International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-9, July 2020

Improved Approach of Rail Fence for Enhancing Security

Khairun Nahar, Partha Chakraborty

Abstract*: In the era of a global village, a huge amount of people are connected to the web through their PC, mobile and any type of communication tool for communication purposes, hence we require a safe approach that provides security and protection from unauthorized clients and misuses of data and information. Cryptography is a widespread technique to guarantee security for the internet-based communication framework. Many cipher technique have developed but the rail Fence is the simplest and amusing cryptographic algorithm until now. In this technique, the plain text is organized as crosswise and read it from top to the bottom row produces the cipher text. An inadequate quantity of keys is its weakness. This paper redesigned the current rail fence by applying the three basic phases: substitution phase once and transposition phases uses twice. The proposed technique ensures that the resultant cipher text is a fusion of various symbols precise by a chart. The proposed algorithm eliminates the limitation of the existing algorithm and significantly improves the performance by transforming the plain text unrecognizable and unpredictable.

Keywords: Cryptography, Rail fence, Transposition cipher, Cipher techniques.

I. INTRODUCTION

Cryptography renovates the sender's message into an unrecognizable presentation to hide the explanation to the unapproved individuals and only the desired persons can decode it applying exact cryptographic technique and key. In cryptography, the original message is marked as 'plain text' and 'cipher text' after the encryption. The outsider who tries to decode is professed as a cryptanalyst and the procedure itself called cryptanalysis [6]. A cryptographic mechanism and a key are important for any cryptographic algorithm. Four key principles of every cryptographic algorithm are: Integrity, Authentication, Non-repudiation and Confidentiality [7]. Every cryptographic approach is divided into two categories: substitution cipher and transposition cipher. Each character of the plain text is subbed by various characters or symbols in the substitution cipher. The transposition cipher performs combinations and permutations. Once more, every cryptographic algorithm is characterized based on the key: symmetric key and asymmetric key. Symmetric key and asymmetric key utilizes a solitary key and a couple of keys.

Revised Manuscript Received on July 30, 2020.
* Correspondence Author
Khairun Nahar*, Department of CSE, Comilla University, Cumilla, Bangladesh. E-mail: knahareva@gmail.com
Partha Chakraborty*, Department of CSE, Comilla University, Cumilla, Bangladesh. E-mail: partha.chak@cou.ac.bd

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

Rail fence is a symmetric key cryptographic algorithm that employs the transposition cipher method. In this approach, the plain text should be written as a chain of diagonals. The resultant cipher text will be generated after reading it row by rows [7]. Consider the following things:
Input: Plain text: **Rail Fence** Key-Value: **3**
Output: Cipher text: **R calFneie**.

For encryption, create a matrix. Here, the key value is 3 (no. of rows) and the sender's message contains 10 characters calculating the space character (no. of columns), so the dimensions of the matrix will be 3 × 10. Here, 1st row covers 3 characters: R, ,c (Space character is included), the 2nd row covers 5 characters: a, l, F, n, e and the 3rd and final row covers 2 characters: i, e. The cipher characters after reading row by row will be: R, (space) , c, a, l, F, n, e, i, e.

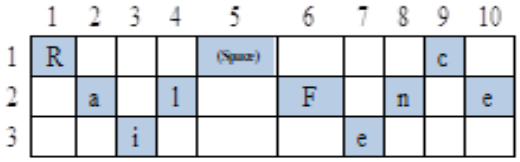

Fig. 1. Rail Fence Encryption Process.

In cryptography, two types of circular shift operations are used: Circular left shift and circular right shift to permute the bit sequence [9]. For example: consider the sequence ***11011*** for a circular shift of 2-bit position.

Fig. 2. Snap shot of Circular Left Shift/Circular Right Shift.

II. RELATED WORK

Umang Bhargaval et al., (2017) proposed a new algorithm that combines two techniques: Transposition and substitution. The proposed algorithm passes through three phases. Substitution (Multiplication cipher) technique is applied to the first phase. The output of the first phase is followed by transposition (Rail fence) technique. The cipher text (output of 2nd phase) is then substituted by symbol produces the output [1].
Akash et al., (2017) presented A.J.Cipher, uses more than one encryption method. It uses substitution (vigenere cipher) cipher in first stage.

The output of first stage along with key is converted to ASCII-to-binary and performed XOR operation. The output of this stage converted back to binary-to-ASCII. The ASCII equivalent character is final output [2].

Andysah Putera et al., (2016) redesigned the rail fence and proposed that the leading letter of the message will be occupied in the lowermost left corner of the matrix and then run corner to corner upwards by placing the remaining letters. Then read the characters from the top to bottom row. This generates output message [3].

N. Abitha et al., (2015) proposed a new cryptographic approach for maintaining privacy. They modified cipher: Rail fence and Vigenere cipher for data mining and applied it for encrypting the bank account number [4].

