# ENCRYPTION USING TRANSPOSITION TECHNIQUES

A Project Report

Submitted in the partial fulfillment of the requirements for the

award of the degree of

## Bachelor of Technology in

## Department of Computer Science and Engineering

Submitted by:

2010030055   GANDE SAITEJA

2010030272   GILLA SAMANTH

2010030236    MD ADNAN

2010030083    K SAI ANIRUDH

Under the esteemed guidance of

Dr. Gayathri Edamadaka



## Department of Computer Science and Engineering

K L University Hyderabad,

Aziz Nagar, Moinabad Road, Hyderabad – 500 075, Telangana, India.

March, 2022

# DECLARATION

The Project Report entitled "Encryption using transposition technique" is a record of bonafide work of Mr. GANDE SAITEJA (2010030055), Mr. GILLA SAMANTH (2010030272), Mr. MD. ADNAN (2010030236) and Mr. K. ANIRUDH (2010030083) submitted in partial fulfillment for the award of B. Tech in the Department of Computer Science and Engineering to the K L University, Hyderabad. The results embodied in this report have not been copied from any other Departments/University/Institute.

Mr. GANDE SAITEJA – 2010030055

Mr. GILLA SAMANTH – 2010030272

Mr. MD. ADNAN – 2010030236

Mr. K. ANIRUDH – 2010030083

# **CERTIFICATE**

This is to certify that the Project Report entitled "Encryption using transposition Techniques" is being submitted by Mr. GANDE SAITEJA bearing Regd. No. 2010030055, Mr. GILLA SAMANTH bearing Regd. No. 20100300272, Mr. MD.ADNAN bearing Regd. No. 2010030236 and Mr. K.TRIBHUVAN bearing Regd. No. 2010030402 submitted in partial fulfillment for the award of B.Tech in Computer Science and Engineering to the K L University, Hyderabad is a record of bonafide work carried out under our guidance and supervision.

The results embodied in this report have not been copied from any other department/ University/ Institute.

Signature of the Supervisor

Dr. Gayathri Edamadaka

(Associate Professor)

Signature of the HOD                                    Signature of the External Examination

# ACKNOWLEDGEMENT

First and foremost, we thank the lord almighty for all his grace & mercy showered upon us, for completing this project successfully.

We take grateful opportunity to thank our beloved Founder and Chairman who has given constant encouragement during our course and motivated us to do this project. We are grateful to our Principal **Dr. L. Koteswara Rao** who has been constantly bearing the torch for all the curricular activities undertaken by us.

We pay our grateful acknowledgement & sincere thanks to our Head of the Department **Dr. Chiranjeevi Manike** for his exemplary guidance, monitoring and constant encouragement throughout the course of the project. We thank **Dr. Gayathri Edamadaka** of our department who has supported throughout this project holding a position of supervisor.

We whole heartedly thank all the teaching and non-teaching staff of our department without whom we won't have made this project a reality. We would like to extend our sincere thanks especially to our parents, our family members and friends who have supported us to make this project a grand success.

# **INDEX**

# INTRODUCTION

Encryption is the process of translating plain text data (*plaintext*) into something that appears to be random and meaningless (*ciphertext*). Decryption is the process of converting ciphertext back to plaintext. To encrypt more than a small amount of data, symmetric encryption is used. A symmetric key is used during both the encryption and decryption processes. To decrypt a particular piece of ciphertext, the key that was used to encrypt the data must be used. The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using the key. If a really good encryption algorithm is used, then there's no technique significantly better than methodically trying every possible key. For such an algorithm, the longer the key, the more difficult it is to decrypt a piece of ciphertext without possessing the key. It's difficult to determine the quality of an encryption algorithm. Algorithms that look promising sometimes turn out to be very easy to break, given the proper attack. When selecting an encryption algorithm, it's a good idea to choose one that's been in use for several years, and has successfully resisted all attacks.

In the cryptography system, a transposition cipher is a method of encryption by changing the position of plain text into different position. In this technique, the character or group of characters are shifted into different positions. That is the order of units is changed mathematically and gets the cipher text. Primarily, the transportation technique explores how to minimize total transportation cost or to maximize total revenue/contribution of its products by devising a meaningful but optimal goods transferring system. The transportation technique is a subset of linear programming and useful to devise the transport network optimally, thus consisting of similar assumptions as in linear programming.

