Development of Data Encryption and Decryption Algorithm using Modified Rail Fence Cipher

J.O Omolehin*++, O.C Abikoye + and R.G Jimoh+

++ Mathematics Department, University of Ilorin, P.M.B 1515 Ilorin, Nigeria.

+ Computer Science Department, University of Ilorin, P.M.B 1515 Ilorin, Nigeria

Abstract

The increase use of electronic means of data transfer from one point to the other coupled with growth in networking and internet has really called for vital security. This security is usually achieved by encryption and digital signature. Data encryption is the automated process of securing data so that no unauthorized person can access them. It makes use of different algorithm to scramble (encrypt) the original message called plaintext into an unintelligible message called cipher text. Key is an important object in data encryption. There are some data encryption algorithm that uses same key for both its encryption and decryption while some uses two keys, one for encryption and the other for decryption.

Rail fence cipher is categorized under data encryption algorithm that uses same key for both its encryption and decryption. The number of rows used to break up text/data to be encrypted into rows and column arrangement serves as the key in Rail fence cipher.

In this paper we present the algorithm that can encrypt and decrypt data using a Modified Rail Fence Cipher.

The modification includes the inclusion of a subroutine that re-encrypts the data at a set time interval so that after the first use of a known key, the subsequent key(s) that will be used will be internally determined by the algorithm. This ensures that the key is kept confidential.

Keywords

Encryption, Decryption, Cipher text, algorithm, Rail Fence Cipher, Plain text, Row, Modified Rail Fence Cipher.

1. Introduction

In today's computer-permeated world, it can be difficult to remember that only a few years

* Corresponding author: Email:omolehin_joseph@yahoo.com

have elapsed since the microprocessor evolution enable the computer to move out of esoteric glass-isolation to become an every day part of work and play for millions of people. In fact, the computer designer industry has grown from minor adjunct of computer (hardware) industry into a major economic sector, containing some of the largest companies in the world.

During the early days, there was nothing like secrecy. We can see today that some business moguls transact their business with their customers through communication channel (e.g. computer) and other important software therefore, these message medium has to be secured in a way that only those concern will easily understand. Now we are witnessing a transformation in the role computer and software plays in people's life. Advances in hardware technology and in software design are changing the definition of system and shrink –wrapped word processors.

The need for information security cannot be overemphasized. It has been appreciated for many years that it is one of the progress achieved. An alternate protection techniques is provided by transformation of data into a form that does not provide information when intercepted, such methods can protect information in an insecure environments and can provide effective secrecy. This field of computer application is very important because majority of information transfer is now done over public networks like the internet where information can be intercepted easily by anyone. This field is known as CRYPTOGRAPHY

Cryptography is the art or science encompassing the principle and method of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to it original form. Cryptography is not a puzzle to test a patient but is the science of secret communication. Its object is arranged in some sort of systematic disorder, which can be set right quickly and accurately by the one for whom the secret message is intended [4].

In advancement, there is need for implementation of cryptography in information transmission technology. Infact there are important confidential and diplomatic information that needs to be transmitted which required proper protection from the unauthorized users. Therefore, the implementations of cryptographic techniques are really called for. The use of cryptography is one method that has greatly enhanced the security of communication through networks.

When we talk of protection of information under the study of cryptography, it can be defined as the art of safeguarding information or data from accidental or deliberate threats which might cause unauthorized modification or disclosure of data. This is just to make sure that unauthorized user cannot have access to information. [2, 10, 5].

1.1 Data Encryption and Decryption.

The process of cryptography is divided into two major part i.e. encryption and decryption.

Encryption

Encryption is defined as the authorization of hiding data system so that no unauthorized persons can access them. This is done by means of a procedure (algorithm) and a key. Thus, encryption can be said to be the process of creating a secret out of data.

Encryption also includes making authentication or digital signature schemes that use an algorithm and a key. A clear message (plain text message) is transformed into a cipher text message during the process of encryption.