Baljit Saini (2015) presented algorithm uses substitution cipher (Modified Ceasar) and transposition cipher (Rail Fence). It uses modified ceasar technique in first stage and rail fence is the last stage [5].

III. PROPOSED METHOD

A. Description of the Modified Rail Fence Approach

The existing rail fence encodes the plain text by disposing of space, number, and symbols. Space, digit, symbol are not the piece of this encryption. It works pitiable for short message. The reason behind this is inadequate keys. Proposed algorithm conquers the above restriction by engaging itself with three distinct phases:

Phase 1: Substitution: Represent the Plain text by the special symbol.

Phase 2: Transposition: Circular Shift.

Phase3: Transposition: Rail Fence.

B. Procedure for Encryption

Step 1: Read the plain text (PT).

Step 2: Take a random integer for a key (K).

Step 3: Rrepresents each character by the special symbol indicated by the following chart:

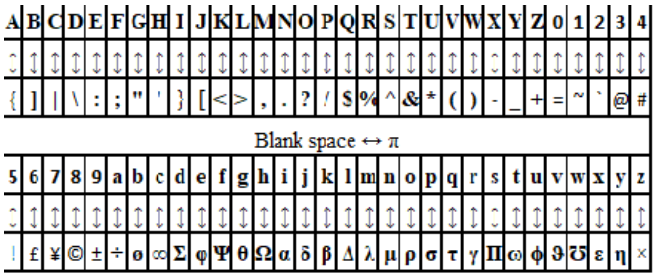

Fig.3. Substitution Chart (Character-to-symbol and Symbol-to-character).

Step 4: If the key value is even/odd performs the circular left shift/circular right shift operation by K positions. Here K denotes the key-value.

Step 5: The resultant message of the previous steps is written as a chain of diagonals/ zigzag sequence.

Step 6: Final step, read it row by rows to produce the output cipher text (C).

Step 7: End

C. Procedure for Decryption

Step 1: Input: Key (K) and the Cipher (C).

Step 2: Build a matrix for decryption. Key-value (total rows) and size of cipher text (total columns) will be the dimensions of the matrix. The leading letter will be occupied in the uppermost left corner of the matrix and then runs corner to corner downwards by placing a dash (-), later these dashes (-) will be replaced by the remaining cipher letters. Then coming back to the top row, the next character of the cipher will be placed. Carry on this within the row and jump to the subsequent row until we arrive at the end. Then we read it diagonally [8].

Step 3: Performs the circular shift operation (circular right shift/circular left shift) by K positions based on the key-value (even/odd).

Step 4: Each symbol of the text obtained from step 3 will be replaced by letters based on the Fig.3.

Step 5: After replacing each character brings back the desired plain text (PT).

Step 6: Stop

IV. EXPERIMENTAL RESULTS AND DISCUSSION

EXAMPLE 1

PLAIN TEXT (PT): Rail Fence

KEY: 2 (EVEN)

Table I. Encryption process for an even key

Step 1	Input: Plain text (PT).	Rail Fence
Step 2	Input: Key (K).	2 (Even)
Step 3	Represent the Plain text (PT) by a special symbol	R a i l F e n c e % ÷ Δ π ; φ μ ∞ φ
Step 4	Perform a circular left shift by 2 positions. Because the key is even.	Before: % ÷ α Δ π ; φ μ ∞ φ After: α Δ π ; φ μ ∞ φ % ÷
Step 5	Create Zigzag sequence	α π φ ∞ % Δ ; μ φ ÷
Step 6	Read it row by rows	Read 1st row: απφ∞% Read 2nd row: Δ;μφ÷
Step 7	Cipher text (C)	απφ∞%Δ;μφ÷

Table II. Decryption process for an even key

Step 1	Input: Cipher text (C)	απφ∞%Δ;μφ÷
Step 2	Input: Key (K).	2 (Even)
Step 3	Create Diagonal matrix and read the cipher character diagonally.	α π φ ∞ % Δ ; μ φ ÷

Step 4	Perform circular right shift by 2 positions. Because key is even.	Before: α Δ π ; φ μ ∞ φ % ÷ / After: % ÷ α Δ π ; φ μ ∞ φ
Step 5	Replace symbol by Character.	% ÷ α Δ π ; φ μ ∞ φ / R a i l F e n c e
Step 6	Plain Text (PT)	Rail Fence

EXAMPLE 2

PLAIN TEXT (PT): Rail Fence
KEY: 3 (ODD)