Encryption has long been used by militaries and government to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. For example, the CSI reported that in 2007, 71% of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage. Encryption can be used to protect data "at rest", such as information stored on computers and storage devices In recent years, there have been numerous reports of confidential data, such as customers' personal records, being exposed through loss or theft of laptops or backup drives; encrypting such files at rest helps protect them if physical security measures fail. Digital rights management systems, which prevent unauthorized use or reproduction of copyrighted material and protect software against reverse engineering, is another somewhat different example of using encryption on data at rest. Encryption is also used to protect data in transit, for example data being transferred via networks

# ABSTRACT

This presentation contains the details of the project 'Encryption using transportation Techniques'. Text-encryption is a process in which the message send by the sender is encrypted so that only receiver can understand the message. Encryption converts data into scrambled text. The decoded text can be read by the receiver which maintains the security. Information is an important asset. Today, storing of information and data securely has become important. Cloud computing is the current trend. Cloud is place where these data can be stored. Cloud can be a private, public or hybrid. Cloud computing allows for easy storage, access, and manipulation of various data. It is less expensive, allows for backing up data and helps in disaster recovery. It is flexible, easy to use and scalable. Security of this data over cloud is a crucial aspect. When two parties communicate over a medium, the two parties ensure that third party should not get access to their message. That is, they ensure confidentiality of the message over the communication medium. A simple way to achieve this is using cryptography. There are many substitution cipher techniques and transposition cipher techniques which allows conversion of plain text to cipher text.

# ENCRYPTION

A simple example for a transposition cipher is columnar transposition cipher where each character in the plain text is written horizontally with specified alphabet width. The cipher is written vertically, which creates an entirely different cipher text. It uses the same secret key to encrypt the raw message at source, transmit the encrypted message to the recipient, and then decrypt the message at the destination. A simple example is representing alphabets with numbers.

Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as ciphertext. In simpler terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of a cryptographic key: a set of mathematical values that both the sender and the recipient of an encrypted message agree on.
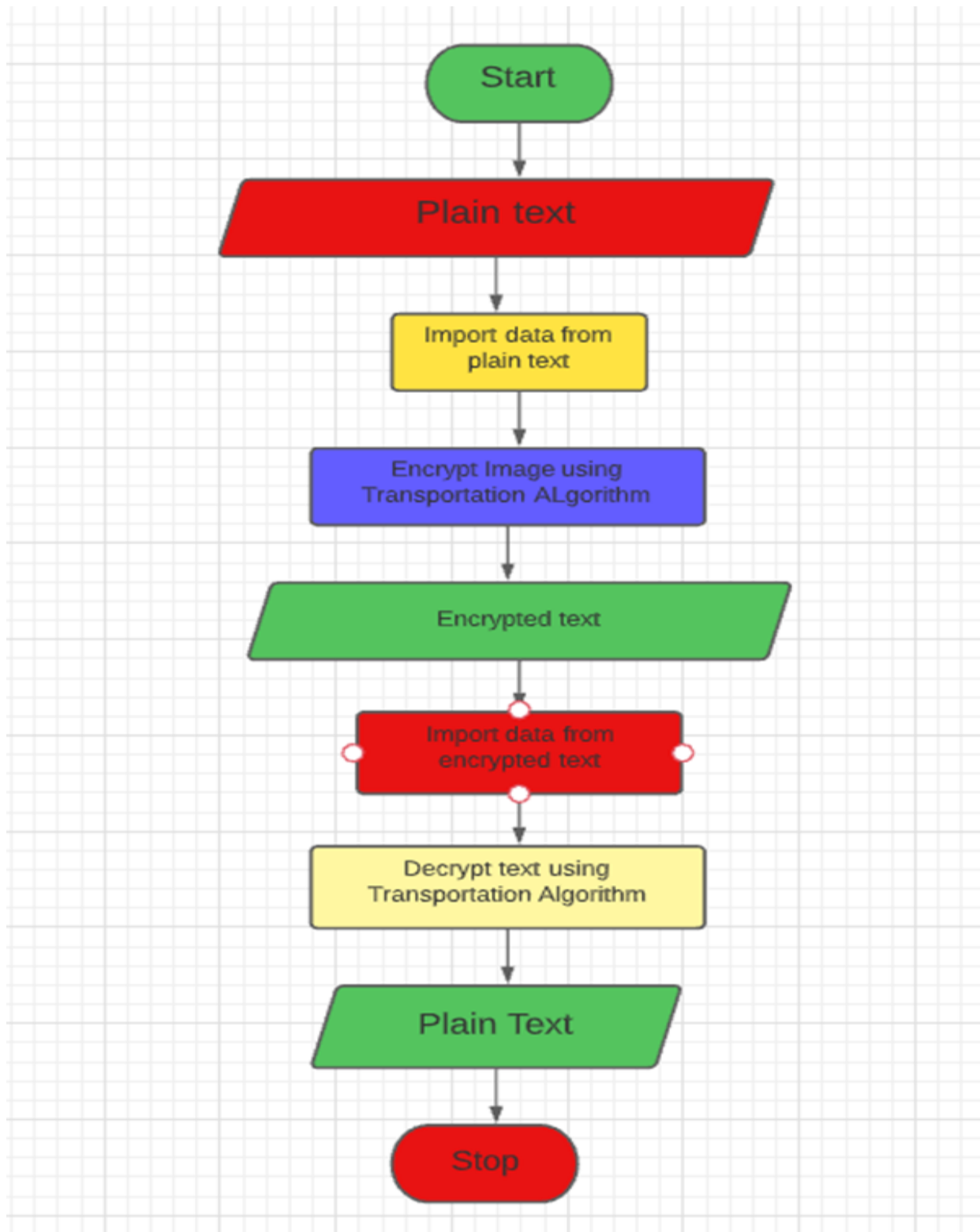
# TRANPOSITION

