ENHANCEMENT OF EFFICIANT DATA SECURITY ALGORITHM USING COMBINED AES AND RAIL FENCE TECHNIQUES

Khadidja NYIRANSABIMANA[1], NKUBITO Serge[2], Dr. Papias NIYIGENA[3]

[1]UNIVERSITY OF LAY OF ADVENTISTE OF KIGALI (UNILAK)
[2]FACULTY OF COMPUTING AND INFORMATION SCIENCES
[3]MASTERS OF SCIENCES IN INFORMATION AND TECHNOLOGY, RWANDA

---***---

ABSTRACT - Cryptography is the security science that allows researcher to improve the confusion of the complex algorithm for the plain text encryption and cipher decryption in order to increase the security rate all over the world. Rail fence techniques are simple methods used to encrypt the plain text and decrypt the cipher text. Objective of this study is to encrypt and to decrypt using the new algorithm by combining the rail fence techniques with AES. The general purpose of this research is to improving the complexity cipher Security.

Key terms: Aes, Cryptography, cipher text, Decryption, Encryption, Plain text, Rail Fence, Security.

I. INTRODUCTION

With the growth of internet hackers and spies make big issue for security. Many people use internet like online shopping, money transfer from bank account, etc while hackers and spiers use also the internet. It is difficult to distinguish hackers from normal clients. This makes the security of data to be strongly protected during data transmission and transactions. This requires highest degree of understanding the security. Since this information is sensitive, we don't like it to reach the unauthorized persons. This study makes more complex the efficient data security combined AES and Rail fence techniques and to allow people who have the decryption algorithm, are the only one able to decrypt the cipher into the readable message.

Encryption is the process of encoding the message to be sent to the recipient in order to hide the content (wikipedia, 2019). To make the message doubtful, we have to use transposition techniques to encrypt the plain text and to decrypt the cipher. The plain text is the original message to be sent to the recipient and the cipher is encoded message. The Rail fence cipher is a form that referred as zigzag cipher and transposition cipher is a form of rectangular table. This enhancement of data security algorithm consists encrypting the plain text once by dividing the cipher into different sections and permutation of those sections depending on the row boundaries this how the cipher text is obtained. This new algorithm has been proposed to increase the complication of the cipher text without the time complication of the encryption algorithm.

II. METHODOLOGY

The proposed algorithm is used for the encryption and decryption of data by providing New Rail fence Algorithm which is more confused than the first one.

CASE1:

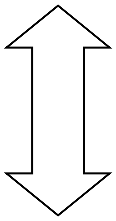
The given plain text: I like to study

Its encryption by rail fence with row boundary 2, is:

	1	2	3	4	5	6	7	8	9	10	11	12
R1	I		I		E		O		T		D	
R2		L		K		T		S		U		Y

FIGURE1.

The cipher text is: IIEOTDLKTSUY



By knowing the row boundary we can make this **NEW** table:

Step 1: simple transposition

1	2	1	2	1	2	1	2	1	2	1	2
I	L	I	K	E	T	O	S	T	U	D	Y

FIGURE2.

The cipher is obtained by writing down the letters containing the same number starting from right to left:

Simple Cipher is: IIEOTDLKTSUY

Step 2: double transposition

The new plain text become: IIEOTDLKTSUY

1	2	1	2	1	2	1	2	1	2	1	2
I	I	E	O	T	D	L	K	T	S	U	Y

FIGURE 3

Double cipher: IETLTUIODKSY

Step 3: Triple transposition

The new plain text become: IETLTUIODKSY

1	2	1	2	1	2	1	2	1	2	1	2
I	E	T	L	T	U	I	O	D	K	S	Y

FIGURE 4

The triple cipher = final cipher =ITTIDSELUOKY

The decryption is:

Because of the row boundary were 2, the total number of letters composed the cipher text is 12(nCT), nCT divide by 2 equal to 6,

We are going to divide the cipher text into sections of 6 letters from right to left.

CT= ITTIDSELUOKY

Xi | Yi

$PT = \sum_{I=1}^{\infty}(XiYiZi)$

PT = X_1 Y_1 X_2 Y_2 X_3 Y_3

PT_1= IETLTUIODKSY

X_i | Y_i

PT_2=IIEOTD LKTSUY

X_i | Y_i

PT= ILIKETOSTUDY

CASE 2:

Let consider also the row boundary is 3:

1	2	3	1	2	3	1	2	3	1	2	3
I	L	I	K	E	T	O	S	T	U	D	Y

FIGURE5.

The cipher is: IKOULESDITTY

1	2	3	1	2	3	1	2	3	1	2	3
I	K	O	U	L	E	S	D	I	T	T	Y

FIGURE 6.

The cipher is: IUSTKLDTOEIY

1	2	3	1	2	3	1	2	3	1	2	3
I	U	S	T	K	L	D	T	O	E	I	Y

The cipher is: ITDEUKTISLOY

The decryption is:

Because of the row boundary were 3, the total number of letters composed the cipher text is 12(nCT), nCT divide by 3 equal to 4.

We are going to divide the cipher text into sections of 4 letters from right to left.

