# Classical Hybrid Technique – Substitution and Transposition Techniques

S. Kiran, PhD
Assistant Professor

G. Madhavi
Academic Consultants

D. Lakshmi Sharanya
Student IV BTech

Syed Farzana
Software Engineer

## ABSTRACT

The most important issue for every organization is nothing but security. This paper deals with the confidentiality of electronic data which is transmitted over the internet. To ensure security we are cryptography. **"Cryptography"** is the process of converting readable format of text to unreadable format of text. This is mainly used for secured communication. Many ciphers have been developed to provide security. Out of these techniques we considered five cipher techniques those are **"Caesar Cipher, Mono alphabetic Cipher, Poly alphabetic Cipher, Row Transposition Technique, and Rail fence Techniques".** The main objective of this proposed system is to combine the functionality of these five techniques to overcome the disadvantages of these techniques and to form a new hybrid technique named as **"Classical Hybrid Encryption Substitution and Transposition Techniques"** which can provide a good security when compared to techniques.

This method uses two stages of encryption. In the first stage Substitution techniques – Mono alphabetic, Caesar cipher, poly alphabetic cipher are used to generate partial cipher text. The key for Caesar cipher and poly alphabetic technique is generated randomly by using Multiplicative linear congruential generator (Random number generation technique). In the second stage of Encryption Technique Transposition methods – Row Transposition and Rail fence Techniques are used to generate final cipher text.

This algorithm provides 91! Of key space and in addition of that this encryption technique is multistage with each stage uses different key. Through this technique we will achieve good security against Brute-Force Attack and Cryptanalysis.

## Keywords

Cryptography, C, Decryption, Ciphers, Multiplicative linear Congruential Generator, Key space, Brute-Force Attack, Cryptanalysis

## 1. INTRODUCTION

### 1.1 Why do we need cryptography

The satiations that arised to implement the cryptography wants privacy or security to protect the information. The main areas such as ecommerce, politics, government actions, financial transaction needs implementation of cryptography techniques.

### 1.2 Cryptography

The information must be in unrecognized format whie in transmissiom only authenticated one able to convert the information from unrecognized format to recognized format. This is known as decryption. Some times there may be breaking of code as done in modern cryptography by intruders to make it as unbreakable modern mechanisms are needed. As electronic media utilization is increasing security becomes more precious to protect the data. The cryptography systems classified as two types

1. Symmetric
2. Asymmetric

1. Symmetric : It's a public key cryptography only one key is used for convertion of data from recognize to unrecognize and viceversa

2. Asymmetric: in this two keys are involved to convert the data from recognize to unrecognize and viceversa. It is essential to maintain third party for potential communication in cryptography. There exists four aspects to protect the information such as confidential, integrity, authentication and nonrepudation. A concept of security is used in multi disciplines such as mathematics, electrical engineering applications, electronic commerce etc. In modern age their exists effective encryption techniques which converts information from readable state to nonreadable state. The receiver must know decipher technique then only appropriate message has been received.

## 2. SYSTEM ANALYSIS:

### 2.1.Existing system

The project "improved Caesar cipher with random number generation with multistage encryption" aims to provide good security against Brute-force attack and cryptanalysis by increasing the key space, generating the key randomly and using multistage encryption.

**Disadvantages of existing system:**

- Plaintext of length is not multiple 25 cannot be encrypted.
- Spaces and lines are not considered while Encryption
- It needs to memorize some intermediate results of the encryption technique for the decryption other than the key
- Same key is used for Caesar cipher technique for whole text

### 2.2. Proposed system

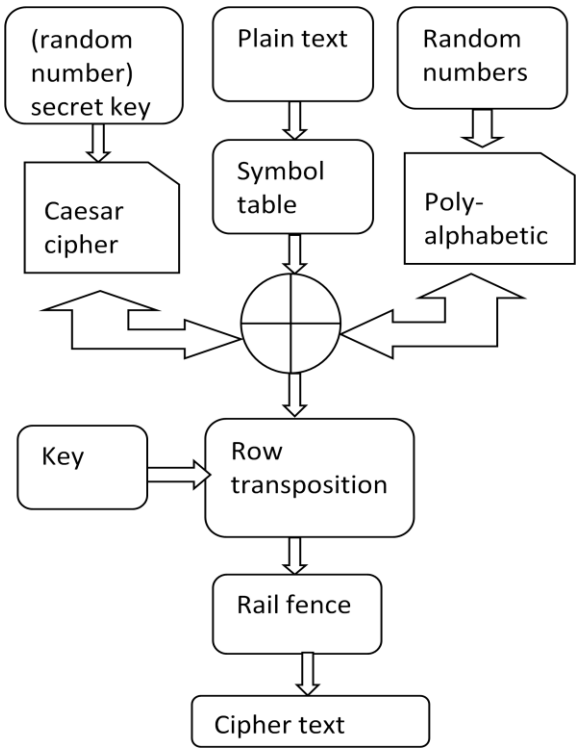
The proposed system **"classical hybrid Encryption-Substitution and Transposition Techniques"** is the combination of some substitution and transposition techniques. This proposed system inherits functionality of existing system.

