Rail Fence Cryptography in Securing Information

Andysah Putera Utama Siahaan

Abstract — Rail Fence Cipher is a further development method of Caesar Cipher. In Caesar algorithm, the results derived from the ciphertext letters shifting each character in the plaintext. While in the Rail Fence, it is taken from the ciphertext block formation matrix diagonally. The level of security in this method has advantages than in the previous method. In this study, the research tries to encrypt and decrypt the message using the Rail Fence algorithm. The ciphertext is obtained by taking a certain set of characters in the line that has been determined earlier.

Index Terms — Rail Fence, Cryptography, Security, Zig Zag, Encryption, Decryption

1. Introduction

Cryptography is the art of science [1] [2]. It has two main subfields (i.e. cryptography and cryptanalysis). Cryptography is the science of creating secret codes; Cryptanalysis is the science of breaking codes. These two aspects are closely related; when creating a secret code the analysis of its security plays an important role [3]. It has been an interesting part to understand. It is primarily used by military and government peripherals. Private and commercial organizations have rarely considered it necessary to support the security of all link to the obvious place. There is a various method of applying the cryptographic systems [7][8][13]. The crypto companies are interested in financial circumstances. Rail Fence is one of the classic cryptosystem worked by substituting the position of the characters. It also called Transposition Cipher. Transposition ciphers rearrange the letters of plaintext without replacing them with another character.

2. Theories

2.1 Polybius Square

The Polybius Square is an ancient cryptography invention. It is discovered by a scholar named Polybius in the second century BC. Polybius find a password system that eventually were used for several centuries. Polybius put the letters in the column line array size of 5 × 5. The way this system works is that every letter is expressed as rows and columns in which the letters are placed [6][11][12]. For example, the letter "A" is encoded with "1-1", "B" as "1-2", “C” as “1-3”, “D” as “1-4”, “E” as “1-5” and so on. Because of the complete standard letters are 26, whereas only 25 places available, so in this system, the letter "I" and "J" have the same code. Figure 1 shows the form of the square matrix. It has five columns and five rows. Every character is replaced by the cell index which was taken from column and row index. The cell name is used to change the plaintext to be ciphertext. The grid must be extended if the characters used is more than 26 letters. The 6 x 6 can cover 36 characters, 7 x 7 has 49 characters and so on. However, at Polybius time, it was only used to hide the standard message. It is usually done in war. They hoped the message did not fall into enemy lines.

11 A	12 B	13 C	14 D	15 E
21 F	22 G	23 H	24 IJ	25 K
31 L	32 M	33 N	34 O	35 P
41 Q	42 R	43 S	44 T	45 U
51 V	52 W	53 X	54 Y	55 Z

Fig. 1. The Polybius Square

Polybius does not have the specific key. It only uses the transposition to turn into ciphertext. It is a very standard encryption and weak. It needs to combine with another security system to its algorithm. The password is a good idea to make it secure. Alternatively, maybe the character position in the grid can be reordered.

2.2 Rail Fence

Rail Fence inspired from Polybius square modeling. However, in Rail Fence, the ciphertext does not follow the Polybius regulation. He formed his trajectory. This trajectory shaped Zig Zag. That is why this method is often called Zig Zag Cryptography. The Rail Fence is a simple example of the transposition ciphers and very weak algorithm [4]. Generally, in this method, the plaintext elements are written into a matrix form approved by the sender and the receiver. It means the matrix model is approved or know by both participants. There are many ways how to form the ciphertext [9][10]. Sometimes it can be performed by diagonal retrieval.