In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed (the plaintext is reordered). Mathematically a bijective function is used on the characters' positions to encrypt and an inverse function to decrypt.In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext.

# LITERATURE REVIEW

| ALGORITHM NAME | SUBMITTER |
|---|---|
| CAST-256 | Entrust Technologies, Inc. |
| CRYPTON | Future Systems, Inc. |
| DEAL | Richard Outerbridge, Lars Knudsen |
| DFC | CNRS - Centre National pour la Recherche Scientifique - Ecole Normale Superieure |
| E2 | NTT - Nippon Telegraph and Telephone Corporation |
| FROG | TecApro Internacional S.A. |
| HPC | Rich Schroeppel |
| LOKI97 | Lawrie Brown, Josef Pieprzyk, Jennifer Seberry |
| MAGENTA | Deutsche Telekom AG |
| MARS | IBM |
| RC 6 | RSA Laboratories |
| Rijndael | Joaen Daemen, Vincent Rijmen |
| SAFER+ | Cylink Corporation |
| Serpent | Ross Anderson, Eli Biham, Lars Knudsen |
| Twofish | Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson |

# DESIGN IMPLEMENTATION

# TECHNIQUES

TRANSPOSITION TECHNIQUES:-

1) Rail Fence Transposition

2) Columnar Transposition

## 7.1) Rail Fence Transposition: -

A rail fence cipher is a type of written code or cipher that allows its users to transform text for the purposes of encoding, using only a pencil and paper. In a rail fence cipher, letters are not changed, but only switched around regarding their positioning in the message. This type of cipher is often called a transposition cipher, because letters are simply transposed in terms of their placement. Transposition ciphers like the rail fence cipher are relatively weak forms of encoding, and can easily be broken, especially with today's technology. These types of ciphers date back to the American Civil War, where soldiers would use the code to send encrypted messages.

In a rail fence cipher, the writer takes a message and writes it into descending lines or "rails." The rail fence cipher is sometimes called a zig zag cipher if the writer uses a zigzag or W pattern to represent text.