**Advantages of proposed system:**

- This handle text of any length
- There is mechanism to remember appearance of spaces and lines.

- There is no need to remember the intermediate results of the encryption technique for the decryption process
- Different keys are generated for each set of 25 characters of the plain text in the first stage of encryption technique.

## 2.3.Block Diagram Of Encryption Algorithm




## 2.4.Encryption algorithm

1. Read the plain text message
2. Replace the plaintext characters by their corresponding values in symbol table
3. Generate a secrete key using random number generation technique, by multiplicative Linear congruential generators Xn=KXn-1 +1 mod n
4. Arrange the secret key generated in step3, into matrix from order I X J
5. Obtain the Trace of the random number matrix
6. SECRET KEY VALUE=(Trace of random matrix)mod 91
7. Add this secret key (Caesar cipher) and random matrix (polyalphabetic cipher) to the plain text numerical matrix and mod with 91.
8. Applying Row Transposition technique by using key 0,1,2,3,4 values permutations for matrix obtained in step6
9. Take the output of step 8, replacing the values by characters using symbol table and perform the rail fence technique
10. By using symbol " ? " append the lines and spaces to the encrypted text
10. Transmit the cipher text

## 2.5.Algorithm description and illustration:

This proposed method can be applied o encrypt, plain text message all alphabets, numbers and symbols which are in keyboard. The below character have been assigned to character to the values.

Totally, 91 characters are below

## 2.6.Symbol Table

| CHARACTER | VALUE |
|---|---|
| + | 0 |
| - | 1 |
| * | 2 |
| / | 3 |
| 0 | 4 |
| 1 | 5 |
| 2 | 6 |
| 3 | 7 |
| 4 | 8 |
| 5 | 9 |
| 6 | 10 |
| 7 | 11 |
| | |
| 8 | 12 |
| 9 | 13 |
| [ | 14 |
| ] | 15 |
| { | 16 |
| } | 17 |
| \ | 18 |
| : | 19 |
| ; | 20 |
| ‘ | 21 |
| , | 22 |
| . | 23 |

| | |
|---|---|
| ! | 24 |
| # | 25 |
| $ | 26 |
| % | 27 |
| ^ | 28 |
| & | 29 |
| - | 30 |
| A | 31 |
| B | 32 |
| C | 33 |
| D | 34 |
| E | 35 |
| F | 36 |
| G | 37 |
| H | 38 |
| I | 39 |
| J | 40 |
| K | 41 |
| L | 42 |
| M | 43 |
| N | 44 |
| O | 45 |
| P | 46 |
| Q | 47 |
| R | 48 |
| S | 49 |
| T | 50 |
| U | 51 |
| V | 52 |
| W | 53 |
| X | 54 |

| | |
|---|---|
| Y | 55 |
| Z | 56 |
| A | 57 |
| B | 58 |
| C | 59 |
| D | 60 |
| E | 61 |
| F | 62 |
| G | 63 |
| H | 64 |
| I | 65 |
| J | 66 |
| K | 67 |
| L | 68 |
| M | 69 |
| N | 70 |
| O | 71 |
| P | 72 |
| Q | 73 |
| R | 74 |
| S | 75 |
| T | 76 |
| U | 77 |
| V | 78 |
| W | 79 |
| X | 80 |
| Y | 81 |
| Z | 82 |
| ‘ | 83 |
| \| | 84 |
| @ | 85 |

| | |
|---|---|
| ( | 86 |
| ) | 87 |
| < | 88 |
| = | 89 |
| > | 90 |

**Figure 5.3.1 Symbol table**

Encryption operation is expressed as:

C=E(P)=(P+K)mod 91

"K" can take any value in the range of 0 to 91

Decryption operation is expressed as:

P=D(c)=(c-k) mod 91

"k" can take any value in the range of 0 to 91

Algorithm Illustration,

Consider a plain text message which is to be encrypted using the proposed algorithm

"I Love India"

Now replace each character of the plain text with corresponding value in symbol table values.