Rail Fence Cipher security is very weak. The weakness can be seen from the lack of key. The number of practical keys is small enough that a cryptanalyst can break. It allows mixing up of characters in plaintext to produce the ciphertext, it offers essentially no communication security and will be shown that it can be easily broken. It cannot be used to encrypt images containing large areas of single color. Although the Rail Fence is weak, it can be mixed with another cryptography algorithm such as substitution cipher, the combination of which is harder to break than either

- *Andysah Putera Utama Siahaan is currently working as a lecturer at Universitas Pembangunan Panca Budi and pursuing doctor degree program in Computer Science Universiti Sains Malaysia, Penang.*
- *E-mail: andiesiahaan@gmail.com*

cipher on its own [5].

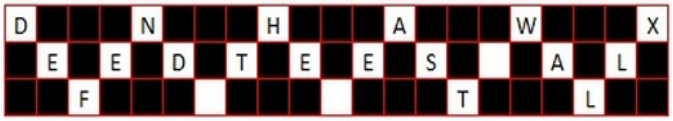

Fig. 2. The Rail Fence Structure

Figure 2 illustrates how to form the text into Zig Zag cryptography. The grid above consists of three rows. The sentence “DEFEND THE EAST WALL” is split into the array of a character. The rest is filled with “X”. The Rail Fence has a unique trajectory, diagonal step. The length of the column depends on the total amount of characters divides how many rows to be expected. The ASCII can be implemented by using this method since it does not have the new character table.

3. EVALUATION

As implementation, this section tries to figure out how the Rail Fence algorithm works. The calculation of this algorithm is very simple and easy. It just arranges the position of the characters instead of having a calculation of a heavy mathematical operation. To find how it works, let’s see the explanation below. Assume the message is “**ANDYSAH**” as the plaintext. First, the grid must be determined. The total row, in this case, is three.

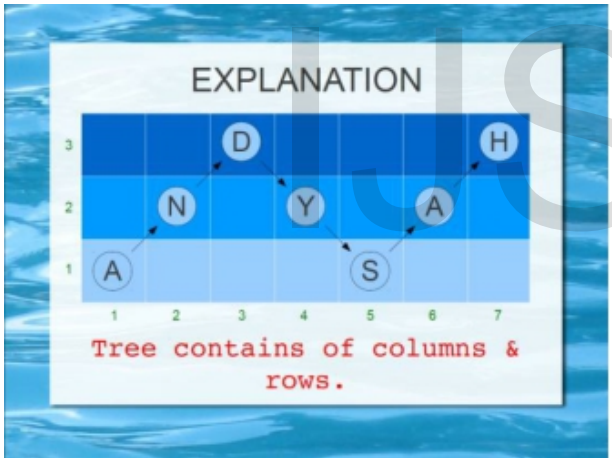

Fig. 3. Grid division

The word is arranged in diagonal order as seen in Figure 3. The first character places on the first row and the first column. The next characters are put by adding row and column simultaneously. The arrangement goes up continuously. After it reaches the top rows, it turns back down to reach the first row again. It continues until reach the last character. If it does not get the top character but the rest of character is empty, the rest of cell is placed by letter “X” or something else decided earlier.

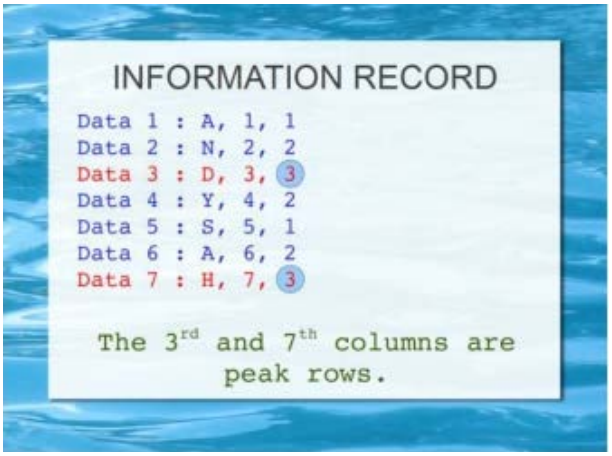

Fig. 4. The row and column information.

