International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cryptography with Different Techniques

Kirandeep Kaur

Assistant Professor, Global Group of Institutes

Abstract:
Cryptography is a field to solve the problems related to Information Security. There are numerous techniques like substitution and transposition methods to convert the real message into secret code which will be tough for intruder to understand .These techniques change the position or substitute intelligible message characters to produce the ciphertext which is more secure to transfer as compare to plaintext. Columnar Technique is also such technique which changes the position of plaintext message characters and produces the ciphertext. In this research paper, improved columnar technique is presented which will produce more randomness in the ciphertext generated to make it difficult for cryptanalyst to predict the plaintext from it.

Keywords: Cryptography, Information Security, Rail Fence Technique, Transposition Techniques, Enhanced Algorithm

INTRODUCTION

Cryptography:

Cryptography is a field to secure information over the network. It is ever growing field to improve already existing techniques to increase the confidentiality and privacy of the data of the sender. Encryption and Decryption Algorithms are deployed on the sender and receiver respectively to maintain the privacy of the important information on the network [10].

Encryption and decryption:

Encryption-The encryption algorithms are used to convert the plaintext into ciphertext. Plaintext is the intelligible text which could be read by the user ad understood by them, whereas ciphertext is the converted message with the help of an encryption algorithm received by the receiver in more secured form[1][5].

FIGURE 1. ENCRYPTION AND DECRYPTION ALGORITHM

Types of Encryption Algorithms [2]

1. Substitution Techniques
2. Transposition Techniques
3. Rotor Machines
4. Steganography

In this paper, only Transposition Technique is touched in depth.

Transposition Techniques:

In transposition techniques, position of characters of plaintext changes making it more difficult for intruder to break the code. Rail Fence technique and Columnar Transposition Techniques are such techniques [6] [7].

The example of **Rail Fence Technique** is following:

The plain text (message) like: "I have arranged a meeting today" characters are placed alternatively in two different rows and repositioned to form ciphertext like this:

Plaintext:

I ae rag d m e i g oa

h v a r n e a e t n t d y

Converted **ciphertext** will be:

"I a e r a g d m e ig o a h v a r n e a e t n t d y"

The more complex example of Transposition Technique represented in Table 1.

TABLE1. AN EXAMPLE OF COLUMNAR TRANSPOSITION TECHNIQUE

3	2	4	1
i	h	a	v
e	a	r	r
a	n	g	e
d	a	m	e
e	t	i	n
g	t	o	d
a	y	x	x

Where x is the filler used at the end of the table to just fill the complete matrix. The ciphertext will be like "vreendxhanattyieadegaargmiox" where 3421 is the key to reposition the plaintext that is arranged in a matrix above. The ciphertext is generated by writing the data column wise according to the key i.e.3421 [3].The security issue related to this technique is that intruder can rearrange the data to guess the message by just knowing the key,as the key is an important factor in maintaining the security of this algorithm. The objective of the research is also same. It can be made tough for cryptanalyst to guess it if we will convert this simple method into some complex method [8].

A MORE ENHANCED COLUMNAR TRANSPOSITION TECHNIQUE Encryption Process:

In this method, we will perform the initial procedure same as Columnar Transposition Technique. We will rearrange the data arranged in matrix according to some key k (as described in above example).Let the number of columns be 'n'. The digits of key 'k' are added to each other to generate sum i.e 's' .The sum 's' will be divided by the number of columns 'n' in a matrix.

The remainder is stored in variable 'r'.

r= (s) mod n

Then the remainder 'r' will be added to every digit of key 'k' and the result is stored in key t1 with the help of the following equation:

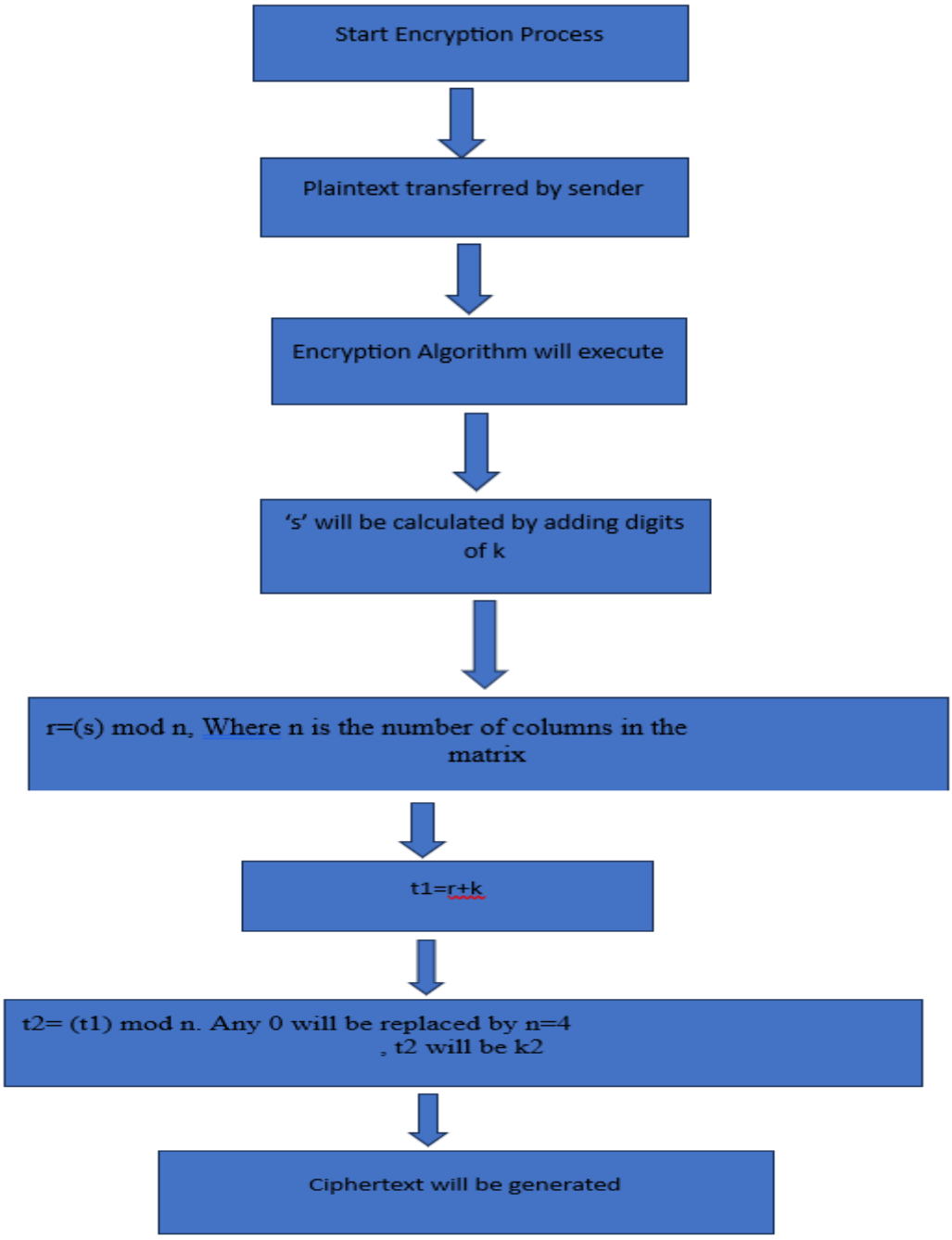
t1i=r + (ki)

Where 'i' ranges from 1 to n and describes the position of the digit in key 'k'.The next equation will be

t2i= (t1i) mod n

Where if t2i will have value zero it needs to be replaced by the number of columns. This complete procedure will generate the second key from first key with help of which further transposition can happen. Figure 2 represents flow chart of Enhanced Transposition Technique.

FIGURE 2 FLOW CHART OF ENHANCED TRANSPOSITION



For Example:

Let the key 'k' be 3241.The sum of key's digits will be 10(3+2+4+1). So, 's' will be 10.

Divide it by the number of columns of the matrix i.e. n=4. The remainder will be 2, 'r' will be 2 according to the equation r=s (mod n).Now, calculating **t1i=r + ki**

t14=2+3=5,

t13=2+2=4,

t12=2+4=6,

t11=1+2=3

Therefore, t1=5463.

Now to put t1 into the range of 'n', calculation of t2 will be done.

Further calculating t2 by equation**t2i=t1imod n**

t24=5mod4=1,

t23=4mod4=0,

t22=(6)mod4=2,

t21=(3)mod4=3;

Therefore, **t2=1023.**

The problem arises here is the number '0' which appeared in the t2.k2 will be t2i by replacing 0 with the number of columns i.e. n=4.

k2=1423

k2 will be another key with which we can do transposition of our already transposed plaintext.

For Example: The above example consider in section 1will be transposed again with the help of the k2.The text generated after the transposition of the plaintext with key 3241 was "vreendxhanattyieadegaargmiox". Again transpose this text with the help of k2 which is generated with the help of enhanced transposition technique. Table 2 represent an example of enhanced columnar technique.

TABLE 2: AN EXAMPLE OF ENHANCED COLUMNAR TECHNIQUE

1	4	2	3
v	r	e	e
n	d	x	h
a	n	a	t
t	y	i	e
a	d	e	g
a	a	r	g
m	i	o	x

The final ciphertext with the help of key k2 will be:"vnataamexaieroehteggxrdnydai". This is final ciphertext achieved by double transposition with two keys where second key is also attained from the first key through above defined procedure.

Decryption Process:

Now decryption process has to be done at the receiver side because the receiver needs to know what the sender intends to say. *Decryption process* will be reverse of the encryption process [4]. Figure 3 represent the Flow chart of Decryption Process.

The k2 is 1423 as described above. We have to sum the digits of k2 with number of columns i.e n='4'.

t3i=k2i+n;

t3i=k2i+4;

The intermediary result will be 't3' which is 5867.The t3's digits should be added to each other, which will result in s1 and then be divided by number of columns in the matrix i.e.

