IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

Rail Fence Cipher Based Encryption Technique For Secure Data Transfer

Debolina Dalui[1], Sudipta Sahana[2]*

[1,2]Dept. of Computer Science and Engineering, JIS College of Engineering, Kalyani, India 741235

*Corresponding Author: ss.jisce@gmail.com, Tel.: +91 9474733974

DOI: https://doi.org/10.26438/ijcse/v7i4.910914 | Available online at: www.ijcseonline.org

Accepted: 16/Apr/2019, Published: 30/Apr/2019

***Abstract*—** Network security has become one of the major talking points in today's technological world. Although several research activities were carried out pertaining to security in order to ensure confidentiality, authenticity, integrity, non-repudiation etc., there remained some loopholes which need to be taken care of. There are chances that cyber attackers or hackers may tamper or alter the texts and cause a severe leakage of confidential information of IT organizations, business firms, etc. Hence, it is of utmost importance to protect vital information from such attackers or hackers by using some standard techniques. In our paper, we have discussed the cryptographic techniques with proper encryption and decryption. We have suggested the use of Rail Fencing Cypher along with ASCII codes and mapping tables for end to end encryption of plain text comprising of several characters and then decrypting the encrypted text into plain text.

***Keywords*—** Cryptography, Rail Fence Cipher, Mapping, Encryption, Decryption

I. INTRODUCTION

The practice and study of techniques for secure communication in the presence of third parties for hackers is termed as cryptography. In other words, it is the process of conversion of plain text into encrypted text, popularly known as cipher text and then decrypt in the cipher text into plain text is termed as cryptography. Cryptography is mainly done in order to achieve data confidentiality, data integrity, authentication and non-repudiation. There are two types of cryptography which are Asymmetric key cryptography and symmetric key cryptography.

Symmetric key cryptography uses the same cryptographic key for both encryption of plain text and decryption of cipher text. Asymmetric key cryptography uses pairs of keys which are public key and private key. This type of cryptography uses two different keys for encryption of plain text and decryption of cipher text.

The Rail Fence cypher is a kind of transposition cypher where the plain text can be represented in a zig zag manner and then rearranged. Hence, the total pattern can be changed by this technique. In this technique successive rails on an imaginary fence is used to write the plaintext downwards and then moving up when we reached the bottom. Then we can read the message in rows.

Mapping tables are constructed for both encryption and decryption. In encryption it consists of no from 0 to 37 and their corresponding symbols and in decryption different symbols are represented in the form of no's starting from 0 to 37. In our case the mapping table is required to represent the octal value as two-bit words and vice versa.

In this paper, we have discussed the cryptographic techniques with proper encryption and decryption. We have suggested the use of Rail Fencing Cypher along with ASCII codes and mapping tables for end to end encryption of plain text comprising of several characters and then decrypting the encrypted text into plain text.

The rest of the paper discusses about the following aspects of an effective encryption technique using the rail fence cipher. Section 2 of this paper discusses about the research works which carried out related to secure data transfer using various kinds of encryption techniques. Section 3 talks about the complete algorithm to achieve the same along with a well-defined example and flow chart. The results obtained from the algorithm and their comparison with traditional approaches along with well-defined graphical representation for both proposed approach and traditional approach are all discussed in section 4 in this paper. The conclusion of this paper along with further scope of research on this field are all discussed in section 5 in this paper.

II. RELATED WORK

In paper [1] a new and more sophisticated way of combining steganography with cryptography was introduced so that the whole system became more compact and safer for any kind of vital message transfer. The concept of Archimedean spirals was used in the cryptography part, where the initial

private key determined the width of the spiral, and it was according to the length of the message to be sent. The initial private key was sent by the sender to the receiver using some modes of transmission After it, the encrypted text was embedded into some kind of graphics image and then the stego object was sent to the receiver. The receiving end could decrypt the message just by knowing the actual pixel values and the initial key. This technique was considered to be more safer and sound as there was a usage of two steps of protection.

Sudipta Sahana et al. [2] proposed a data hiding system which was grounded on audio steganography and cryptography for authenticated data transfer. The audio medium used here was the steganographic medium. The encryption and decryption methods of cryptography used in developing this system make the surety of the proposed system more efficient in securing the data from unauthorized access. Therefore, there was a recommendation of this system to be used by the internet users for finding a more safe and secure system. An audio medium was also used as the steganographic and an advanced algorithm was applied for encoding the private data into the audio file. The main objective was to combine both cryptography and steganography for the purpose of developing a better and credible communication in this insecure open network.