**Plain Text:** meet me Tomorrow

Now, we will write this plain text sequence wise in a diagonal form as you can see below:

```
m   e   m   t   m   r   o
  e   t   e   o   o   r   w
```

**7.2) Columnar Transposition: -**

Columnar Transposition involves writing the plaintext out in rows, and then reading the ciphertext off in columns. In its simplest form, it is the Route Cipher where the route is to read down each column in order. For example, the plaintext "a simple transposition" with 5 columns looks like the grid below Classically ciphers that rearranged the letters of plaintext were called transposition ciphers. They can be recognized because ciphertext letter frequencies are the same as plaintext letter frequencies. Columnar transposition is probably the most commonly studied transposition cipher. We will use that method to encrypt the following "pilot's saying:"

| 3 | 1 | 4 | 2 | ← Permuted column Order |
|---|---|---|---|
| M | E | E | T |
| T | O | M | O |
| R | R | O | W |

# IMPLEMENTATION

## Code:

```python
import re
from django.shortcuts import render
import math


# Create your views here.

from django.http import HttpResponse

def index(request):
    return HttpResponse("Hello this is it...")

def encrypt(request):
    key = "HACK"

    def encryptMessage(msg):
        cipher = ""

        k_indx = 0

        msg_len = float(len(msg))
        msg_lst = list(msg)
        key_lst = sorted(list(key))

        col = len(key)

        row = int(math.ceil(msg_len / col))


        fill_null = int((row * col) - msg_len)
        msg_lst.extend('_' * fill_null)


        matrix = [msg_lst[i: i + col]
                  for i in range(0, len(msg_lst), col)]

        for _ in range(col):
            curr_idx = key.index(key_lst[k_indx])
            cipher += ''.join([row[curr_idx]
                               for row in matrix])
            k_indx += 1

        return cipher
```

## 8.1) Rail Fence Transposition Technique code:-

```python
def encrypt1(request):

    def encryptRailFence(text, key):

        rail = [['\n' for i in range(len(text))]
                for j in range(key)]
        dir_down = False
        row, col = 0, 0

        for i in range(len(text)):

            if (row == 0) or (row == key - 1):
                dir_down = not dir_down

            rail[row][col] = text[i]
            col += 1

            if dir_down:
                row += 1
            else:
                row -= 1

        result = []
        for i in range(key):
            for j in range(len(text)):
                if rail[i][j] != '\n':
                    result.append(rail[i][j])
        return ("".join(result))

    def decryptRailFence(cipher, key):

        rail = [['\n' for i in range(len(cipher))]
                for j in range(key)]

        dir_down = None
        row, col = 0, 0

        # mark the places with '*'
        for i in range(len(cipher)):
            if row == 0:
                dir_down = True
            if row == key - 1:
                dir_down = False

            rail[row][col] = '*'
            col += 1

            if dir_down:
                row += 1
            else:
                row -= 1
```
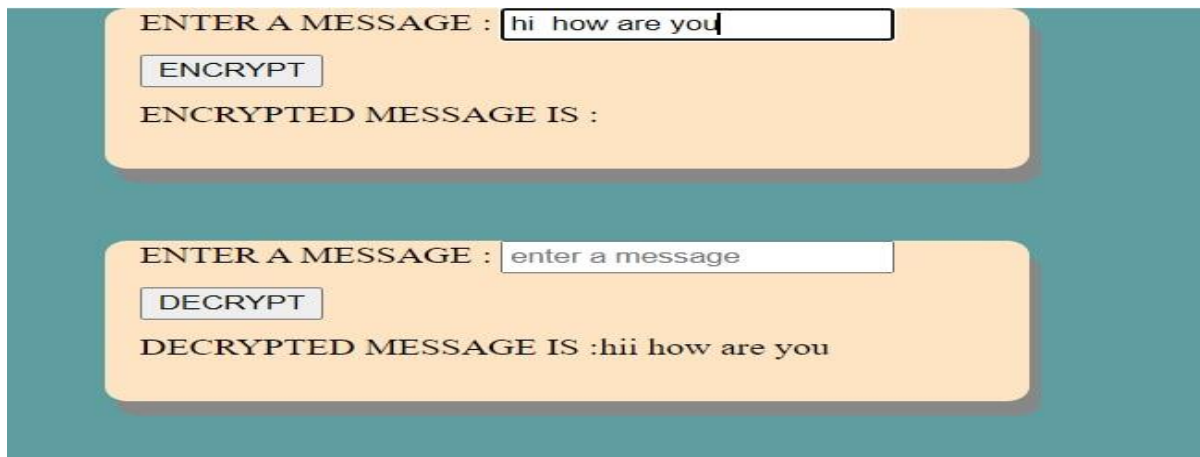
## 8.2) Columnar Transposition Technique code:-

```python
def encrypt2(request):

    def encryptColumnar(text, key):

        rail = [['\n' for i in range(len(text))]
                for j in range(key)]
        dir_down = False
        row, col = 0, 0

        for i in range(len(text)):

            if (row == 0) or (row == key - 1):
                dir_down = not dir_down

            rail[row][col] = text[i]
            col += 1

            if dir_down:
                row += 1
            else:
                row -= 1

        result = []
        for i in range(key):
            for j in range(len(text)):
                if rail[i][j] != '\n':
                    result.append(rail[i][j])
        return ("".join(result))

    def decryptColumnar(text, key):(cipher, key):

        rail = [['\n' for i in range(len(cipher))]
                for j in range(key)]

        dir_down = None
        row, col = 0, 0

        # mark the places with '*'
        for i in range(len(cipher)):
            if row == 0:
                dir_down = True
            if row == key - 1:
                dir_down = False

            rail[row][col] = '*'
            col += 1

            if dir_down:
                row += 1
            else:
                row -= 1

        # now we can construct the
        # fill the rail matrix
        index = 0
        for i in range(key):
            for j in range(len(cipher)):
                if ((rail[i][j] == '*') and
```
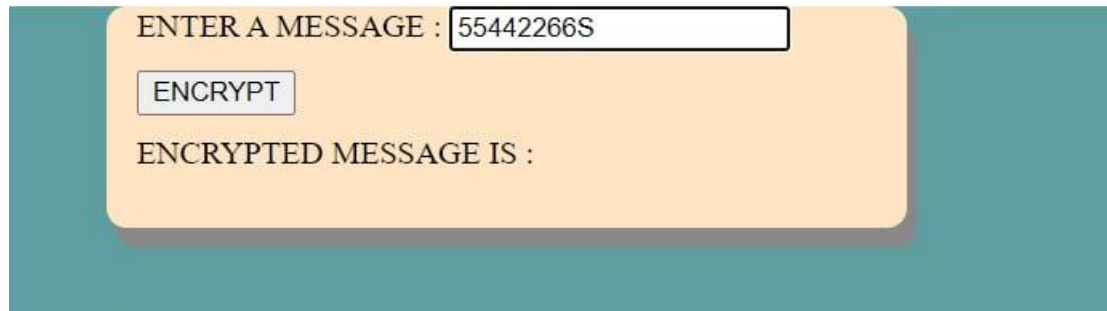
# TESTING



