International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 07 | July 2021 www.irjet.net p-ISSN: 2395-0072

A New Variant of Rail Fence Cipher using Hybrid Block-Swap Method

A. Ashok Kumar[1], S. Kiran[2,*], R. Pradeep Kumar Reddy[2], Sandeep Reddy Devara[2]

[1]Department of Physics, YSR Engineering College of YVU, Proddatur-516360, Andhra Pradesh, India
[2]Department of CSE, YSR Engineering College of YVU, Proddatur-516360, Andhra Pradesh, India

---

Abstract - *Transferring the data securely over any medium needs to concentrate on the three important principles of information which are Confidentiality, Authenticity, and Integrity. A high level of security can be achieved with various algorithms based on various cryptographic principles. Cryptography can be defined as a technique that develops ciphertext, based on specific algorithms that make the data unreadable unless decrypted by algorithms that are predefined by the sender. A rail fence cipher is a form of transposition cipher which is also referred to as a zig-zag cipher. It comes under symmetric key algorithms where the same key is used for both encryption and decryption. In this paper, the author modified the traditional rail fence cipher and fixed the key size as two. The Hybrid Block-Swap Rail Fence Algorithm gives the best randomness in the cipher. The key used in this technique is 64-bit random alpha-numeric characters. In the proposed method, the plain text is divided into blocks and each block consists of four characters, and the characters in the block are represented as 2*2 matrix representation. The position of the characters in every block is swapped internally. Then rail fence technique is applied along with an Exclusive-OR (XOR) operation is performed between the generated result after swapping with the random 64-bit key. The ciphertext generated in the traditional rail fence will be in the range of the plain text only. The limitation of the formation of the ciphertext overcame with the proposed technique. Every character of the ciphertext generated using this proposed algorithm will be in the range of 0 – 127 ASCII values.*

***Key Words*: cipher, confidentiality, authenticity, integrity, encryption, decryption, rail fence, transposition.**

1. INTRODUCTION

From the last few decades, the usage of the internet has evolved drastically. Everything became digital like shopping, money transfer from bank accounts, using social media accounts, ticket booking, etc., where whatever the data i.e., stored or requested is not in the same form as given, it is encrypted because to provide security and it is an automated process [1, 2]. So, this made security a basic need for digital data transmission. Since communication has become a part of life for all age groups, because of this massive data is traveling day-by-day over the world, through the internet [2, 3]. The security of data became an important aspect during the transmission of data over any digital mode [3]. It becomes vulnerable to unauthorized access by hackers or illegitimate users. The receiver should obtain the information which maintains its confidentiality, integrity, and authenticity [4, 1, 2].

- Confidentiality means information that is transferred should be only accessed by authorized users.
- Integrity means information i.e., transferred should be complete and should not be altered by the hackers/attackers.
- Authenticity ensures that only the authorized users can involve in communication.

Cryptography provides the technique to maintain all the three characteristics that are mentioned above in data transmission [5, 3]. The technique involves converting plain text into an unreadable format using mathematical applications and in addition, the technique can also convert any unreadable data into the readable format without knowing the sender information [6, 4].

2. RAIL FENCE CIPHER

Rail Fence Cipher is a cryptographic algorithm that comes under the transposition kind of cipher, and it is also known as zig-zag cipher [1]. The mechanism in this algorithm is that it jumbles up the position of the characters of the message. Every character of the plain text is arranged diagonally from top to bottom. Once the bottom rail is reached the characters are arranged from bottom to top with a sharp edge at the bottom. This pattern is repeated until every character of the plain text gets written on the rails. After arranging the characters in this way, the characters are read from left to right from each rail one by one, starting from the topmost rails. For instance, if we want to encrypt the message "COMPUTER SCIENCE DEPARTMENT" with 5 rails, then this text must be arranged in the order as shown in fig. 1. The selection of the number of rails used in this technique is known as the key. The same number of rails is used in both encryption and decryption.