Decryption

Decryption is the reverse process of encryption. It is the process of revealing data to person authorized to access it. It is the revelation of coded data. It is also carried out by means of an algorithm and a key. [2]

2. Key System

Key is a very important object in cryptography. This is because all process in cryptography requires a key to be implemented. Keys play an important and major part in the security of cryptography since the security of cryptography (including encryption and decryption) has its keys, the keys have to be properly managed and they must have sufficient length to ensure security. Therefore, the two major concerns in key system are: [10]

2.1 Key management

During encryption, the use of key is very important not only that the key should have sufficient length; they must also have to be kept very well. Key management is the most significant part of using encryption. This doesn't helps to use a strong crypto-algorithm if one carelessly handles the key.

One needs to have an idea on how to store key immediately after its generation under protection of a password. A good option is to store the key on magnetic or smart cards. Alternatively, the key may be encrypted by a master key which is closely guarded by a trusted person. The key known as a private key have a lifetime of several years which must be guarded from disclosure.

2.2 Key length

Key must be of sufficient length to resist a brute force attack. The number of key to be tried by brute force attack rose exponentially with key length. To keep abreast of advance in computer technology, it is important to raise key length by one bit every one and half years. It was understood that a minimum symmetric key length is 75bit should be standard for securing message for some time to come, while asymmetric key lengths vary from 768 to 2048 bit in length.

2.3 Type of Key System

There are several ways of classifying cryptography algorithm. This study considers two categories of cryptography based on the number of key that is employed for encryption and decryption. The two types of key system are symmetric and asymmetric. [8]

2.3.1 Symmetric key System

The symmetric key system is a key system in which the same key is used for both encryption and decryption. As a result, the key must always be guarded as a secret. Symmetric key are known as secret keys and the process or system of using secret key is known as private cryptography.

The drawback of symmetric key system is that the key used to be distributed securely. Conventional cryptography cannot be used for this method because a common key is needed.

In a process of large groups, the required numbers of secret become enormous. Despite these methods, the symmetric key systems are computationally faster than asymmetric key system. In symmetric key system, the encryption key is the sane as the decryption key. Though the key management has some problems but is still computationally fast.

2.3.2 Asymmetric Key system

This key system was introduced in 1976 by Diffie and Hellman. It is base on one-way trap door function. A one-way function is a mathematical operation that is easy to do in one way but impossible or difficult to reverse.

Asymmetric key system is one in which a public key is used for encryption while a secret key decrypts the coded information. The public key is spread widely as possible while the private key is guarded secretly. Any one with a public key can encrypt the data or message. Asymmetric key system is also call public key system.

The problem with asymmetric key is that it is susceptible to attacks and is a very slow process.

2.3.3 Characteristics of Public and Private Key system

Public key systems have the following characteristics

1. Encryption key is the same as the decryption key.
2. It can be encrypted and decrypted using a lot of keys which make key management difficult
3. It is computationally fast

While private key systems have the following characteristics

1. The encryption and decryption keys are different.
2. Encryption is easy, but decryption is very difficult.

3. It is a slow process.

3 Cipher System

When we talk of cipher system, we refer to a system of secret or private system. In a cipher system, the message or information which is going to be encrypted or the key used in decrypting the message is agreed upon by the encipher(person who send the encrypted message) and the recipient(person who decrypt the message) . In cipher system it always involved two parties in communication. In this, the two parties agreed on a particular key which should be kept secret and will always be assured that although he knows the enciphering algorithm, an interceptor does not know the particular key word. The enciphered decide on the message that he wishes to send using a key and encryption algorithms before transmission.