**FIG (9.1)**

**Here we are testing with the input given in the string format so that the encrypted message will be only in string format.**

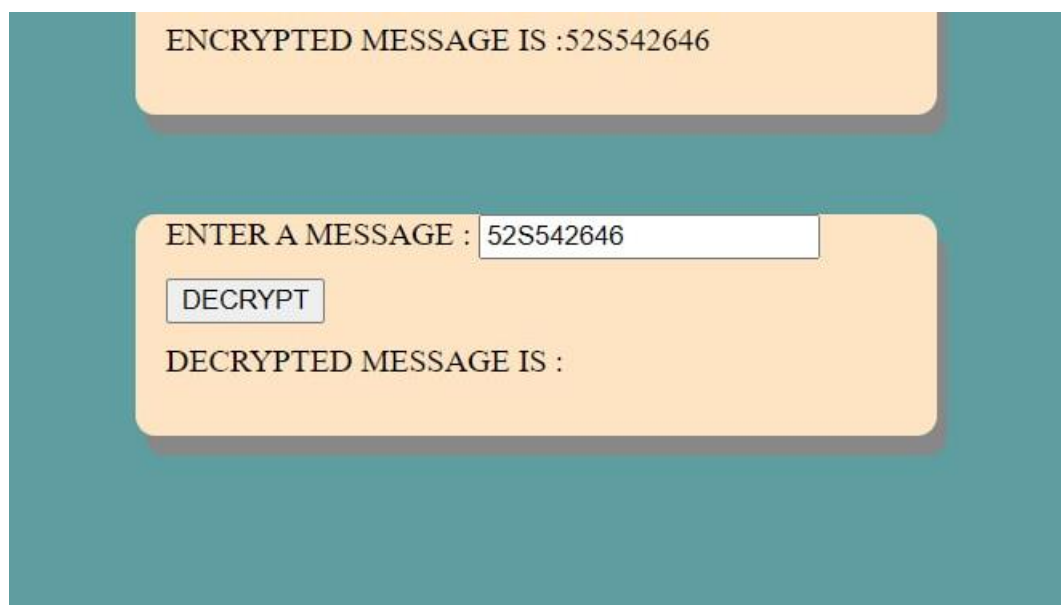**Re-entering output as input to Decrypted message to get the Real message:**