Rail 1	C							–						–							E			
Rail 2		O					R		S					E		D					M		N	
Rail 3			M				E				C				C				E				T			T
Rail 4				P		T						I		N						P		R				
Rail 5					U								E								A					

Fig. 1 Encryption of message though rail fence cipher

After the arrangement, the characters are read line by line from left to right to get the ciphertext. It is evident from fig. 1, the encrypted message formed is 'C--EORSEDMNMECCETTPTINPRUEA'. It is to be noted that if the number of rails is greater than the number of characters in the message, then no encryption mechanism occurs. If the number of rails is lesser then the characters of the ciphertext are placed closer to their actual position, which would make

it easier for the attackers to guess the plain text, hence the number of rails should be chosen accordingly. One of the problems with rail fence cipher is that it would be easier if the cryptanalyst identifies the encryption method and then the cipher would be broken easily. Further, with the trial-and-error method, the key would be found easily [7]. Another problem with the rail fence cipher is that it is not strong. This means that the number of possible solutions is so small that a cryptanalyst can try them all by hand. This makes the rail fence cipher easy to break as we must test all the possible divisors up to half the length of the text [8]. Therefore, a new hybrid method is proposed using a rail fence cipher called the substitution block-swap rail fence cipher to increase its security.

3. RAIL FENCE

The algorithm requires two inputs from the user the first input is the plain text, and the second input is the no of rails (key) used to encrypt and decrypt the message and the ciphertext, respectively. The key value must be greater than or equal to two. This feature makes the proposed algorithm popular in the transformation of plain text or messages in a wiser way. Every character of the plain text is arranged diagonally from top to bottom on each rail once you reach the bottom rail and the characters are arranged from bottom to top with a sharp edge at the bottom. This pattern is repeated until every character of the plain text gets written on the rails [9, 1, 5]. For instance, the key is 2 and the plain text is 'PRODDATUR' it will be represented as shown in fig. 2.

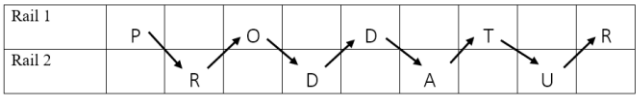


Fig 2 division of plain text using rails

The representation of plain text shown in the above fig 2 is in a zig-zag pattern so that is `why it is called a zig-zag cipher [1, 6]. The encrypted text or ciphertext is reading the characters from left to right and in a top-down manner one rail at a time till the completion of all rails [3]. With the increase in the number of rails, the difficulty of breaking the cipher also increases. So, it is suggested to use a greater number of rails for encrypting the plain text as the same number of rails is used for the decryption mechanism [10].

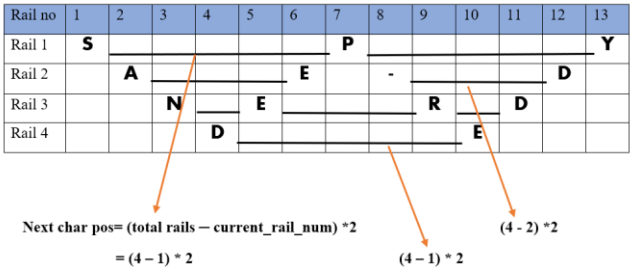


Fig. 3. calculation of the position of the next character in the rail fence ciphertext.

The position of the next character in the ciphertext depends on the total number of rails, current rail number, and even or odd character in that corresponding rail [5]. It is observed from fig. 3 that a slight variation in finding the position of the next character in the first and last rail as all the characters are placed at equidistant in these two rails when compared to other rails [4]. It is observed that sharp edges are encountered in the first and last rail so, they differ from the other rails.

First and Last Rail:

The position of the next char is: (total rails – 1) * 2

Eg:

- If the position of the present character is at 7th in the first rail the total number of rails is 4 then the position of the next character is: 7+(4-1) * 2 = 7+3*2 = 7+6 = 13
- The next character of the ciphertext occurs at position number: 13

Eg:

- If the position of the present character is at 4th in the last rail the total number of rails is 4 then the position of the next character is: 4+(4-1) * 2 = 4+3*2 = 4+6 = 10
- The next character of the ciphertext occurs at position number: 10

Remaining rails (other than first & Last):

If the next character even counts, then:

Position of next character = (total rails - current_rail_num) *2

Eg:

- If the present character is the 1st character in rail 3 at position: 3
- Total number of rails is: 4 then the position of next character is: 3+(4-3) * 2 = 3+1*2 = 3+2 = 5
- The next character of the ciphertext occurs at position number: 5

If the next character is odd count, then:

Position of next character=(current_rail_num - 1) *2

Eg:

- If the present character is the 2nd character in rail 3 at position: 5
- Total number of rails is: 4 then the position of next character is: 5+(3-1) * 2 = 5+2*2 = 5+4 = 9
- The next character of the ciphertext occurs at position number: 9

Similarly, all the characters of the plain text are to be processed to generate the ciphertext. Only one character is to be processed at a time. The Ciphertext formed after processing all the characters of the Plain text (SANDEEP REDDY) and the produced key (number of rails=4) is **'SPYAE DNERDDE'**.

