Diyala Journal of Engineering Sciences

ISSN 1999-8716
Printed in Iraq

Vol. 10, No. 01, pp. 39-47, March 2017

A NEW CRYPTOGRAPHY METHOD BASED ON HILL AND RAIL FENCE ALGORITHMS

Ashty M. Aaref [1], Ann Z. Ablhd [2]
[1, 2] Lecturer, Software Engineering Department college technology / Kirkuk, Iraq
ann_zeki2001@yahoo.com [1], ashty_06@yahoo.com [2]
(Received: 29/12/2015; Accepted: 28/3/2016)

ABSTRACT:- Encryption has a great benefit, it provides privacy and security of all concepts of data transmitted across open networks. An urgent need for methods of strong encryption has become important with the rapid development of the computer, it detract from the strength of encryption; and because the increase computer speed means shortening the time that the computer needs to break or disclosure of specific encryption key.

Encryption may be strong or weak, to measure the encryption strength by the time and resources required for the process of detecting non-encrypted texts of encrypted texts. As a result of testing proposed system it appear that this system is strong encryption cipher text because it is hard to detect with the time or provide the necessary tools to detect the plain text.

Due to the wide use of broken cipher methods in Cryptography. There are many important information to be secure. It proposed a new approach of ciphering, by mixing a substitution followed by a transposition cipher methods to produce a new secure method difficult to break. This is a bridge from a classical to modern ciphers.

The substitution cipher algorithm that is used in this paper is Hill cipher, and the transposition cipher algorithm that is used is Rail fence.

The language that is used for this proposed algorithm is C++ with Object Oriented Programming. The proposed system is called RailHill.
Keywords: *encryption, decryption, transposition, substitution.*

1. INTRODUCTION

Cryptography is the science or art of encompassing the principles and methods of transforming an intelligible message into one that is intelligible and then transforming the message back to its original form [(1)].

Today's cryptography is more than encryption and decryption. Authentication is as fundamentally a part of our lives as privacy. We use authentication throughout our everyday lives when we sign our name to some document and for instance and, as we move to world where our decisions and agreements are communicated electronically, we need to have electronic techniques for providing authentication [(2)]. Cryptography provides mechanisms for such procedures. There are two types of operations used for transforming plaintext to cipher text. All encryption algorithms are based on two general types of operations. Those are substitution, in which each element in the plain text is mapped into another element and transposition in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost. Most systems referred to as product systems, involved multiple stages of substitution and transposition, render a message incompressible to the unauthorized reader. The aim of cryptography is to cipher the secret and important information [(3)].

2- TRANSPOSITION CIPHER

In a transposition cipher, the order of plaintext letters is changed to derive the cipher text. Transposition ciphers are stronger than simple substitution ciphers. The message is usually written without word divisions in rows of letters arranged in a rectangular block. The letters are then transposed in a prearranged order, such as by vertical columns, diagonals, or spirals, or by more complicated systems, such as the knight's tour, which is based on the move of the knight in chess. [4] The arrangement of the letters in the enciphered message depends upon the size of the block of code words used and upon the route followed in inscribing and transposing the letters. A cipher in which every pair of letters is swapped is an example of a transposition cipher. In this case, for example, the cipher text for *elephant* would be *lepeahtn*. The first and second letters are swapped, then the third and fourth letters are swapped, and so on. Transposition ciphers may be combined with substitution ciphers to produce a more complex encoded message as this paper algorithm [5]. The transposition cipher method used in this paper is "Rail Fence".

3. RAIL FENCE

Rail fence ciphers are examples of transposition ciphers: The characters in the plaintext message are permuted to create the cipher text. In the rail fence cipher, the permutation is obtained from a very simple pattern Other transposition ciphers use other manipulations to permute the characters .The encryption key for a rail fence cipher is a positive integer[6].

The sequence of letters on the upper line is then followed by the sequence on the lower line, to create the final encrypted message. The security of the cipher can be improved by choosing more than two lines to encrypt your message with .It could change the number of lines by inserting a number into the box labeled "Number of Lines". To decipher a message encrypted using two lines, it will need to divide the message into halves and write the second half below the first. Then it can read the message column by column. When deciphering any cipher text, it is crucial to know how many lines were used to encrypt the message [7].