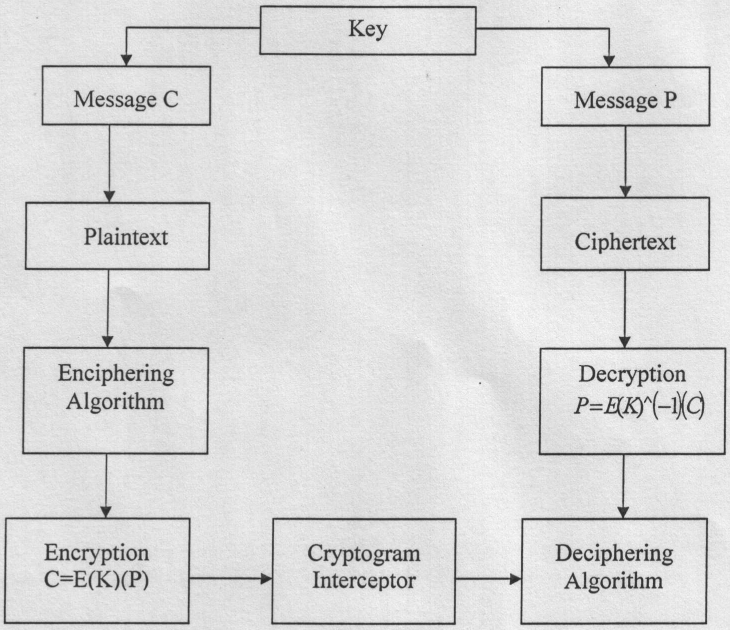


Figure 3.1
Rail fence Cipher

The Rail Fence Cipher is a type of transposition cipher. A transposition cipher involves the rearranging of the letters in the plaintext to encrypt the message [11]. The Cipher is the simplest example or class of transposition cipher called route ciphers. These were quite popular in the early history of cryptography. Generally, the rail fence cipher encompasses row and column rearrangement of letters.

Encrypting a message with Rail Fence Cipher using 4-row

Similar to the diameter of the cylinder in the scytale machine, the number of rows of the rail fence cipher is the key used in encrypting and decrypting secret message. Thus, for the implementation of rail fence cipher, the number of rows used to break up the message serves as the encryption key. It determines the exact form that the secret message will take. To take an example suppose we want to encrypt the message "MERCHANT TAYLOR SCHOOL" using 4-row rail fence cipher. When using rail fence cipher the spaces in the original message may be removed first or not. We would then write the characters in the message in columns of alternating rows, which resembles the rail of a fence. It is better to include the spaces in the original characters so as to make the recovery of our plaintext from our ciphertext meaningful during decryption.

Note that a padding will be always be added to the characters so as to fill up the remaining spaces in the rows of the fence.

M	H		L	S	O
E	A	T	O	C	L
R	N	A	R	H	B
C	T	Y		O	B

Plaintext: MERCHANT TAYLOR SCHOOL

Ciphertext: MH LSOEATOCLRNARHBCTY OB

In trying to arrange the characters, we introduced the last two letters "Bs" to fill in the remaining space in the fence. This is called padding. The padding added to this fence is two characters so as to make a complete fence.

4 Rail Fence Cipher Pseudocode

Pseudocode is an outline, or English like steps of an algorithm in which a program or a problem is solved. In this paper pseudocode is used to outline how the rail fence cipher works.

As discussed earlier that rail fence cipher deals with row and column rearrangement, the numbers of rows used to break up the messages servers as the encryption key. It determines the exact form that the secret message will take. The pseudocode goes thus:

Input number of rows

Input plaintext

If the number of rows and columns space is equal to the number of character in the plaintext,

Arrange the plaintext in column,

Else,

A padding is introduced to fill in the space (padding could be any letter)

Encrypt in column

Print ciphertext

Then,

Decrypt in rows

Print plaintext.

Stop.

5. Rail Fence Cipher Algorithm

An algorithm can simply be defined as a step to step method of solving a particular program or problem at hand. In a more standard definition of algorithm, an algorithm is a finite list of instructions (each of which has a clear meaning) which can be carried out in a fixed order (with a finite amount of effort and time) to find solution to a particular problem or task [12]. An algorithm is implemented using a particular programming language.

The algorithm phase is going to show how the steps in encrypting and decrypting an information or message using a rail fence cipher technique. The algorithm was designed to demonstrate the feasibility of developing programs that can perform encryption and decryption using a rail fence cipher techniques to make data or information to neither be unreadable to an unauthorized party that has no access to it nor that does not have the encryption key. See appendix for the algorithm

6. Conclusion

Rail fence cipher is a cipher system that uses same key for both its encryption and decryption that belongs to the class of transposition cipher called route ciphers. Encryption key depends on the number of rows used to break down message into row and column arrangement to resemble a rail of fence.

The algorithm was designed to demonstrate the feasibility of developing programs that can perform encryption and decryption using a Modified Row Rail Fence Cipher technique so that data and key reliability, confidentiality and integrity can be achieved.

References

1. B. Ahmed, "Implementation of Cryptographic algorithm (A Case study of 4-rows Rail Fence Cipher)" Unpublished B.Sc project under the supervision of O.C Abikoye (Mrs),

University of Ilorin, Ilorin Nigeria, 2005.