In paper [3] a data is encrypted using matrix and Elliptic Curves and the concept of steganography was used by hiding the generated points of the encrypted data in an image. A hybrid model was proposed with the help of public key based Elliptical Curve Cryptography (ECC) and image Steganography which provided more security than a Single ECC or Steganography methods alone. The objective of the proposed work was to archive better encryption for all types of data and the robustness of this work was well evident of the output stego images. The main objective was to help users from different community to transfer crucial information securely who were using public network for communication.

In paper [4] there was an introduction of one of the most powerful cryptographic techniques namely AES. Here confidentiality, authenticity, integrity, non-repudiation and other issues of security of communication in the present world, were discussed.

Prof. Mukund R. Joshi et al. [5] studied cryptography along with its principles. There was description of cryptographic systems with ciphers. The cryptographic models and algorithms are outlined**.**

In paper [6] a cryptographic algorithm was proposed based on techniques like Rail fencing cipher and substitution, which accomplished the goal of security. The proposed algorithm made use of proper encryption and decryption methods and security was achieved at its best possible way.

The objective of paper [7] was to allow the intended recipients of a message to receive the message properly while interrupt eaves-droppers from understanding the Message. A survey was also provided to data security problem through cryptography technique. A set of techniques were included in cryptography for the strive or pretence data so that there was availability of these techniques to someone who could recover the data to its original form.

In paper [8] the plain text was change to cipher text by making use of cryptographic method, where individuals could be able to use their desirable key for encrypting the text and there was use of some Boolean algebraic operation and then there was suppression of this cipher text inside a cover media of 2n X 2n dimension grey scale image. there was a suggestion of a secure pictorial block steganography grounded encryption algorithm for transporting message and exposing the steganalysis and cryptanalysis technique for retrieving data at receiver side. The investigational result specified that for using altered length of message text, distortion of picture was too much less which was negligible in open eyes.

III. METHODOLOGY

In this section we have proposed our encryption & decryption algorithm [**Fig 1**].

A. Encryption algorithm:

Step 1: Take a string as input from the sender
Step 2: Perform the Rail fence cipher
Step 3: Swap the positions of MSB and LSB in the string
Step 4: Convert each character of the string to its corresponding ASCII value and its octal value
Step 5: Take first 2 bits of the octal number together and the last bit alone
Step 6: From the mapping table, we replace the first 2 bits and the last bit with their corresponding symbols.

Step 7: Taking the symbols of all octal numbers from left to right

B. Decryption algorithm:

Step1: Take the encrypted value as an input
Step 2: Divide the cypher text into pairs and consider each pair as a group.
Step3: Match the letters from the mapping table for decryption
Step 4: Convert the octal numbers to their corresponding ASCII values and characters
Step 5: Swap the positions of MSB and LSB in the string
Step 6: perform backtracking of rail fence cipher.

Step 7: Hence the encrypted string can be decrypted into the plain text.

MAPPING TABLE FOR ENCRYPTION:

0	1	2	3	4	5	6	7	8	9	10	11	12
&	o	p	q	r	s	t	u	v	w	x	y	z

14	15	16	17	18	19	20	21	22	23	24	25	26
m	l	k	j	i	h	g	f	e	d	c	b	a

27	28	29	30	31	32	33	34	35	36	37
+	_	*	/	=	>	<	^	%	#	$

MAPPING TABLE FOR DECRYPTION:

&	o	p	q	r	s	t	u	v	w	x	y	z	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13

m	l	k	j	i	h	g	f	e	d	c	b	a
14	15	16	17	18	19	20	21	22	23	24	25	26

+	_	*	/	=	>	<	^	%	#	$
27	28	29	30	31	32	33	34	35	36	37

FLOWCHART FOR ENCRYPTION:

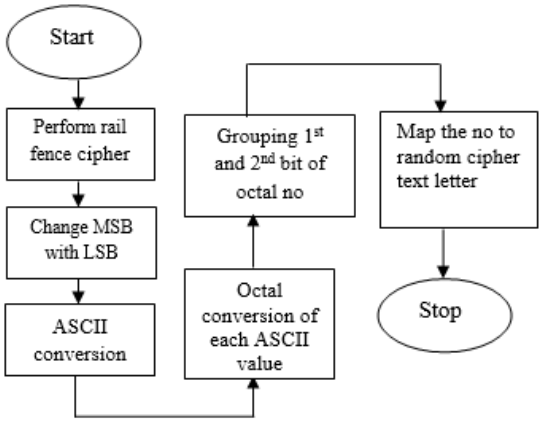


Fig 1: flow chart of our algorithm

Example:

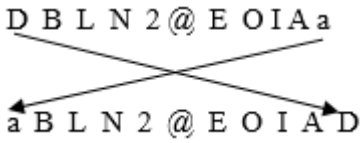
Encryption

Step 1: Consider a string to be "DEBOLINA2a@"

Step 2: Perform the Rail Fence Cipher

So, the string becomes DBLN2@EOIAa

Step 3: Swap the positions of MSB and LSB in the string



So, the new string is a B L N 2 @ E O I A D

Step 4: Convert each character of the string to its corresponding ASCII value and its octal value

Character	ASCII	Octal
a	97	141
B	66	102
L	76	114
N	78	116
2	50	062
@	64	100
E	69	105
O	79	117
I	73	111
A	65	101
D	68	104

Step 5: Take first 2 bits of the octal number together and the last bit alone

Example when we take the octal value 141 we take 14 and 1

Then we design a mapping table for all the numbers starting from 0 to 37

Step 6: From the mapping table, we replace the first 2 bits and the last bit with their corresponding symbols.

For example, for octal value 141, 14 should be replaced by m and the last bit, i.e. 1 should be replaced by o. Hence, 141 is replaced by mo.

141	102	114	116	062	100	105	117	111	101	104
mo	xp	yr	yt	tp	x&	xs	yu	yo	xo	xr

Step 7: Taking the symbols of all octal numbers from left to right, the final cypher text or encrypted text for the string DEBOLINA2a@ becomes moxpyryttpx&xsyuyoxoxr

Decryption:

Step1: Take the cypher text or encrypted value as an input

moxpyryttpx&xsyuyoxoxr

Step 2: Divide the cypher text into pairs and consider each pair as a group.

mo xp yr yt tp x& xs yu yo xo xr

Step3: Match the letters from the mapping table for decryption

mo	141
xp	102
yr	114
yt	116
tp	062
x&	100
xs	105
yu	117
yo	111
xo	101
xr	104

Step 4: Convert the octal numbers to their corresponding ASCII values and characters

Octal	ASCII	Character
141	97	a
102	66	B
114	76	L
116	78	N
062	50	2
100	64	@
105	69	E
117	79	O
111	73	I
101	65	A
104	68	D

The string now becomes aBLN2@EOIAD

Step 5: Swap the positions of MSB and LSB in the string

Step 6: arrange the resultant string in the pattern as shown below

D		B		L		N		2		@
	E		O		I		A		a	

So, the plain text is DEBOLINA2a@

IV. RESULTS AND DISCUSSION

In this paper we have made use of some techniques such as Rail Fencing Cipher, mapping table along with ASCII values and Octal values. Besides achieving an efficient and effective an end to end encryption of plain text into cipher text and then decrypting the cipher text into plain text, our proposed approach gives a significant improvement in performance in terms of efficiency, throughput and response time as compare to traditional approach. Below is the diagram (*Fig 2:*) which shows that the efficiency of our proposed approach will increase with the increasing number of characters.

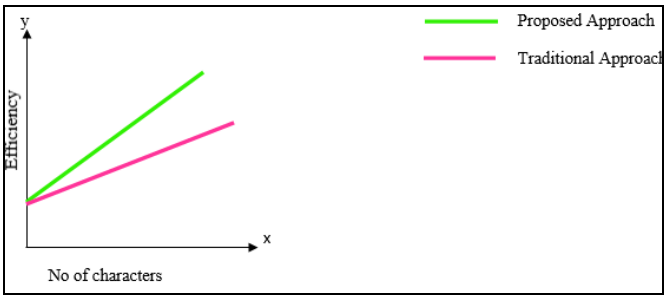


Fig 2: Comparing the proposed approach with the traditional approach showing the efficiency will increase with increasing number of characters

Below is the diagram (*Fig 3:*) which shows that the throughput of our proposed approach will increase with the increasing number of characters

Fig 3: Comparing the proposed approach with the traditional approach showing the efficiency will increase with increasing number of characters.

The response time of our proposed approach will vary with the increasing number of characters as shown below (*Fig 4:*).