Suppose we want to encrypt the message “MEET ME AFTER THE TOGA PARTY”` using a rail fence cipher with encryption key 3. Here is how we would proceed. Arrange the plaintext characters in an array with 3 rows (the key determines the number of rows forming a zig-zag pattern). In the rail fence cipher, the plaintext is written downwards and diagonally on successive "rails" of an imaginary fence, then moving up when we reach the bottom rail. When we reach the top rail, the message is written downwards again until the whole plaintext is written out [8]. The message is then read off in rows with depth for example 3, the cipher text writes out as the example in figure (1).

The simplest such cipher is the rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as sequence of rows. Figure (2) contains the Rail Fence program. Figure (3) contains the results of rail fence program.

4. SUBSTITUTION CIPHER

Substitution ciphers are probably the most common of cipher. They work by replacing each letter of the plaintext (and sometimes punctuation marks and spaces) with another letter or possibly even a random symbol.

The simple substitution has been in it basically consists of substituting every plaintext character for a different cipher text character. In cryptography, a 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), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution [9].

Substitution ciphers can be compared with transposition ciphers. In a transposition cipher, the units of the plaintext are rearranged in a different and usually quite complex order, but the units themselves are left unchanged. By contrast, in a substitution cipher, the units of

the plaintext are retained in the same sequence in the cipher text, but the units themselves are altered.

There are a number of different types of substitution cipher. If the cipher operates on single letters, it is termed a simple substitution cipher [10] a cipher that operates on larger groups of letters is termed polygraphic. A monoalphabetic cipher uses fixed substitution over the entire message, whereas a polyalphabetic cipher uses a number of substitutions at different positions in the message, where a unit from the plaintext is mapped to one of several possibilities in the cipher text and vice versa[10]. The algorithm that used in this paper is Hill cipher.

5. HILL CIPHER

The Hill cipher is a cryptosystem that enciphers blocks. Any block size may be selected, but it might be difficult to find good keys for enciphering large blocks.

5.1 Encryption with the Hill Cipher

The Hill cipher is an example of a block cipher. A block cipher is a cipher in which groups of letters are enciphered together in equal length blocks. In order to encrypt a message using the Hill cipher, first should assign a number to each character of the alphabet of coded letters. A=0, B=1, C=1…etc see fig.(4) .The sender and receiver must first agree upon a key matrix *A* of size *n* x *n*. *A* must be invertible mod 26 [11].

The plaintext will then be enciphered in blocks of size *n*. In the following example *A* is a 2x2 matrix and the message will be enciphered in blocks of 2 characters. Figure (5) represents program part of hill cipher.

Key Matrix: A = $\begin{pmatrix} \mathbf{3} & \mathbf{25} \\ \mathbf{24} & \mathbf{17} \end{pmatrix}$

Plain Text: MISSISSIPPI

The first block MI corresponds to the matrix $\begin{pmatrix} 12 \\ 8 \end{pmatrix}$.

The sender will then calculate:

$$A \cdot \begin{pmatrix} 12 \\ 8 \end{pmatrix} = \begin{pmatrix} 2 \\ 8 \end{pmatrix} \pmod{26}$$

The first two letters of the cipher text correspond to 2, 8 and are therefore CI characters see Figure (4). This step is repeated for the entire plaintext. If there are not enough letters to form blocks of 2, pad the message with some letter, say Z.

Plain text: MI SS IS SI PP IK will be decrypted as:

Cipher text: CI KK GE UW ER OY

Notice that the repeated digraphs IS, SS and repeated letters S and P in the plaintext are masked using the Hill cipher. To decipher a message, first calculate the inverse of the key A, figure (6) contains code of a part for inverse 3x3 [7].

$$A^{-1} = \det(A)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \pmod{26}$$

Then multiply the inverse of the key by each pair of cipher text letters (mod 26) to recover the original text.