PT_1= **ITDE UKTI SLOY**

X_i | Y_i | Z_i

$$PT = \sum_{I=1}^{\infty}(XiYiZi)$$

Aglorithm for encryption

1. Start
2. The plain text(PT) without space
3. Row boundary number(nR)
4. write down the plaintext in a numbered table with the index corresponding exactly to nR
5. write down letters with same number
6. reverse letters
7. write down the cipher text(Ct)
8. end

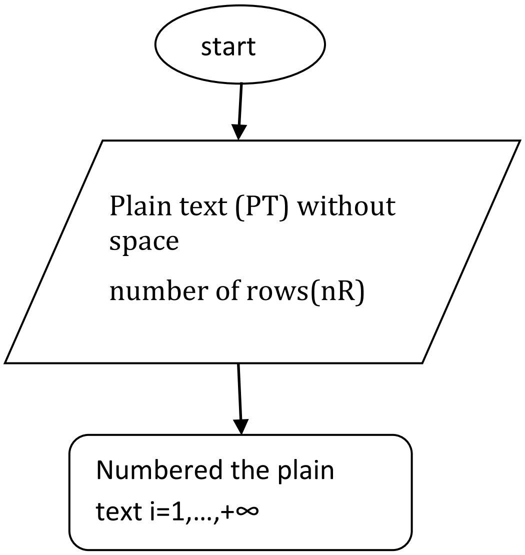
Algorithm for decryption

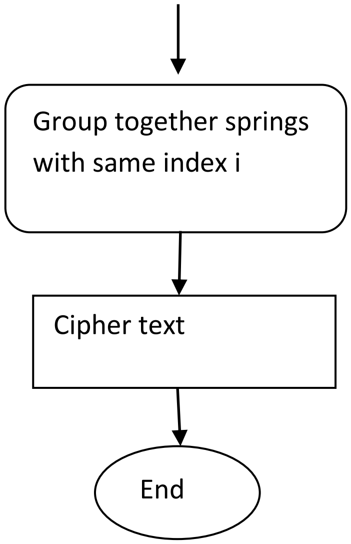
1. Start
2. Number of Given cipher text(nCT)
3. Number of given row boundary(nR)
4. If nCT is multiple of nR
5. S= nCT/nR
6. Split CT into sections of S letters
7. write down the cipher text in a numbered table with the index corresponding exactly to nR
8. permit the strings of cipher text

9. Else
10. Add x,y or z to CT until nCT is multiple of nR
11. Go to 5
12. Reconstruct the plain text
13. Write the plaintext