Table III. Encryption process for an odd key

Step 1	Input: Plain text (PT).	Rail Fence
Step 2	Input: Key (K).	3 (Odd)
Step 3	Represent the Plain text (PT) by a special symbol	R a i l F e n c e / % ÷ α Δ π ; φ μ ∞ φ
Step 4	Perform a circular right shift by 3 positions. Because the key is odd.	Before: % ÷ α Δ π ; φ μ ∞ φ / After: μ ∞ φ % ÷ α Δ π ; φ
Step 5	Create Zigzag sequence	μ ÷ ; / ∞ % α π φ / φ Δ
Step 6	Read it row by rows	Read 1st row: μ÷; Read 2nd row: ∞%απφ Read 3rd row: φΔ
Step 7	Cipher text (C)	μ÷;∞%απφφΔ

Table IV. Decryption process for an odd key

Step 1	Input: Cipher text (C)	μ÷;∞%απφφΔ
Step 2	Input: Key (K).	3 (Odd)
Step 3	Create Diagonal matrix and read the cipher character diagonally.	μ ÷ ; / ∞ % α π φ / φ Δ
Step 4	Perform a circular left shift by 3 positions. Because the key is odd.	Before: μ ∞ φ % ÷ α Δ π ; φ / After: % ÷ α Δ π ; φ μ ∞ φ
Step 5	Replace symbol by Character	% ÷ α Δ π ; φ μ ∞ φ / R a i l F e n c e
Step 6	Plain Text (PT)	Rail Fence

Below us shows that our proposed algorithm works excellent even for a short message.

Table V. Simulation result for short message

PLAIN TEXT (PT)	KEY (K)	RAIL FENCE	PROPOSED ALGORITHM OF MODIFIED RAIL FENCE
Rail Fence	2	Ri ecalFne	απφ∞%Δ;μφ÷
	3	R calFneie	μ÷;∞%απφφΔ
	4	ReaFni cle	π%;φ÷φ∞αμΔ
	5	RcaneielF	μ;∞πφφΔ%α÷
	6	Raeicln eF	φμ;∞πφΔ%α÷

V. CONCLUSION

Earlier we mentioned the weakness of the traditional rail fence algorithm. Then, we proposed our method to overcome all these weakness and increased it strength by applying more than one encryption phase. It is free from brute force attacks and impossible to crack a message decoded by the proposed method using frequency analysis. We observed that the proposed algorithm works best for long messages as well as short messages.

This paper presented the text encryption process. In the future, we will work on the encryption process of the audio, image and video file using this proposed algorithm.

REFERENCES

1. Umang Bhargava and Raghav Chawla, "A New Algorithm Combining Substitution & Transposition Cipher Techniques for Secure Communication," in International Conference on Trends in Electronics and Informatics (ICEI 2017), Tirunelveli, India, 2017, pp. 619-624.
2. Jitendra Kumar Soni and Jitendra Kumar Soni Aakash, "A.J.CIPHER," in 2nd International Conference on Telecommunication and Networks (TEL-NET 2017), Noida, India, 2017.
3. Andysah Putera and Utama Siahaan, "Rail Fence Cryptography in Securing Information," International Journal of Scientific & Engineering Research, vol. 7, no. 7, pp. 535-538, 2016.
4. N.Abitha, G Sarada, G.Manikandan, and Sairam.N, "A Cryptographic Approach for Achieving Privacy in Data Mining," in International Conference on Circuit, Power and Computing Technologies [ICCPCT], Nagercoil, India, 2015.
5. Baljit Saini, "Modified Ceaser Cipher and Rail fence Technique to Enhance Security," International Journal of Trend in Research and Development, vol. 2, no. 5, pp. 348-350, September 2015.
6. Khairun Nahar and Partha Chakraborty, "A Modified Version of Vigenere Cipher using 95 × 95 Table," International Journal of Engineering and Advanced Technology (IJEAT), vol. 9, no. 5, pp. 1144-1148, June 2020.
7. Atul Kahate, Cryptography and Network Security, 3rd ed. New Delhi: Tata McGraw-Hill Education, 2013.
8. Rail Fence Cipher - Crypto Corner. [Online]. Available https://crypto.interactive-maths.com/rail-fence-cipher.html.. [Accessed 28 June, 2020]
9. Circular shift- Wikipedia. [Online]. Available https://en.wikipedia.org/wiki/Circular_shift. [Accessed 28 June, 2020].

AUTHORS PROFILE

Khairun Nahar is now employed as a Lecturer in the CSE Department of Comilla University, Cumilla, Bangladesh. She holds her B.Sc (Engg.) and M.Sc (Engg.) degree from Comilla University. She is currently doing research on Information Security, NLP and Machine Learning.

Partha Chakraborty received his BSc and MSc degree in Computer Science and Engineering from Jahangirnagar University, Savar, Dhaka, Bangladesh. He began his teaching career as a Lecturer, Department of CSE in Comilla University and now he is an Assistant Professor in this department. He is actively engaged in various research activities and educational activities. He published a good number of research articles as well as attends various conferences. His research area includes Machine Learning, Artificial Intellegence, Computer Vision, Robotics, Image Processing and Human Robot Interaction.