**FIG (9.2)**

**FIG (9.3)**

**Here we are testing with the input given in in string format so that the encrypted message will be only in string format.**

**Re-entering output as input to Decrypted message to get the Real message:**



**FIG (9.3)**

# RESULT



**FIG (10.1)**

**First, user will get welcome page then user will ask to click the submit button**



**FIG (10.2)**

**Then user will be redirected to encryption page where user is asked to choose one of the transportation technique to encrypt the msg.**

ENTER A MESSAGE TO ENCRYPT IT : enter a message
SUBMIT
ENCRYPTED MESSAGE IS :
ENTER A MESSAGE TO DECRYPT IT : enter a message
SUBMIT
DECRYPTED MESSAGE IS :

**FIG (10.3)**

**Then user will be redirected to encryption page of user choose encryption transportation technique where user is asked to enter  the message then user will get the encrypted cipher by entering the encrypted cipher he can get decrypted cipher nothing but the real message which was given by the user at starting to encrypt .**

ENTER A MESSAGE : enter a message
ENCRYPT
ENCRYPTED MESSAGE IS :
ENTER A MESSAGE : enter a message
DECRYPT
DECRYPTED MESSAGE IS :

**FIG (10.4)**

**Then user will be redirected to encryption page of user choose encryption transportation technique where user is asked to enter  the message then user will get the encrypted cipher by entering the encrypted cipher he can get decrypted cipher nothing but the real message which was given by the user at starting to encrypt**

# LIMITATIONS

As we can see, the rail fence cipher is being decrypted by reading it in arranging it in columns or rows before reading it. therefore, it is quite a easy and fast process, and it is less prone to mistakes. One of the problems that the rail fence cipher face is that the security of the code is dependent on the fact that a cryptanalyst does not know the method of encryption. Hence, once the method of encryption is broken, the code is broken already. Another problem with the rail fence cipher is that is not very strong. This means that the number of possible solutions are so small that a cryptanalyst can try them all by hand. Therefore, the rail fence cipher is very easy to break as we only have to test all the possible divisors up to half the length of the text.

In the case of columnar transposition, the message is addressed out in rows of a fixed length, and then put out again column by column, and the columns are chosen in any scrambled order. A keyword normally defines both the width of the rows and the permutation of the columns. In a regular columnar transposition cipher, any spare places are filled with nulls; in an irregular columnar transposition cipher, the areas are left blank. Finally, the information made off in columns in the form defined by the keyword.

# CONCLUSION & FUTURE WORK

I have presented how to improve security of Simple columnar Cipher to make it more secure and strong, and finally implement this concept in python. More over the proposed algorithm has lot of advantages in achieving secure communication than Simple One. Simple columnar transposition cipher is the simplest Transposition method. It is also the weak cipher. Its only advantage lies in the fact that it is not complex and can be understood easily. This advantage leads to the problem of easy detection. For overcoming this problem Caesar cipher and rail fence cipher is combined with transposition techniques. Transposition technique used here is simple columnar cipher. For adding further complexity stacks are used which makes the detection of both the techniques (Caesar cipher and rail fencing) are difficult.

# REFERENCES

- Jawad Ahmad Dar, "Humanizing the Security of Rail Fence Cipher Using Double Transposition Techniques, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, Volume 3 Issue 9, September 2014

- Atul Kahate (2009), Cryptography and Network Security, second edition, McGraw-Hill

- William Stalling Network Security Essentials (Applications and Standards), Pearson Education,2004

- jawad ahmad dar, Sandeep Sharma" Implementation of One Time Pad cipher with Rail Fence and Simple Columnar Transposition Cipher, for Achieving Data security, ,International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, Volume 3 Issue 11, November 2014

- jawad ahmad dar, Enhancing the data security of simple columnar transposition cipher by Caesar cipher and Rail fence cipher technique. International Journal of Computer Science & Engineering Technology (IJCSET), ISSN : 2229-3345 Vol. 5 No. 11 Nov 2014