Replace characters with numerical values: I=65,L=68, o=45,v=52,e=35, I=65, n =44, d=35, i=39, a=31, X=80, X=80, X=80, X=80, X=80, X=80, X=80, X=80, X=80, X=80, X=80, X=80, X=80, X=80.

80 80 80 80 80

$$\begin{pmatrix} 65 & 68 & 45 & 52 & 35 \\ 65 & 44 & 34 & 39 & 31 \\ 80 & 80 & 80 & 80 & 80 \\ 80 & 80 & 80 & 80 & 80 \end{pmatrix}$$

Now to encrypt the plain text, generate the key using random number generation technique using recursive equation.

Consider Multiplicative Linear Congruential Generation(LCGs):

Xn=a*Xn-1 mod p

Multiplicative Linear Congruential Generator, a prime number is need and primitive root of the modulus p is need. Prime – number should be greater than the plaintext length, because for generating random numbers and avoid repetitions of numbers

Let prime number (p)=31

Least primitive root (a)=3

Xn=3Xn-1 mod 31

This is the equation for key generation using random number generation technique.

Let the seed value be Xo=1

Xn=a*Xn-1 mod p

Here a=primitive root, p=prime number.

X1=3*1 mod 31=3

X2=3*3 mod 31=9

X3=3*9 mod 31=27

:

:

X24=3*11 mod 31=2

Considering the 25 random numbers and arranging them in 5 X 5 matrix form, we get

Random Numbers:

01 03 09 27 19 26 16 17 20 29 25 13 08 24 10 30 28 22 04 12 05 15 14 11 02

$$\begin{pmatrix} 01 & 03 & 09 & 27 & 19 \\ 26 & 16 & 17 & 20 & 29 \\ 25 & 13 & 08 & 24 & 10 \\ 30 & 28 & 22 & 04 & 12 \\ 05 & 15 & 14 & 11 & 02 \end{pmatrix}$$

The key required performing Caesar encryption is derived from the random number matrix as:

Key =[Trace of random number matrix 5 X 5] mod 91

Trace of above matrix = Sum of diagonals mod 91 =[01+16+08+04+02] mod 91= 31 mod 91= 31

The plain text Message considered for encryption is 'I Love India"

The matrix from of the numerical values of the above plain text Message is represented below

$$\begin{pmatrix} 65 & 68 & 45 & 52 & 35 \\ 65 & 44 & 34 & 39 & 31 \\ 80 & 80 & 80 & 80 & 80 \\ 80 & 80 & 80 & 80 & 80 \\ 80 & 80 & 80 & 80 & 80 \end{pmatrix}$$

Perform the Caesar substitution encryption using secret key and random number of element in the matrix, adding to the plain text.

| | | | | |
|---|---|---|---|---|
| 65+31+01 | 68+31+09 | 45+31+09 | 52+31+27 | 35+31+19 |
| 65+31+26 | 44+31+16 | 34+31+17 | 39+31+20 | 31+31+29 |
| 80+31+25 | 80+31+13 | 80+31+08 | 80+31+24 | 80+31+10 mod 91 |
| 80+31+30 | 80+31+28 | 80+31+22 | 80+31+04 | 80+31+12 |
| 80+31+05 | 80+31+15 | 80+31+14 | 80+31+11 | 80+31+02 |

After performing above process,

| | | | | |
|---|---|---|---|---|
| 06 | 11 | 85 | 19 | 85 |
| 31 | 0 | 82 | 90 | 0 |
| 45 | 33 | 28 | 44 | 30 |
| 80 | 48 | 42 | 24 | 32 |
| 25 | 35 | 38 | 31 | 22 |

Now performing Columnar Transposition on the above matrix in a random order of C4, C3, C2, C1, C0

Reading the above matrix in the sequential of row

C= 85 00 30 32 22 19 90 44 24 31 85 82 28 42 38 11 00 33 48 35 06 31 45 50 25

Now replacing the values by characters in symbol table,

@+-b,:>n!a@Z^1h7+cre2aot#

Applying rail fence to that text,

@-,>!@^h+r2o#+b:naZ17ceat

Now append the Lines and spaces to the above (partially cipher text),spaces and lines are indicated by symbol "?", first lines are encrypted and then spaces