Figure 4 illustrates the information of every character. It consists of seven data of the message. The first data is letter “A” which placed in row 1 and column 1. Next, the second is letter “N” in row 2 and column 2. The top row is 3. If the data reaches this row, it will be subtracted until it reaches the first row. The message above contains two data which rows are in the top rows such as data 3 and data 7.

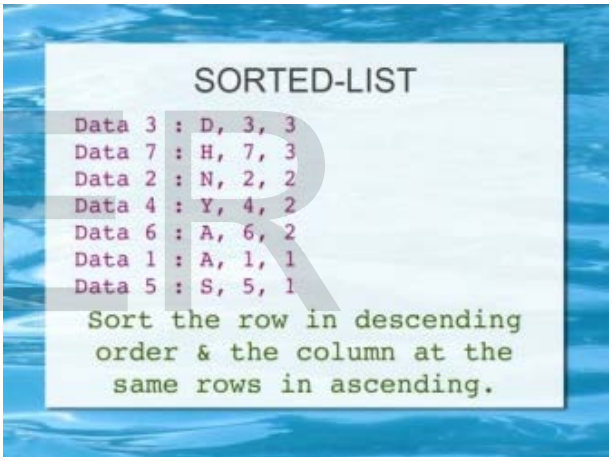

Fig. 5. Data is sorted in descending order.

Figure 5 explains the data than has previously been arranged in row order. The ciphertext is obtained by sorting the data in descending order. At this step, the row is the header of the sort. The data number 3 and 7 will be the first order since they have the highest row. In the other word, they are categorized based on rows.

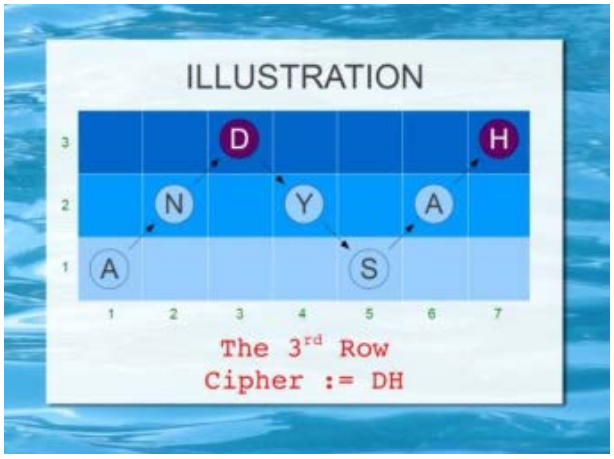

Fig. 6. The data taken from the third row.

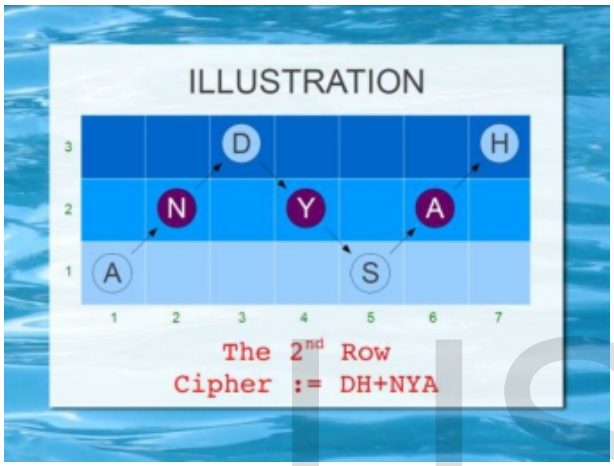

Fig. 7. The data taken from the second row.

