (**sometimes called **cleartext).** The process of disguising a message in such a way as to hide its substance is **encryption.** An encrypted message is **ciphertext.** The process of turning ciphertext back into plaintext is **decryption.**

A **cryptographic algorithm**, also called a **cipher**, is the mathematical function used for encryption and decryption. Both the encryption and decryption operations use a key. The range of possible values of the key is called the **keyspace.**

* *EK(M) = C*
* *DK(C) = M*
* *DK(EK(M)) = M*

There are two basic types of classical ciphers:

* + Transposition ciphers
  + Substitution ciphers

A **substitution cipher** is one in which each character in the plaintext is substituted for another character in the ciphertext. The receiver inverts the substitution on the ciphertext to recover the plaintext.

For example:

**Caesar Cipher,** in which each plaintext character is replaced by the character three to the right modulo 26 ("A" is replaced by "D," "B" is replaced by "E,"..., "X“ is replaced by "A," "Y" is replaced by "B," and "Z" is replaced by "C") is a simple substitution cipher.

A **transposition cipher** is obtained by performing some sort of permutation on the plain text symbols. Here, the symbols remain the same but their order is shuffled around.

For example:

In a simple columnar transposition cipher, the plain text is written horizontally row by row in rectangle of fixed width. To form cipher, the text is read off vertically. The order of columns is kept secret and is the key. Decryption involves writing the ciphertext vertically of identical length and then reading the text horizontally. Let me illustrate this with the help of an example:

Consider the sentence: “IT IS RAINING TODAY”

Key value: 4 (rectangular width)

Encryption process:

|  |  |  |  |
| --- | --- | --- | --- |
| I | T | I | S |
| R | A | I | N |
| I | N | G | T |
| O | D | A | Y |

Ciphertext: IRIO TAND IIGA SNTY

PART B

(PART B : TO BE COMPLETED BY STUDENTS)

***(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no Black board access available)***

|  |  |
| --- | --- |
| Roll. No. E040 | Name: Shlok Shah |
| Class: BTech CS | Batch: E2 |
| Date of Experiment:26/11/19 | Date of Submission:26/11/19 |
| Grade: | |

**B.1 Software Code written by student:**

**Caesar Cipher**

#include <iostream>

using namespace std;

int main()

{

cout<<"Enter text: ";

string text;

cin>>text;

cout<<"Enter shift: ";

int s;

cin>>s;

string result = "";

for (int i=0;i<text.length();i++)

{

result += char(int(text[i]+s-65)%26 +65);

}

cout << "\nText : " << text;

cout << "\nShift: " << s;

cout << "\nCipher: " << result;

string text1=result;

string result1;

for (int i=0;i<text1.length();i++)

{

result1 += char(int(text1[i]-s-65)%26 +65);

}

cout << "\n\nCipher : " << text1;

cout << "\nShift: " << s;

cout << "\nText: " << result1;

}

**Columnar Transposition Cipher**

#include<iostream>

using namespace std;

int main()

{

char mat[3][3];

char name[9];

cout<<"Enter name: ";

cin>>name;

int k=0;

for (int i=0;i<3;i++)

{

for(int j=0;j<3;j++)

{

mat[i][j]=name[k];

k++;

}

}

cout<<"Encrypted text: ";

for (int i=0;i<3;i++)

{

for(int j=0;j<3;j++)

{

cout<<mat[j][i];