Key Matrix: A = $\begin{pmatrix} 3 & 17 \\ 8 & 25 \end{pmatrix}$

Cipher text: CI KK GE UW ER OY

The receiver will calculate:

$$A^{-1} \begin{pmatrix} 2 \\ 8 \end{pmatrix} = \begin{pmatrix} 12 \\ 8 \end{pmatrix} \text{ (mod 26)}$$

To decrypt the message. The first two letters are 12, 8 which correspond to M and I characters, see Figure (4). The receiver will repeat this step for every pair of letters in the cipher text to recover the original plain text message "MISSISSIPPIK". To use a Hill cipher with different block size the number of rows and columns in matrix *A* should be equal to the block size. For example if the block size is 4 the *A* should be a matrix of size 4 x 4.

6. RAILHILL SYSTEM

Program in C++ with Object Oriented Programming was built to combine Rail Fence cipher (to represent transposition cipher) with Hill cipher (to represent substitution cipher) to produce an encryption control system is difficult to break. The algorithm of the RailHill as follow:

1. Start
2. Input Plain Text (P1) // for cipher where P :Plain Text
3. Find C1= Rail Fence (P1) // and C : Cipher Text
4. Let P2=C1
5. Find C2=Hill(P2)
6. Find P2=Hill(C2) // for decipher
7. Find P1=Rail Fence(P2)
8. Output P1
9. End

7. RESULTS

To get started to run RailHill at first it should has a plain text. For example the plain text that used as input to RailHill is "SOFTWARE PART" to be cipher with the proposed system as output cipher text "NEXRX HCBED VOP" see figure (7) . The result is strong and difficult to break. And same character ciphered to different characters and all the plain text characters quite different from the original text.

The steps of RailHill that lead to the above results are as following:

1. At first the plain text "SOFTWARE PART" pass to Rail Fence algorithm where used as follow:

   S - - - W - - - - P - - -
   - O - T - A - E - A - T
   - - F - - - - R - - - R

The output of this is: Cipher text = "SWPOT TAEAT FRR".

2. The Cipher text = "SWPOT TAEAT FRR" is considered as plain text to Hill cipher algorithm by use the encryption key as follow:

Where C1=(k11.p1+k12.p2+k13.p3) mod 26

C2=(k21.p1+k22.p2+k23.p3) mod 26

$$K=\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

The first three letters of the plain text are represented by the vector as Figure (4) :

$$\begin{pmatrix} 19 \\ 23 \\ 16 \end{pmatrix} . \begin{pmatrix} 17 \\ 17 \\ 5 \end{pmatrix} = \begin{pmatrix} 14 \\ 5 \\ 24 \end{pmatrix}$$

The corresponding characters = N E X . With the same way it gets the cipher text :
Plain Text : SWPOT TAEAT FRR
Cipher Text: NEXRX HCBED VOP

Decryption requires using the inverse of the matrix K. The inverse K' of a matrix K is defined by the equation : KK'=K'K=I ,where I is the matrix that is all zeros except for ones along the main diagonal from upper left. The inverse of a matrix does not always exist, but when it does, it satisfies the preceding equation, the inverse for above example:

$$K'=\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 06 \\ 24 & 0 & 17 \end{pmatrix}$$

This is demonstrated as follows:

$$\begin{pmatrix} 17 & 17 \\ 21 & 18 \\ 2 & 2 \end{pmatrix}\begin{pmatrix} 5 \\ 21 \\ 19 \end{pmatrix}\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 \\ 858 \\ 494 \end{pmatrix} \quad \begin{pmatrix} 442 & 442 \\ 495 & 780 \\ 52 & 365 \end{pmatrix} \text{ mod } 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

It is easily that if the matrix K' is applied to the cipher text, then the plain text is recovered. In general the proposed system can be expressed as follows:
C=E(K,P)=KP mod 26
P1=D(K,P)=K' C mod 26= k'KP
P2=reverse Rail Fence

7. DISCUSSION AND CONCLUSION

There are several methods of conventional cryptography, and since it is possible to break the cipher text ,that why it tried to propose a system RailHill written in Object Oriented programming of C++ language to be more secure for protect the information from breaking cipher. Mixing Hill cipher with Rail Fence, it is seem that the modified Hill cipher Encryption and Decryption requires generating random Matrix, which is essentially the power of security of RailHill. As we know in Hill cipher decryption requires inverse of the matrix. Hence while decryption one problem arises that is, inverse of the matrix does not always exist. Then if the matrix is not invertible them encrypted text cannot be decrypted. But this drawback is completely eliminated in modified Hill cipher algorithm.