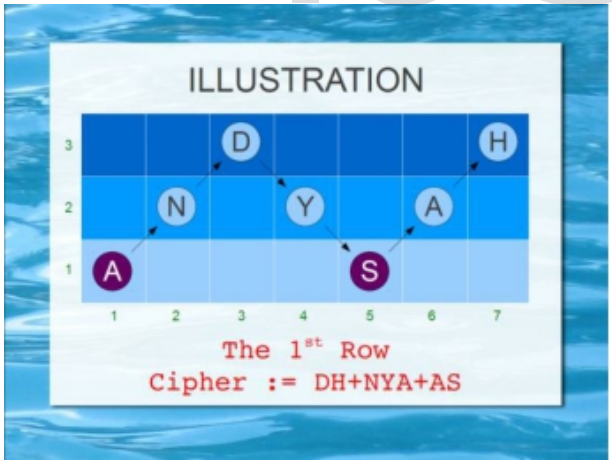

Fig. 8. The data taken from the first row.

Figure 6 to Figure 8 are the process of the ciphertext retrieval. In Figure 6, the characters at the top row are drawn. They are letter “D” and “H”. In Figure 7, the data is drawn from the second row again. The characters will be letter “N”, “Y”, and “A”. Then the last retrieval is from the first row, such as letter “A” and “S”. The letters will be concatenated soon after completed.

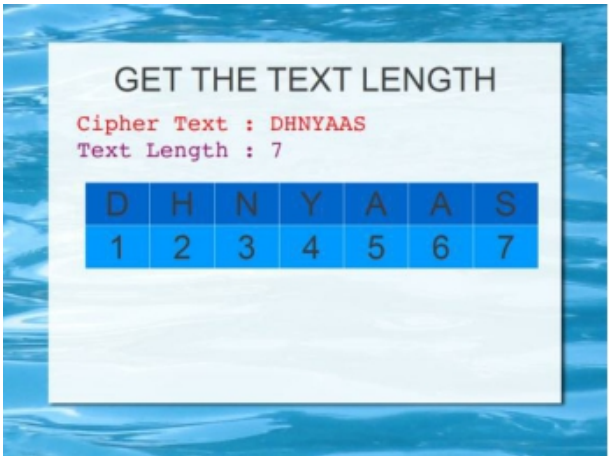

Figure 9. The ciphertext.

Figure 9 shows the result of the Rail Fence process. The ciphertext obtained is “**DHNYAAS**”. The decryption step is to reconstruct the grid using the previous message. It starts putting characters from the highest row. If the top row is recognized, the ciphertext is breakable. The top row or how much is the row is the decryption key. Anyone can break the message by trying such a set of keys, start from 1 and so on. Let’s see the illustration in following tables below. The following explanation will try to decrypt the previous ciphertext “**DHNYAAS**”.

TABLE I
DECRYPTION PROCESS (PART 1)

	1	2	3	4	5	6	7
C			**D**				**H**
B							
A							

Table 1 shows the first two characters is put in cell C3 and C7. Since the length of the ciphertext is 7, it needs to make the length of the column is 7 as well. The first character is put in C3 because the top row is 3. The second character in cell C7. Why? Let’s see the formation. The first in column 3. The next character must be in C3 – B4 – A5 – B6 – C7 formation. The column number 7 is still available.

TABLE III
DECRYPTION PROCESS (PART 2)

	1	2	3	4	5	6	7
C							
B		**N**		**Y**		**A**	
A							

Table 2 shows the next characters is put in cell B2, B4, and B6. The first character has been occupied in C3. The first character in row B must be in B2. So, the formation will be B2 – C3/A3 – B4 and B4 – C5/A5 – B6. The letters “N”, “Y” and “A” are put in cells B2, B4, and B6.

TABLE IIIII
DECRYPTION PROCESS (PART 3)

	1	2	3	4	5	6	7
C							
B							
A	**A**				**S**		

The rest of two characters, letter “A” and “S” are placed in cell A1 and A5. The first character is put in cell A1 since cell C3 and B2 have been occupied before. The formation will be A1 – B2 – C3 – B4 – A5. The last character is put in Cell A5 based on the formation.