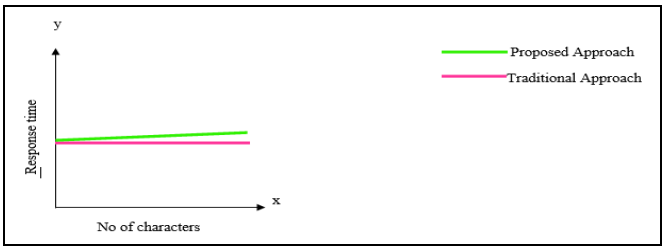


Fig 4: Comparing the proposed approach with the traditional approach showing the response time will get reduced with increasing number of characters.

V. CONCLUSION AND FUTURE SCOPE

Although the different techniques applied in ensuring the security of confidential data of IT organizations, business firms provide confidentiality, integrity, authenticity, non-repudiation, they differ in terms of providing better efficiency, throughput etc. An effective cryptographic technique meets these two parameters, which are throughput and efficiency. In our paper, we have used the logic of Rail Fencing Cypher, mapping table etc. along with ASCII values and mapping table. We sincerely believe that the techniques we have used, besides providing an effective security, will help us in achieving high degree of performance in terms of providing better throughput and better efficiency.

ACKNOWLEDGMENT

Authors are grateful towards JIS College of Engineering for providing lab and related facilities to conduct the research.

REFERENCES

[1] Sudipta Sahana, Asmita Bhattacharya, Rittik Mondal, Rohan Chattopadhaya, Titas Das, "*SECURING AND HIDING TEXTS USING ARCHIMEDEAN SPIRAL TECHNIQUE WITH IMAGE STEGANOGRAPHY*", International Journal of Computer Engineering and Applications, Volume IX, Issue IV, ISSN 2321-3469

[2] Sudipta Sahana, Goutami Dey, Madhurhita Ganguly, Priyankar Paul, Subhayan Paul, "*Adaptive Steganography Based Enhanced Cipher HidingTechnique for Secure Data Transfer*", IOSR Journal of Computer Engineering (IOSR-JCE)e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. V, PP 55-60

[3] Sudipta Sahana, Madhusree Majumdar, Shiladitya Bose, Anay Ghoshal, "*Security Enhancement Approach For Data Transfer Using Elliptic Curve Cryptography And Image Steganography*", International Journal of Advanced Research in Computer and Communication EngineeringVol. 4, Issue 4, April 2015

[4] Sarita Kumari, "*A research Paper on Cryptography Encryption and Compression Techniques*", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 6 Issue 4 April 2017, Page No. 20915-20919

[5] Prof. Mukund R. Joshi, Renuka Avinash Karkade , "*Network Security with Cryptography*", International Journal of Computer Science and Mobile Computing, Vol.4 Issue.1, January- 2015, ISSN 2320–088X

[6] Ujjwal Barman, Suchismita Gupta, Sudipta Sahana, "Substitution Technique Based Noble Approach Towards Base64 Crypting System Incorporating Rail Fence Cipher", CCET JOURNAL OF SCIENCE AND ENGINEERING EDUCATIONCCET JOURNAL OF SCIENCE AND ENGINEERING EDUCATION, Vol. - 3, Page-60-65, Year-2018, ISSN 2455-5061

[7] Prof. Swapnil Chaudhari, Mangesh Pahade, Sahil Bhat, Chetan Jadhav, Tejaswini Sawant, "A Research Paper on New Hybrid Cryptography Algorithm", INTERNATIONAL JOURNAL FOR RESEARCH & DEVELOPMENT IN TECHNOLOGY, Volume-9,Issue-5(May-18) ISSN (O) :- 2349-3585

[8] Abhipsa Kundu, Sudipta Sahana, "*Dynamic Size Based Cipher Aided Image Steganography Technique for Network Security Enhancement*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 10, October 2014, ISSN: 2277 128X

Authors Profile

Sudipta Sahana is an assistant professor of a renowned engineering college of west Bengal. More than 4 years he has worked in this region. He has passed his MTech degree in Software Engineering and B.Tech Degree in Information Technology from west Bengal university of technology with a great CGPA/DGPA on 2010 and 2012 respectively. He is recently working in Ph.D. on the domain of "cloud computing". He is a member of the Computer Science Teachers Association (CSTA), Computer Society of India (CSI) and also a member of International Association of Computer Science and Information Technology (IACSIT).

Debolina Dalui is a 2nd year student, pursuing Master of Technology in the department of Computer Science and Engineering, from a renowned engineering college of West Bengal .Engineering and B.Tech Degree in Computer Science and Engineering from west Bengal university of technology with a great CGPA/DGPA on 2016.