At the same time, this method requires the cracker to find the inverse of many square matrices which is not computationally easy. So this mixed system implement difficult cipher to be break from the cracker.

After measuring the execution time of RailHill and the strong of this algorithm it seems that faster implementation time and more secure than substitution and transposition algorithms. It is faster because it use the Object Oriented programming of C++ language.

9. REFERENCES

1) Nicolas Courtois, Josef Pieprzyk, (2002), "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations", pp267–287, Asiacrypt.
2) Delfs, Hans, Knebl, Helmut, (2007), "Symmetric key encryption, Introduction to cryptography: principles and applications", Springer.
3) Mullen, Gary, MummertCarl, (2007), "Finite fields and applications", American Mathematical Society. p. 112, IEEE 1363: Standard Specifications for Public-Key Cryptography.
4) A. F. A. Abidin, O.Y. Chuan and M.R.K. ariffin, (2011), "A Novel enhancement Technique of the Hill Cipherfor effective Cryptographic Purposes", Journal of Computer science .
5) Dharmendra Kumar Gupta , Sumit Kumar Srivastava, Vedpal Singh,(2012), "New Concept of encryption algorithm A hybrid approach of Caesar Cipher and Columnar transposition in multi stages", Journal of Global Research in Computer Science, Volume 3,p.60- 66.
6) Fauzan Saeed, Mustafa Rashid- "Integrating Classical Encryption", Volume 10, No. 5, May 2010.
7) Amogh Mahapatra, (2007), "DATA ENCRYPTION AND DECRYPTION BY USING HILL CIPHER TECHNIQUE AND SELF REPETITIVE MATRIX", A thesis submitted in partial fulfillment of the Bachelor of Technology in Electronics & Instrumentation Engineering Rourkela.
8) Prof. K. Govinda, Dr. E. sathiyamoorth, (2011), "Multilevel Cryptography Technique Using Graceful Codes", Volume 2, No.7
9) Monodeep Banerjee, SaptarshiNaskar, krishnenduBasuli, Samar SenSarma, (2012), "A Novel scheme for Text data encryption", No.1.
10) Phillip I Wilson and Mario Garcia, (2006), "A Modified Version of the Vigenere algorithm", No.3B.
11) Raj jain, (2006), "Design of a Robust Cryptosystem Algorithm for Non Invertible Matrices Based on Hill Cipher", No.5.
12) Sriram Ramanujam, Mrimuthu Karuppiah,(2011), "Designing an algorithm with high Avalanche effect International Journal of Computer Science and Network Security", Volume11, No.1.
13) William Stallings, (2012), "Cryptography and Network security", Second Edition.

Plain text: MEET ME AFTER THE TOGA PARTY

Row 1: M M T H G R

Row 2: E T E F E T E O A A T

Row 3: E A R T P Y

Cipher Text: MMTHGR ETEFETEOAAT EARTPY

Figure (1) Represents example of rail fence cipher

```
#include<conio.h>
#include<string.h>
#include <iostream.h>
#include<ctype.h>
void main()
{
inti,j=0,d,k=0;
char p[50],ct[50][50];
printf("Enter the plain text:\n");
gets(p );
printf("\nEnter the depth in the integer"  );
cin<<d;
declare null for empty array values/  ////
for (i=0;i<50;i++)
{
For (j=0;j<50;j++){
ct[i][j]='\0';
}}
k=0;
loop up to string length of the plaintext///
{
++)for(i=0;i<strlen(p);i
{
for(j=0;j<d;j++)
{
if(k<=strlen(p ))
ct[i][j]=p[k];
++ct[i][j]='\0;k ';
.
```