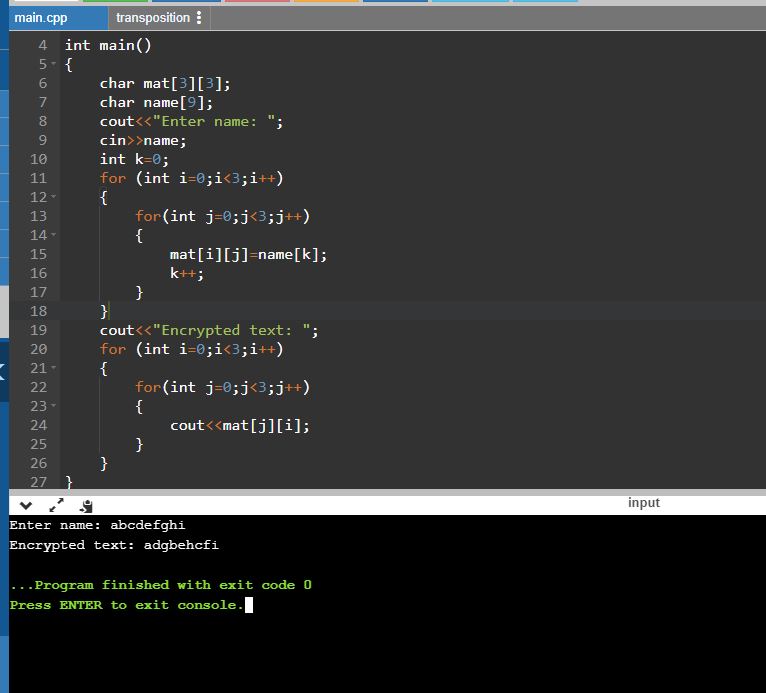
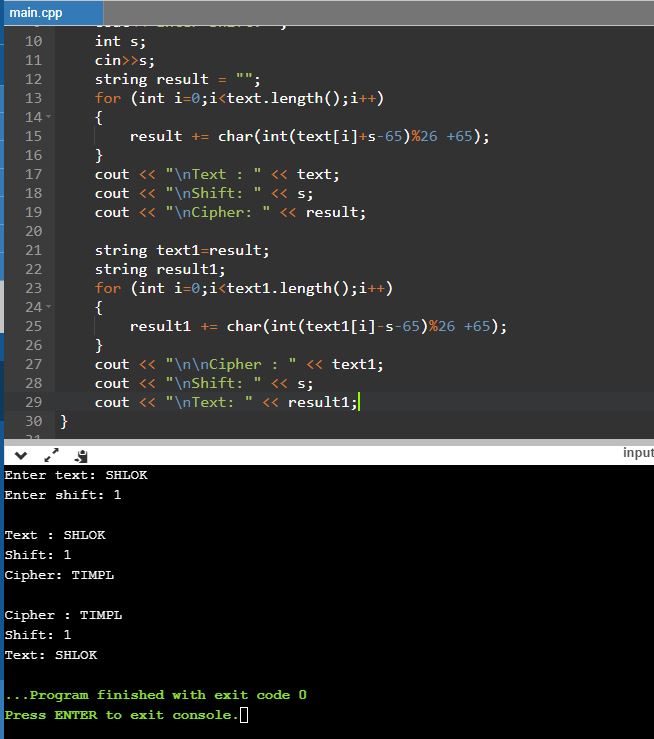
}

}

}

**B.2 Input and Output:**

**Caesar Cipher**



**B.3 Observations and learning:**

***(Students are expected to comment on the output obtained with clear observations and learning for each task/ sub part assigned)***

The more complex the encryption method, the better the encryption and harder for the code to be broken. A substitution method relatively very easy to encrypt and decrypt.

**B.4 Conclusion:**

*(****Students must write the conclusion as per the attainment of individual outcome listed above and learning/observation noted in section B.3)***

Encryption is done using a key or a shift value as the basis for the encryption. It is a very important security measure and a proper encryption is done by selecting a confidential and complicated key.

**B.5 Questions:**

**Q1. Enlist the advantages and limitations of substitution and transposition ciphers.**

The major problem with simple substitution ciphers is that the frequencies of letters are not masked at all. If the enciphered message LOOQLOTQWMUOAEFAEN was intercepted, the interceptor could look at the frequencies of each letter and compare them to the frequencies of English

The major disadvantage of the transposition cipher is that keys very close to the correct key will reveal long sections of legible plaintext.

**Q2. Explain the algorithms used for encryption in whatsapp, instagram and gmail.**

WhatsApp partnered with Open Whisper Systems for the cryptographic portions of messaging. The process involves a variation of Off the Record (OTR), Perfect Forward Secrecy (PFS), and the Double Ratchet Algorithm (DRA).

Open Whisper Systems has blog posts on cryptographic ratcheting, and their Signal Protocol Integration for WhatsApp.

Google uses Transport Layer Security (TLS) to encrypt emails in transit. It provides an encrypted pipe through which your emails can travel. But TLS depends on both the sender’s and recipient’s email provider, so it doesn’t always work.

When you send a Gmail-encrypted email, your browser contacts Google’s server and creates a secure connection. The message is encrypted, sent to the server and decrypted. The server repeats the process with the next server, until it reaches your recipient’s server.

To help prevent unencrypted emails from exposure, Google warns users when TLS won’t work; an open red padlock symbol signifies that an incoming or outgoing message isn’t encrypted.

Google for Work users can also require TLS, preventing their email from sending or accepting messages that can’t be secured with Gmail encryption. You can require TLS for all inbound messages, all outbound messages or just certain domains and email addresses.