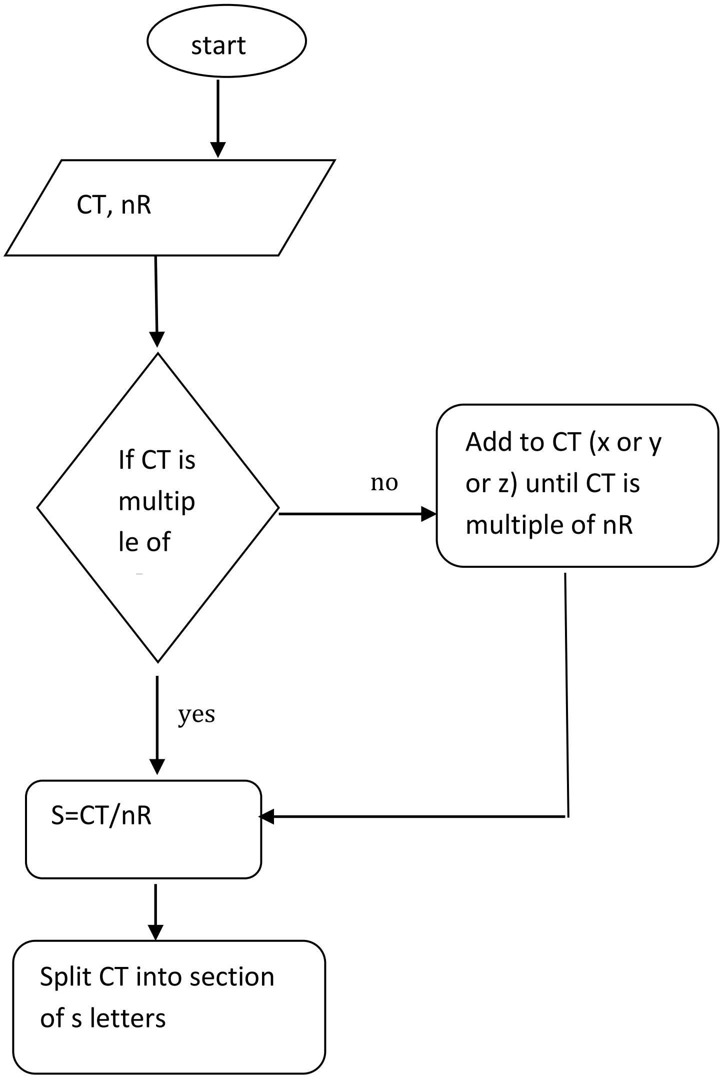
Flow charts

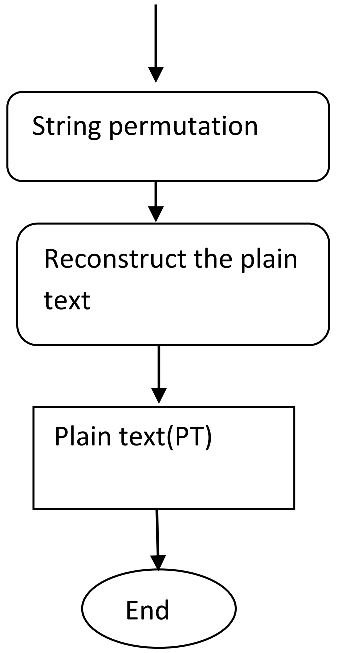
1. **For encryption**


start
Plain text (PT) without space
number of rows(nR)
Numbered the plain text i=1,…,+∞



2. **For decryption**


start
CT, nR
If CT is multip le of
no
Add to CT (x or y or z) until CT is multiple of nR
yes
S=CT/nR
Split CT into section of s letters



III. RETERATURE REVIEW

Substitution cipher is a method of encoding by which units of plaintext are replaced with cipher text, according to a regular system; the "units" may be single letters (the most common), as Rail fence Cipher is not very well-built; The integer of practical keys is tiny sufficient that a cryptanalyst can attempt them all by hand and simply allows reversing of characters in plain text to form the cipher text, it offers essentially no communication security and will be shown that it can be easily broken. (Dar, Humanizing the Security of Rail Fence Cipher, 2012), (Godara, An Improved Algorithmic Implementation of Rail Fence Cipher, 2018) He converted given plain text into Rail Fence cipher text by generating the permutation of the plain text. The outer loop of the algorithm chooses the rail number, starting from 1 and the inner loop puts letters into cipher and computes the place of letter of the letter which will be the subsequent letter in the Rail chosen by outer loop, until all the letters in that Rail gets written out. (Singh, 2012), He find out the algorithm by combined Caesar and Rail fence techniques with stack by using PUSH and POP, this algorithm was difficult to implement. (M.Lavanya, 2018) Improved data security by combining AES with Rail Fence techniques. The key generation was carried out by hybrid cipher which is the combination of public key and symmetric key cryptosystem; it was harder to decode the cipher. (Dar, Humanizing the Security of Rail Fence Cipher, 2012)) improved the algorithm security of Rail fence cipher using double transposition and substitution, this algorithm was difficult to implement and use two keys than.

IV. CONCLUSION

Along this paper I have showing how to improve the security data security combining AES (Advanced encryption standard) and Rail fence techniques in order to make it more secured and strong than the first. Future scope need to focus on more research to boost the security of substitution techniques.

BIBLIOGRAPHY

1. Dar, J. A. (2012). Humanizing the Security of Rail Fence Cipher. *International Journal of Science and Research (IJSR)* , 2319-7064.

2. Dar, J. A. (2012). Humanizing the Security of Rail Fence Cipher. *International Journal of Science and Research (IJSR)*, 2.

3. Dar, J. A. (2012)). Humanizing the Security of Rail Fence Cipher. *International Journal of Science and Research (IJSR)* , 2319-7064.

4. Godara, S. (2018). An Improved Algorithmic Implementation of Rail Fence Cipher. *International Journal of Future Generation Communication and Networking*, pp.23-32. Retrieved from https://pdfs.semanticscholar.org/9d0e/3bd3f1cb881465cd04e3279b3bcc2ed0f1af.pdf

5. Godara, S. (2018). An Improved Algorithmic Implementation of Rail Fence Cipher. *International Journal of Future Generation Communication and Networking*, pp.23-32.

6. M.Lavanya. (2018). EFFICIENT DATA SECURITY ALGORITHM USING COMBINED AES AND. *International Journal of Pure and Applied Mathematics*, 3219-3227.

7. Siahaan, A. P. (2016). *"Vernam Conjugated Manipulation of Bit-Plane.* Medan: in ICEST.

8. Siahaan, A. P. (2016). *Dynamic Key Matrix of Hill Cipher Using Genetic.* Senapati: Bali.

9. Siahaan, A. P. (2016). Rail Fence Cryptography in Securing Information. *International Journal of Scientific & Engineering Research, Volume 7, Issue 7*, 2229-5518.

10. Siahaan, A. P. (RC4 Technique in Visual Cryptography). RC4 Technique in Visual Cryptography. *International Journal of Computer Science and Engineering, vol. 3,*, pp. 1-5.

11. Singh, A. (2012). Implementation of Caesar Cipher with Rail Fence for. *International Journal of Advanced Research in*, pp. 78-82.

12. U, B. O. (2016). Three-Pass Protocol. *IOSR*, vol. 18, no. 4.

13. wikipedia. (2019, september 20). *The free encyclopedia*. Retrieved 2019, from Encryption: https://en.wikipedia.org/wiki/Encryption

14. Y. RANGEL-ROMERO, R. V.-G.-M.-C. (2008). Comments on "How to repair the Hill cipher". *Journal of Zhejiang University SCIENCE A*, pp 211–214.