TABLE IVV
DECRYPTION PROCESS (PART 4)

	1	2	3	4	5	6	7
C			**D**				**H**
B		**N**		**Y**		**A**	
A	**A**				**S**		

Table 4 shows the complete process of the decryption. Knowing the top row or the highest row used in the construction set, it is easily obtained the plaintext back without asking permission getting the key. After the characters in the table are constructed, it will be concatenated each other in series of string. The plaintext obtained is “**ANDYSAH**”. Until now, the process of Rail Fence is just finished.

4. CONCLUSION

In this paper, the research has presented how to implement the Rail Fence encryption and decryption. The Rail Fence algorithm is a simple cryptography algorithm. However, it is not secure. The key is how many rows is implemented. It can be guessed by making a brute-force attack. The decryption process can 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 or modify the table by changing the trajectory. Random position [6] [7]of transposition might improve the security. It is the introduction to the further research to develop this algorithm to be more protected. There are many ways can contribute in this method.

REFERENCES

[1] J. Omolehin, O. A. C. and A. O. Bajeh, "The Complexity of 4-Row Rail Fence Cipher Encryption Algorithm," *International Journal of Mathematical Science,* vol. 1, no. 1, pp. 8-14, 2009.

[2] J. O. Omolehin, O. C. Abikoye and R. G. Jimoh, "Development of Data Encryption and Decryption Algorithm Using 4-Row Rail Fence Cipher," *Jounal of Nigerian Association of Mathematical Physics,* vol. 13, pp. 411-416, 2008.

[3] T. S. Kondo and L. J. Mselle, "An Extended Version of the Polybius Cipher," *International Journal of Computer Applications,* vol. 79, no. 13, pp. 30-33, 2013.

[4] J. A. Dar, "Humanizing the Security of Rail Fence Cipher Using Double Transposition and Substitution Techniques," *International Journal of Science and Research,* vol. 3, no. 9, pp. 1787-1791, 2012.

[5] J. A. Dar and S. Sharma, "Implementation of One Time Pad Cipher with Rail Fence and Simple Columnar Transposition Cipher, for Achieving Data security," *International Journal of Science and Research,* vol. 3, no. 11, pp. 2415-2421, 2012.

[6] A. P. U. Siahaan, "High Complexity Bit-Plane Security Enhancement in BPCS Steganography," *International Journal of Computer Application,* 8 2016.

[7] A. P. U. Siahaan, "RC4 Technique in Visual Cryptography," *International Journal of Computer Science and Engineering,* vol. 3, no. 7, pp. 1-5, 2016.

[8] A. P. U. Siahaan, "Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm," in *Senapati*, Bali, 2016.

[9] A. P. U. Siahaan, "Blum Blum Shub in Generating Key in RC4," in *KNSI*, Batam, 2016.

[10] A. P. U. Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique," in *SNATI*, Yogyakarta, 2016.

[11] A. P. U. Siahaan, "BPCS Steganography Noise-For Region Security Improvisation," *International Journal of Science & Technoledge,* 2016.

[12] A. P. U. Siahaan, "Vernam Conjugated Manipulation of Bit-Plane Complexity Segmentation," in *ICEST*, Medan, 2016.

[13] B. Oktaviana and A. P. U. Siahaan, "Three-Pass Protocol Implementation on Caesar Cipher in Classic Cryptography," *IOSR Journal of Computer Engineering (IOSR-JCE),* vol. 18, no. 4, 2016.

AUTHOR PROFILE

Andysah Putera Utama Siahaan was born in Medan, Indonesia, in 1980. He received the S.Kom. degree in computer science from Universitas Pembangunan Panca Budi, Medan, Indonesia, in 2010, and the M.Kom. in computer science as well from the University of Sumatera Utara, Medan, Indonesia, in 2012. In 2010, he joined the Department of Engineering, Universitas Pembangunan Panca Budi, as a Lecturer, and in 2012 became a junior researcher. He is applying for his Ph. D. degree in 2016. He has written in several international journal and conference. He is now active in writing papers and joining conferences.