'n'=4 .The sum 's1' will be 5+8+6+7=26.Another variable, r1 will be calculated from s1 with the help of following equation:

r1= (s1) mod n

r1= (26) mod 4=2

The result will be 2 i.e. r1=2.The t3i will be subtracted from r1

t4i=t3i-r1

t44=5-2=3;

t43=8-2=6;

t42=6-2=4;

t41=7-2=5;

Which will result in (5867-2=3645).

t5 will be final key with the help of the following equation:

t5i= (t4i) mod n

t54=3 mod4=3;

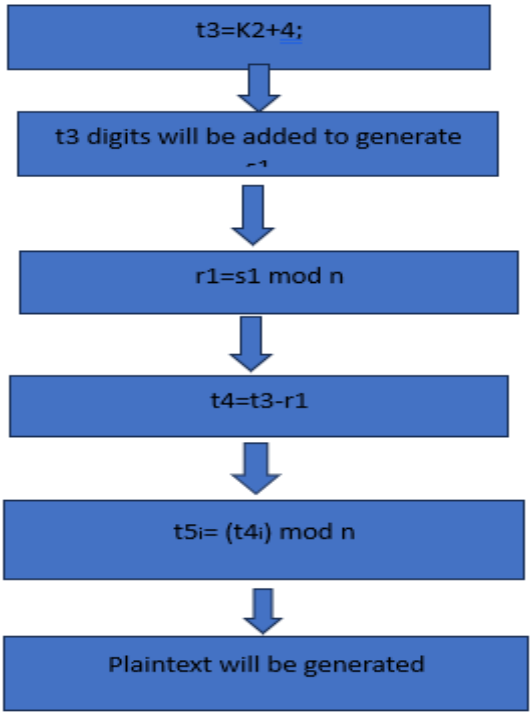
t53=6 mod4=2;

t52=4mod 4=0; [0 should be replaced by n]

t51=5mod4=1;

It will result in initial key i.e.3241.The ciphertext should be rearranged with the help of k2 and t5 to generate the plaintext again.

FIGURE 3: FLOW CHART OF DECRYPTION PROCESS



Analysis:

Simple Columnar Technique can be easy for an intruder to decrypt the message [9]. By using dual key for this technique the security will enhance. The data will be encrypted or shifted with two different keys. The randomness characteristics in encrypted text will be key feature in enhancing the security of plaintext. The method will protect the encrypted message from brute force attack as the number of tries will be more to decrypt the data. Table 3 compare the both methods simple and enhanced columnar techniques.

TABLE 3: COMPARISON BETWEEN SIMPLE COLUMNAR TECHNIQUE & ENHANCED COLUMNAR TECHNIQUE

Factors to lookout	**Enhanced Columnar Technique**	**Simple Columnar Technique**
No. of rounds of Transposition	2	1
No of Keys	2	1
Randomness in result	more	less
Decryption	simole	complex
Time taken for Encryption	more	less
Susceptibility to Insecurity	less	more

Conclusion:

This method is another step in improving already existing transposition techniques. More number of keys used will bring randomness in the ciphertext generated. This, in turn, will make it tough for intruder to decrypt the ciphertext generated and extract the plaintext from it. The Algorithm will not generate any randomness in the original key if 'r' (the modulus calculated in r=(s) mod n) will be zero.

ACKNOWLEDGMENT

The authors wish to thank the Global Group of Institutes, Amritsar for their support and Motivation

REFERENCES

1. S. M. Naser, "Cryptography: from the ancient history to now, its applications and a new complete numerical model" International Journal of Mathematics and Statistics Studies 2021
2. Mr. Ashwini Seth; Sachin S Bhosle "Research paper on Cyber Security", Researchgate 2021.
3. Cryptography and Network Security" by William Stallings, Fourth Edition.
4. Abdalbasit Mohammed Qadir; NurhayatVarol"A Review Paper on Cryptography" IEEE, June 2019.
5. Anjula Gupta, Navpreet Kaur Walia "Cryptography Algorithms: A Review" IJEDR, Volume 2 Issue 2, 2014.
6. Khairun Nahar, Partha Chakraborty **"**Improved Approach of Rail Fence for Enhancing Security" International Journal of Innovative Technology and Exploring `1 Engineering 9(9):583-585, July 2020.
7. Dr. Sumathy Kingslin, R.Saranya "Evaluative Study on Substitution and Transposition Ciphers" 8 IJCRT Volume 6, Issue 1, January 2018.
8. Rihartanto Rihartanto; Supriadi Supriadi; Didi Susilo Budi Utomo "Image Tiling Using Columnar Transposition"IEEEXplore,11 April 2019.

9. Ashwin Ramesh "Enhancing the Security of Hill Cipher using Columnar Transposition" IJERT Volume 4 Issue 7 July 2015.
10. T. Rajani Devi "Importance of Cryptography in Network Security" IEEEXplore, 10 June 2013.