ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

Implementation of Rail Fence & Position Analyze Technique for More Secure Data

N.Sivakumar[1], V.Navamani[2], V.Yuvaraj[3]

[1]HOD, Dept. Information Technology, KSG College of Arts and Science, Coimbatore, Tamilnadu ,India

[2,3]Research Scholar, Dept. Computer Science, KSG College of Arts and Science, Coimbatore, Tamilnadu, India

Abstract: In this faster world peoples shares important information through network and wants strong security while sharing data. So to provide such a strongest security to our data the most popular method is used which is known as cryptography. Cryptography is the art and science of achieving security by encoding messages to make them non-readable. In this paper, we combine the rain fence technique and positions analyze technique to achieve more secure data than the normal transposition technique. To increase security we use such type of techniques.

Keywords: cryptography**,** transposition technique, rail fence technique, position analyze technique, cipher text, plain text

I. INTRODUCTION

Cryptography is technique of keeping message secret means protect our data from unauthorized user by applying encryption of message and decryption of message. Encryption converts readable form of message into readable form. Decryption converts unreadable form of message to readable form. Cryptography is divided into two types symmetric key cryptography, asymmetric key cryptography. Here two encryption method is used which is substitution techniques and transposition techniques.

Symmetric key cryptography use single key for encryption and decryption hence it is called as secret key cryptography and asymmetric key use pair of public and private key so it is called as public key cryptography.

II. BASICS OF CRYPTOGRAPHY

Cryptography provides security to a data at the time of transmission by performing some operations. The main goal of using cryptography is to help user to hide information from unauthorized user.

A. ENCRYPTION

It is a technique of converting a readable form of message into unreadable form means conversion of plain text into an cipher text. Encryption is performed when message is send by sender. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. Internet, e-commerce).
Encryption is the process of converting data to an unrecognizable or "encrypted" form. It is commonly used to protect sensitive information so that only authorized parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the Internet.

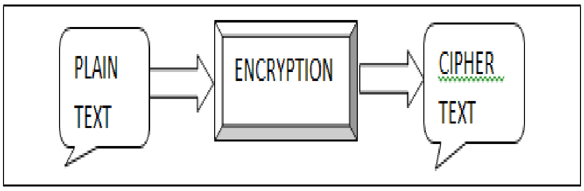

Fig 1 shows the process of encryption

B. DECRYPTION

It is an technique of converting a unreadable form of message into readable form means conversion of cipher text into an plain text. Decryption is perform when message is received. Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys.

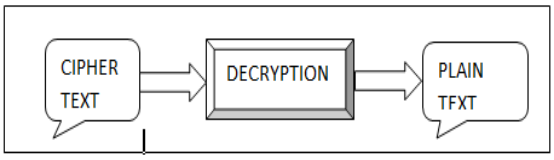

Fig 2 shows the process of Decryption

III.NETWORK SECURITY

Computer and network security is an ever expanding area. Security issues and incidents rise at an alarming rate every year. As the complexity in the network rises the need for security also rises. Many applications, softwares and companies have the need to hide details from the users.

- Authentication: the origin of a message can be verified.
- Integrity: proof that the contents of a message have not been changed since it was sent.

- Non-repudiation: the sender of a message cannot deny sending the message.
- Monitoring Communication: Fractional observing of data-used when the sender wants only some part of the message to be monitored and not all. In this case translucent cryptography is used that works on the space between strongly encrypted and weak/no encryption areas.

IV. METHODOLOGY

In cryptographic terms, the message in its original form is called plaintext and the encrypted form is called the cipher text. The transmitter in a secure system encrypts the plaintext to hide its meaning. The process of encoding the plain text into cipher text is called encryption and reverse the process of decoding ciphers text to plaintext is called decryption. Rail fence and position analyze technique, first we apply the rail fence technique to encryption and next we apply the odd even technique to decrypt the original message.

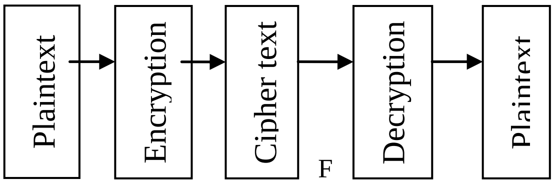

Fig3. Block Diagram of cryptographic system

If the sender uses the rail fence technique for encryption and the receiver uses the position analyze technique for decryption. I used this method we got original text.

V. IMPLEMENTATION & RESULT

A. RAIL FENCE TECHNIQUE

Rail fence technique involves writing plain text as sequence of diagonals and then reading it row by row to produce cipher text. 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.

Algorithm:

1. Write down the plain text message as sequence of diagonals.
2. Read the plain text written in step1 as a sequence of roes.

Example:

WHERE ARE YOU
W E E R Y U
H R A E O

Result is: WEERYUHRAEO

B. POSITION – ANALYZE TRANSPOSITION TECHNIQUE

Title Position-analyze technique means writing plaintext as a sequence of odd number of text (or) character to produce a cipher text.

Algorithm:

1. Every letter in the plain text message as a number in sequence. i.e.1,2,3…,,
2. Collect the odd numbers as a sequence (1,3,5) and then collect even number as a sequence (2,4,6)
3. Combine all the odd number sequence and even number sequence we get a sophisticated cipher text.
4. Repeat steps 1-4 based on the key.

Example:

WEL COME
1,2,3,4,5,6,7
Odd sequence (1,3,5,7)
=>(W L O E)
Even sequence (E C M)
Combine odd &even sequence = W L O E + E C M
W L O E E C M
Again assign the number sequence.

Example:

First Encrypt the message HELLOWORLD using the Rail Fence techniques, we Get the message like HLOOLELWRD. Next apply the odd even transposition technique to that message until we get the original message.

HELLO WORLD
H L O O L
E L W R D
HLOOELWRD
HOLLRLOEWD
HLROWOLLED
HRWLELOOLD
HWEOLRLLOAD
HELLOWORLD

Result is:
HELLOWORLD

VI. CONCLUSION

Rail fence techniques and position analyze transposition technique we find a mere complicated cipher text. These two classic techniques are combined, a strong cipher which is mere secure is obtained. Feature enhancement we combine two text or characters to apply this technique more secure data than single characters.

REFERENCES

[1] ”Transposition method for cryptography” by Sathish Bansal and Rajesh Shrivastava In ‘The IUP journal of computer sciences, Vol. 5, No.4, 2011’.
[2] Atul Kahate (2009), Cryptography and Network Security, 2nd edition, McGraw-Hill.
[3] Stallings W (1999), Cryptography and Network Security, 2nd edition, Prentice Hall.
[4] William Stallings (2003), Cryptography and Network Security, 3rd edition, Pearson Education.
[5] “A Survey Paper on Type and Method of Cryptography Technique” Anuja Saykhede, Priya Raut and Jayshree Kaurase.
[6] ”Review and Recent Trends in Cryptography (2014), ”Vaishnavi Kannan Smita Jhajharia, Dr.Seema Verma.