Fig. 2 Contains part of the program used to process Rail Fence

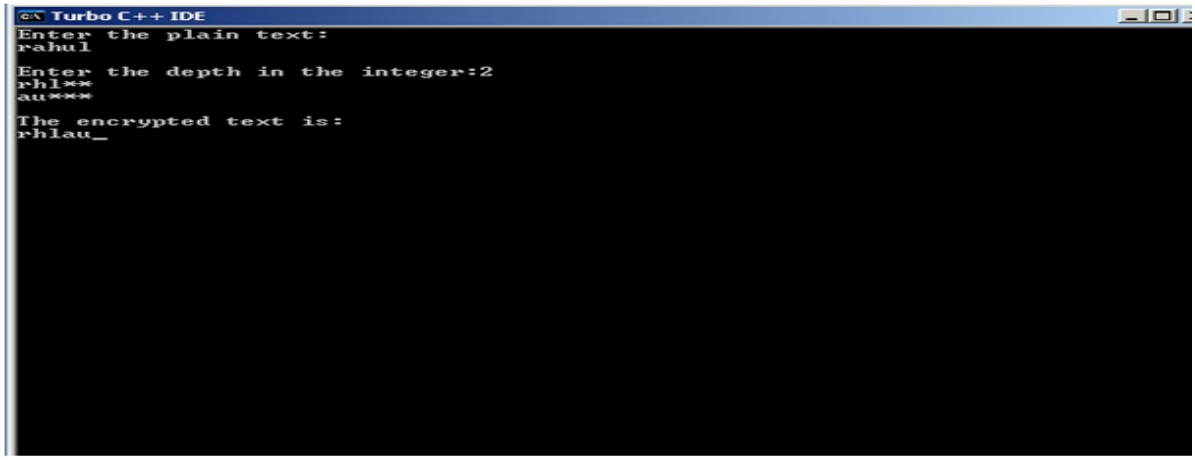

Fig. (3) represents the output Rail Fence with the key 2

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Figure (4) Each character represents by number

```
#<include<stdio.h>
#include<conio.h.
<include<string.h#
void main()
{char aa[26]="abcdefghijklmnopqrstuvwxyz";
char pt[10];intm,d,q=0,i,j,k[2][2],p[4],pp[4],t[5];int k1[2][2],k2[2][2],det;clrscr();
printf("enter the plaintext:" );
scanf("%s",pt);m=strlen(pt);
printf("enter the numbers:");for(i=0;i<2;i++){for(j=0;j<2;j++)
{scanf("%d",&k[i][j]);}}for(i=0;i<m;i++)
{for(j=i;j<26;j++){if(pt[i]==aa[j])
{t[q]=j%26;++q;}}}
p[0]=(k[0][0]*t[0])+(k[0][1]*t[1]);……..
p[1]=(k[1][0]*t[0])+(k[1][1]*t[1]);
p[2]=(k[0][0]*t[2])+(k……
```

Figure (5) contains code of a part for Hill cipher.

```
include<stdio.h>
int main()
{ int a[3][3],i,j;
 float determinant=0;
printf("Enter the 9 elements of matrix: ");
for(i=0;i<3;i++) for(j=0;j<3;j++)
scanf("%d",&a[i][j]);
printf("\nThe matrix is\n");
for(i=0;i<3;i++){ printf("\n"); for(j=0;j<3;j++) printf("%d\t",a[i][j]); } for(i=0;i<3;i++) determinant =
determinant + (a[0][i]*(a[1][(i+1)%3]*a[2][(i+2)%3] - a[1][(i+2)%3]*a[2][(i+1)%3])); printf("\nInverse of
matrix is: \n\n ;("
for(i=0;i<3;i++)
{ printf("\n"); for(j=0;j<3;j++)
printf("%d\t",a[i][j]); } for(i=0;i<3;i++) determinant = determinant + (a[0][i]*(a[1][(i+1)%3]*a[2][(i+2)%3] -
a[1][(i+2)%3]*a[2][(i+1)%3])); printf("\nInverse of matrix is: \n\n");
 for(i=0;i<3;i++){ for(j=0;j<3;j++)……..
printf("%.2f\t",((a[(i+1)%3][(j+1)%3] * a[(i+2)%3][(j+2)%3]) - (a[(i+1)%3][(j+2)%3]*a[(i+2)%3][(j+1)%3]))/
{;determinant); printf("\n"); } return 0
```