4. A HYBRID BLOCK-SWAP RAIL FENCE ALGORITHM

The proposed Hybrid Block-Swap Rail Fence Algorithm is an extension of the Rail Fence Algorithm. In this method, the rail Fence algorithm along with Exclusive-OR (XOR) operation is performed with the key and internal swapping in blocks. If the length of plain text is not an integral multiple of 32-bits, then padding for plain text is required. The padding is done with the character 'Z' because the usage of this character would be less when compared with the other

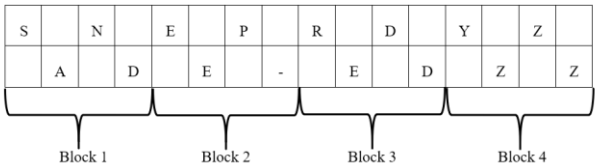
characters [1, 6]. The length of the plain text after padding must be an exact multiple of 32-bits. The hybrid algorithm is explained with an example containing two rails. Considering four characters from which two characters are chosen from each rail in sequential order as one block. Exchanging the mean position characters and extreme position characters respectively only one block is chosen at a time and then performing the rail fence technique with the resulting plain text i.e., formed after swapping the characters, then each character of the text is converted to its respective 8-bit binary number (considering the ASCII value for each character) then a 64-bit random binary number is generated, and it is to be considered as the key value. An exclusive OR operation is performed between the text and the key if the length of the plaintext higher the key is repeated same in the Vigenère cipher until every character has a pair with the key the formed text is ciphertext. The cipher text generated using this proposed will be in the range of 0 to 127 ASCII characters. To obtain this result MODULAR DIVISION (mod 128) operation is performed with the resulted text. The reverse process to this is the process of decryption [11, 5].

Steps Involved in Encryption

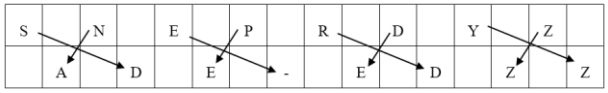
1. The first step is calculating the length of plain text, if it is not an integral multiple of 32-bits then padding is required.
2. Arrange the plain text into two rows, adding one character to each row, respectively. Divide these rows into blocks. Each block consists of 4 characters, 2 from each row.
3. Now, swap extremes of the block (1st& 4th character) and means of the block (2nd and 3rd character) respectively in all the blocks.
4. In this step, apply the rail fence algorithm to the text and generate the resultant text.
5. Now, generate a 64-bit random key value. Convert the resultant text to its respective ASCII value and then to an 8-bit binary value for each character.
6. Perform Exclusive OR operation with the resultant text and key value. Convert the result back to ASCII value apply mod 128 and then to characters accordingly.
7. The resulted text after all the operations is the ciphertext.
8. The reverse of the encryption process is the decryption process.

Example for Encryption Process

1. Let the plain text is SANDEEP REDDY.
   The length of plain text is 13.
   As 13 is not an integral multiple of 4 so padding is done.
   The next nearest multiple of 4 is 16.
   No of padding bits= 16-13= 3.
   So, it requires 3 additional bits for padding.
   The new plain text is SANDEEP REDDYZZZ.
2. Dividing into blocks

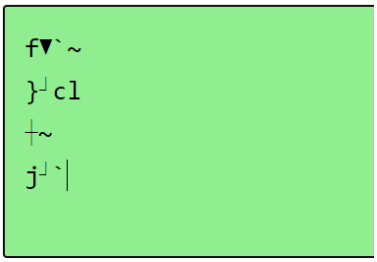


3. Swapping the characters.



After Swapping

4. Now perform Rail Fence and the resulted text is DA EDEZZNSPEDRZY.
5. Let the randomly generated 64-bit key value is00100010 01011110 01000000 00111011 01001001 00111000 01011110 00111001 and text in 8-bit binary value is 01000100 01000001 00100000 01000101 01000100 01000101 01011010 01011010 01001110 01010011 01010000 01000101 01000100 01010010 01011010 01011001.
6. After X-OR is performed the result is 01100110 00011111 01100000 01111110 00001101 01111101 00000100 01100011 01101100 00001010 00010000 01111110 00001010 01101010 00000100 01100000.
7. The ciphertext is