2. D.E. Dening, "Cryptography and Data security", Reading (MA) Addison – Wesley, 1982 .
3. W. Diffie and S. Landau, "Privacy on the line Boston", MIT press, 1998.
4. N. Ferguson and B. Schneier, "Practical Cryptography", New York: John Wiley and Son, 2003.
5. D. Kahu, "The Codebreakers: The story of secret writing", revised Ed. New York: Scriber, 1996.
6. C. Kaufman, R. Perlman and M. Speciner, "Network Security; Private Communication in a public word", Englewood Cliffs (NJ) Prentice Hall, 1995.
7. R.J. Spillman, "Classical and Contemporary Cryptology" Upper Saddle River (NJ) Pearson Prentice-Hall, 2005.
8. W. Stallings, "Cryptography and Network Security: Principles and Practice", 4th Ed. Englewood Cliffs (NJ): Prentice Hall, 2005.
9. A. Sinkov ," Elementary Cryptanalysis: A Mathematical Approach", The Mathematical Association of America, Washington , D.C, 1966.
10. L.D. Smith, "Cryptography: The science of secret writing", Dover Publication Inc, New York, 1955.
11. URL: (http://starbase.trincoll.edu/~crypto/historical/railfence.html) S. Knight, "Cryptography: The Rail Fence Cipher", 2003.
12. T. H. Cormen, C. E. Leiserson and R. L. Riverst, "Introduction to Algorithms", The MIT press Cambridge, Massachusetts London, England, 1992.

Appendix

Encryption Algorithm

RFCEncrypt Algorithm.

```
Function RFCEncrypt (Indata: String, RowSize:Integer): String
StartPos <---- 1
NextCol <---- 1
MainBlock <---- Int(Length(Indata)/RowSize)
MainLenght <---- RowSize * MainBlock
RemainLenzw <---- Length(Indata) – MainLenght
If RemainLen > 0 then
  PaddingLen <---- RowSize – RemainLen
```

```
            If Padding > 0 then
               For i <------ 1 to PaddingLen
                  Padding <------ Padding & "B"
               End
         End
         MainLenght <------ Length(Indata) + PaddingLen
         BlockData <------ Indata & Padding
         MainBlock <------ Int( Length(BlockData)/RowSize)
         Redim  Matrix(RowSize,MainBlock)
         For i <------ 1 to MainBlock
            Chunk <------ Mid(BlockData,StartPos, RowSize)
            StartPos <------ StartPos + RowSize
            For j <------ 1 to RowSize
               Matrx( j,NextCol) <------ Mid(Chunk,j,1)
               ReDim Preserve Matrix(RowSize, NextCol + 1)
           NextCol <------ NextCol + 1
         For i <------ 1 to RowSize
            For j <------ 1 to NextCol
               CombinedBlock <------ CombinedBlock & Matric(i,j)
         RFCEncrypt <------ CombinedBlock
End Function
Procedure reEncrypt ( timeInterval:Integer)
         Indata <------ RFCDecrypt(CipherData, CurRowSize)
         CurrentTime <------ GetCurrentTime
         If (CurrentTime – PrevTime) > = timeInterval Then
         20: RowSize <------ rnd( ) * 10
            If RowSize <> CurRowSize Then
               RFCEncrypt ( Indata, Rowsize)
            Else Go to 20
            End
        End
End Procedure
```

Decryption Algorithm

RFCDecrypt Algorithm

```
FunctionRFCDecrypt (Indata:String, RowSize:Integer):String
StartPos  <——  1
NextRow  <——  1
MainBlock  <——  Int(Length(Indata) /RowSize)
Mainlenght  <——  RowSize * MainBlock
BlockData <——  Indata
Matrix(RowSize, MainBlock)
For i <——  1 to RowSize
    Chunk <——  Mid(BlokData, StartPos, MainBlock)
    StartPos <——  StartPos  + MainBlock
    For j <——  1 to MainBlock
        Matrix(NextRow,j)  <——  Mid(Chunk, j,1)
        Preserve Matrix (RowSize, MainBlock)
    NextRow  <——  NextRow +1
For i <——  1 to MainBlock
   For j <——  1 to RowSize
      CombinedBlock  <——  CombinedBlock  & Matrix(j,i)
RFCDecrypt <——  CombinedBlock
End Function
```