Figure (6) contains code of a part for inverse 3x3

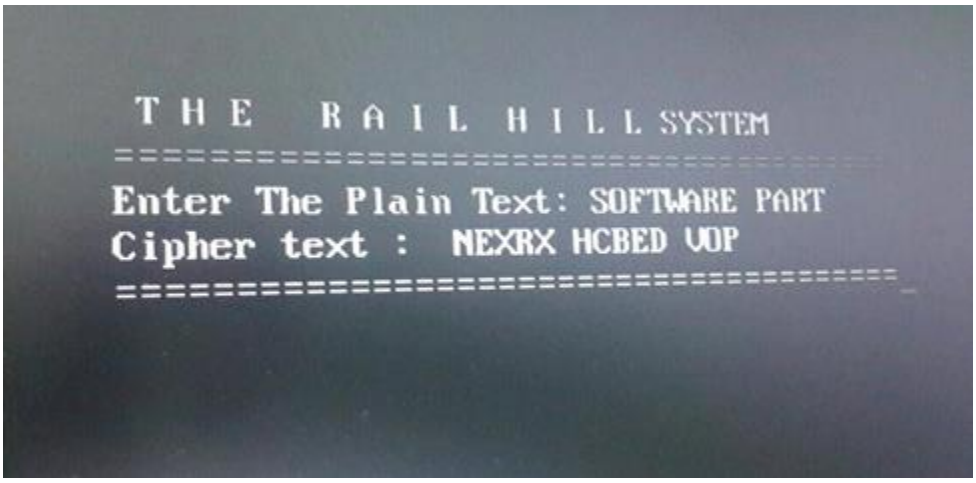

Figure (7) represents the run of RailHill

تصميم طريقة جديدة بالتشفير بدمج طريقتي التشفير Hill , RailFence

[1] د.آن زكـــي أبلحد ,[2] د.أشتي مهدي عارف
مدرس , الكليـــة التقنيـــة / كركـــوك,قسم هندسة البرمجيات [1،2]

الخلاصة

للتشفير فوائد كبيرة حيث يوفر خصوصية وأمن لجميع مفاهيم البيانات المرسلة عبر الشبكات المفتوحة. حيث أصبح لطرق التشفير الصعبة الكسر حاجة ملحة مع التطور السريع للكمبيوتر. ولأن زيادة سرعة الكمبيوتر يعني تقصير الوقت الذي يحتاج الكمبيوتر إلى كسر أو الكشف عن مفتاح تشفير معين.
إن طرق التشفير المستخدمة في تحسين أمنية إرسال واستقبال المعلومات بين الأشخاص المختلفين تعتبر من الأمور الهام.

لذا تم من خلال هذا البحث المساهمة بتطوير طريقة جديدة تختلف عن طرق التشفير الكلاسيكية المألوفة وذلك بدمج الطريقتين المعروفتين طرق التحويل والاستبدال معا .

نظرا إلى اتساع وشيوع طرق كسر الشفرات المستخدمة في اغلب طرق التشفير المألوفة في علم التشفير, ونظرا إلى أهمية وسرية المعلومات المستخدمة لذا فقد ارتأينا إلى إعداد طريقة جديدة من التشفير بدمج إحدى طرق الاستبدال Hill مع طريقة من طرق التحويل **RailFence** لينتج نص مشفر يصعب كسره من أي متطفل.

اللغة التي يتم استخدامها لهذه الخوارزمية المقترحة C ++ مع البرمجة الشيئية. ويطلق على النظام المقترح RailHill.