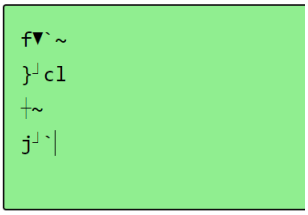


Steps Involved in Decryption

1. Both the encrypted text and key-value are received at the recipient end.
2. Convert every character of the encrypted text and key to ASCII value and then to an 8-bit binary value.
3. Now, perform Exclusive-OR operation with the encrypted text and key and convert this to ASCII values and then to characters.
4. Now, perform the decryption technique of the rail fence algorithm for the text resulted above.
5. Now divide the resulted text into blocks, where each block consists of 4 characters in a sequential manner.
6. Now, swap extremes of the block (1st& 4th character) and means of the block (2nd and 3rd character) respectively in all the blocks.
7. The resulted text after internal swapping is the decrypted text

Example for Decryption Process

1. The encrypted text is



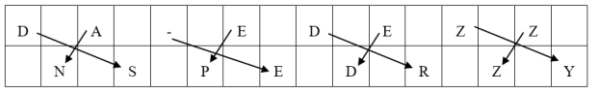
and the key is"^@;I8^9

2. The 8-bit binary value of encrypted text is 01100110 00011111 01100000 01111110 00001101 01111101 00000100 01100011 01101100 00001010 00010000 01111110 00001010 01101010 00000100 01100000 and transferred 64-bit key value is 00100010 01011110 01000000 00111011 01001001 00111000 01011110 00111001
3. The text resulted after Exclusive OR of key-value with ciphertext is 01000100 01000001 00100000 01000101 01000100 01000101 01011010 01011010 01001110 01010011 01010000 01000101 01000100 01010010 01011010 01011001 and the text is DA EDEZZNSPEDRZY
4. The resulted text after the rail fence decryption is DNAS PEEDDERZZZY.
5. Divide the text into blocks.

D		A		-		E		D		E		Z		Z	
	N		S		P		E		D		R		Z		Y

Block 1 Block 2 Block 3 Block 4

6. Now, swap extremes of the block (1st & 4th character) and means of the block (2nd and 3rd character) respectively in all the blocks.



After Swapping

S		N		E		P		R		D		Y		Z	
	A		D		E		-		E		D		Z		Z

7. The resulted text after internal swapping is the decrypted text i.e., SANDEEP REDDYZZZ.

5. CONCLUSION

Sending the data securely is an important task nowadays. The existing rail fence algorithm alone is not secure, as the plain text used, and the ciphertext formed using this algorithm starts with the same character. If this is identified by an attacker, then there is a chance of finding the key using a brute force attack. The process of decryption could be solved quickly by hand. Moreover, it is quicker if solved by using a computer. The way to increase the security level, this algorithm must be combined with another technique along with divide the table into blocks and swap the positions of the characters in their respective blocks. The ciphertext generated in the traditional rail fence algorithm will be in the range of plain text only. A hybrid algorithm is proposed to overcome the said limitations of the existing rail fence algorithm. Every character of the ciphertext generated using this proposed algorithm will be in the range of 0 – 127 ASCII values. The key generated in the proposed algorithm is a Random 64bit, this is additional security.