@-,>!@^h+r2o#+b:naZ17ceat??-0

The final cipher text message is:

Cipher text C=@-,>!@^h+r2o#+b:naZ17ceat??-0

## 2.7.Block Diagram Of Decryption Algorithm

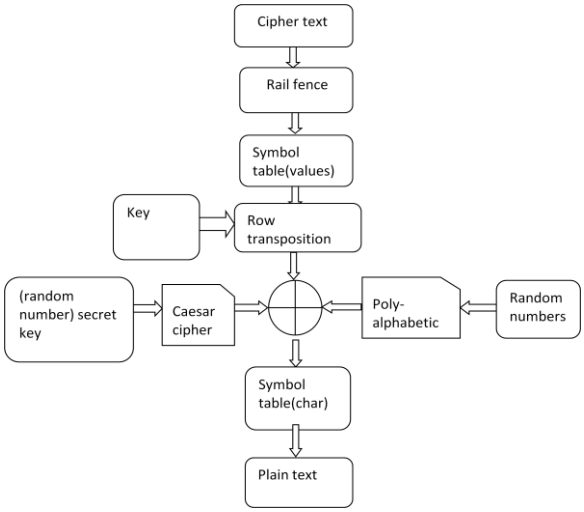



**Figure 5.4. Block Diagram Of Decryption Algorithm**

### *2.7.1 Decryption Algorithm:*

1. Read the cipher text without spaces and lines
2. Divide the text into two rows,

First row=(Total text /2)+1

Remaining text as second row

3. Perform reverse Rail fence Technique
4. By using symbol table replace characters by numerical values & perform Row Transposition in reverse by using symmetric key
5. Perform reverse of

Caesar cipher, poly alphabetic Cipher for matrix values and mod with 91

6. A matrix is obtained, replace the values by characters by using symbol table
7. Place the matrix in sequence of rows
8. Until all cipher text not processed go to step1

Insert spaces and lines into text

After applying decryption algorithm:

Plain text P= I Love India(with padding)

## 3. CONCLUSION

Security is an significant aspect in communication. It is essential to consider throughput and memory needs in case of design of unreadable formats. The modern ciphers are included to provide effective security along with classical ciphers. The key must be truly random to increase the confusion unreadable information. This proposed system combined the functionalities of the techniques namely Caesar cipher, mono alphabetic, poly alphabetic, row transposition and rail fence. The system can be further improved by using modular arithmetic and exponential mathematical operations. The proposed method provides high throughput and occupies less memory.

## 4. REFERENCES

[1] S.G. Srikantaswamy, H.D.Phaneendra-NIT-"Improved Caesar cipher with Random number generation technique and multistage encryption"- International Journal on Cryptography and information Security IJCIS, vol.2, No.4, December 2012.

[2] A.F.A.Abidin, O.Y. Chuan and M.R.K. Ariffin- "A Novel enhancement Technique of the Hill Cipher for effective Cryptographic Purposes '- Journal of Computer science, 7(5):785-789, 2011

[3] Dharmendra Kumar Gupta, Submit Kumar Srivastava, Vedpal Singh- "New concept of encryption algorithm. A hybrid approach of Caesar Cipher and Columnar transposition in multi stages "-Journal of Global Research in Computer Science, Volume 3, No.1 , January 2012, P.No.60-66.

[4] Fauzan Saeed, Mustafa Rashid- "Integrating Classical Encryption with Modern Tehnique"- IJCSNS, Volume10, No. 5, May 2010

[5] Prof.K.Govinda, Dr.E. sathiyamoorth – "Multileve l Cryptography Technique using Graceful codes" – JGRCS, Volume 2, No.7, July 2011

[6] Monodeep Banerjee, Saptarshi Naskar,krishnendu Basuli, Samar Sen Sarma –"A novel scheme for text data encryption "-JGRCS, volume 3, no.1, January 2012

[7] Phillip I Wilson and Mario Garcia –"A Modified Version of the vigenere Algorithm "- IJCSNS, Vol.6, No.3B, march 2006

[8] Packirisamy Murali and Gandhi doss Senthil Kumar-"Modified Version of Playfair cipher using Linear feedback Shift Register "-IJCSNS, vol.8, No.12, December 2008