REFERENCES

[1] Samarth Godara, Shakti Kundu and Ravi Kaler "An Improved Algorithmic Implementation of Rail Fence Cipher" International Journal of Future Generation Communication and Networking, ISSN: 2233-7857, Vol. 11, No. 2, pp. 23-32 (2018)

[2] Andysah Putera Utama Siahaan "Rail Fence Cryptography in Securing Information" International Journal of Scientific & Engineering Research, ISSN: 2229-5518, Vol. 7, No. 7, pp. 535-538 July-(2016)

[3] Benni Purnama, Hetty Rohayani.AH "A New Modified Caesar Cipher Cryptography Method with Legible Ciphertext from A Message to Be Encrypted" Procedia Computer Science, ISSN: 1877-0509, Vol. 59, pp. 195-204 (2015)

[4] Ritwik Goyal, Prof. Binod Kumar Mishra, Prashant Lakkadwala, "Enhancing the performance of Data Encryption Standard algorithm by using Rail Fencing" International Journal for Research Trends and Innovation, ISSN: 2456-3315, Vol. 2, No. 3, pp. 130-134 (2017)

[5] Ashty M. Aaref, Ann Z. Ablhd "A NEW CRYPTOGRAPHY METHOD BASED ON HILL AND RAIL FENCE ALGORITHMS" Diyala Journal of Engineering Sciences, ISSN: 1999-8716, Vol. 10, No. 01, pp. 39-47 March-(2017)

[6] Jawad Ahmad Dar "Humanizing the Security of Rail Fence Cipher Using Double Transposition and Substitution" International Journal of Science and Research (IJSR), ISSN (Online): 2319-7064, Vol. 3, No. 9, pp. 1787-1791 September-(2014)

[7] Fahad Naim Nife "A New Modified Cesar Cipher Cryptographic Method Along with Rail Fence to Encrypt Message" International Journal of Advanced Research, ISSN: 2320-5407, Vol. 3, No. 2, pp. 331-335 (2015)

[8] U. Thirupalu, Dr.E. Kesavulu Reddy FCSRC (USA) "A New Cryptosystem for Ciphers using Transposition Techniques" International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 8, No. 04, pp. 402-406 April-(2019)

[9] Sumathi. R, N.R. Raajan "A SECURED APPROACH FOR CRYPTOGRAPHY USING MULTILEVEL ENCRYPTION" International Journal of Pure and Applied Mathematics, ISSN: 1314-3395, Vol. 119, No. 12, pp. 16613-16619 (2018)

[10] Baljit Saini "Modified Ceaser Cipher and Rail fence Technique to Enhance Security" International Journal of

Trend in Research and Development, ISSN: 2394-9333, Vol. 2, No. 5, pp. 348-350 October-(2015)

[11] Fahrul Ikhsan Lubis, Hasanal Fachri Satia Simbolon, Toras Pangidoan Batubara, Rahmat Widia Sembiring, "Combination of Caesar Cipher Modification with Transposition Cipher" Advances in Science, Technology and Engineering Systems Journal, ISSN: 2415-6698, Vol. 2, No. 5, pp. 22-25 (2017)

BIOGRAPHIES

Dr. A. Ashok Kumar, Assistant Professor, Department of Physics at Y.S.R. Engineering College of Yogi Vemana University, Proddatur. He completed Ph.D. from Department of Physics, Sri Venkateswara University, Tirupati. His areas of research includes Development of novel materials for energy applications and fabrication of semiconductor devices, Corrosion of Metals, applications of image processing in Engineering.

Dr. S. Kiran is Assistant Professor in the department of Computer Science and Engineering at Yogi Vemana University, Proddatur. He acquired M.Tech. Degree from Nagarjuna University, Guntur. He completed Ph.D. in computer science from S. K. University. He has been continuously imparting his knowledge to several students in research activities. He published many articles National and International journals. His research areas are image Processing, Cryptography and Network Security, Software Engineering and Data mining and Data warehouse.

Dr. R. Pradeep Kumar Reddy received his B.Tech. Degree in Computer Science and Engineering from Bellary Engineering College, Bellary (VTU)., M.Tech. Degree in Computer Science and Engineering at S.R.M University, Chennai and he obtained Ph.D. from Yogi Vemana University. Currently He is working as Assistant Professor in the Department of CSE at YSR Engineering College of Yogi Vemana University, Proddatur. He has got 12 years of teaching experience. He has published 25 research papers in various National and International Journals and about 8 research papers in various National and International Conferences. He has attended 10 workshops. He is a member of ISTE.

Sandeep Reddy Devara is currently in studying final year B.Tech. (Computer Science and Engineering) from YSR Engineering College of Yogi Vemana University, Proddatur. His interested areas include Network security and Image processing. He is a qualified GATE 2021 ranker with 18,497 rank.