11th International Conference on Researches in Science, Technology and Management
Osmania University Campus, Hyderabad (India) RSTM-18
11th March 2018 www.conferenceworld.in ISBN : 978-93-87793-05-7

AN APPROACH TO DATA SECURITY USING STRONG NUMBER AND MATRIX MULTIPLICATION

V. Harsha Shastri

Research Scholar, Dept. of CSE, Sunrise University, Alwar, Rajasthan, India

ABSTRACT

One of major issue in today's world is the data security while transferring the data from one place to another. We need to protect the data from unintended user. We can provide security for the data using cryptography. Encryption and decryption techniques are used at the sender and receiver side respectively. We use strong number while encrypting and decrypting the data. The proposed algorithm is simple there by making the implementation easier.

Keywords: cryptography, encryption, decryption, strong number, matrix multiplication

I.INTRODUCTION

Computer security rests on confidentiality, integrity and availability. In real world, secure data transmission is really difficult because of hackers. Cryptography is an art of science of secret writing. The term is derived from the Greek language krytos means secret and graphos means writing. It is the universal technique consisting of encryption and decryption processes that provide us secured data transmission. Encryption is the actual process of applying cryptography. Much of cryptography is math oriented and uses patterns and algorithms to encrypt messages, text, words and other form of communication. It has many uses especially in the areas of intelligence and military operations. Today security systems and companies use cryptography to transfer information over the internet. Simple encryption techniques can help uphold the privacy of any person.

II.CRYPTOGRAPHY

The most basic problem of cryptography is secure communication over an insecure channel. Cryptology encompasses both cryptography and cryptanalysis. Cryptography is the science of securing data while cryptanalysis is the science of applying and breaking secure information. Cryptography is based on message which is the plain text, encryption, decryption, keys and algorithms. The plain text is encrypted which cannot be understood by unauthorized person. Keys are used in encryption and decryption process and can be categorized as symmetric and asymmetric key. Symmetric key means there is one key used by both the parties. Asymmetric key uses two keys- one for encryption and the other for decryption. Plain text can be processed by algorithms in two ways- one by stream cipher and other by block cipher. Stream ciphers process text one character at a time, while the block ciphers process text as block and output a block.

There are two main steps involved in cryptography such as encryption and decryption. Encryption is the transformation of plain text into some unreadable form. Decryption is the reverse of Encryption; it is the transformation of encrypted data back into some readable form. The data to be encrypted is called as plain text. The encrypted data obtained as a result of encryption process is called as cipher text.

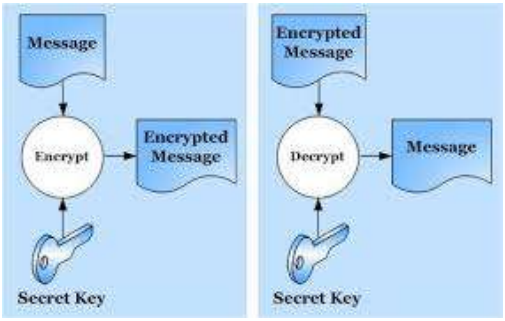

Figure 1: Encryption and Decryption Process

The statement X →Y : { Z } k means that entity X sends entity Y a message Z enciphered with key k The same or different key might be used for encryption and decryption depending on the situation. Here, we use same keys for both encryption and decryption. The various goals of cryptography are:

Authentication: It is the process of providing proof of identify of the sender to the recipient; so that the recipient can be assured that the person sending the information is who and what he or she claims to be.

Privacy/Confidentiality: it is the process of keeping the information secret so that the intended recipient can understand the information.

Integrity: information is not tampered during transit.

Non-repudiation: It is the mechanism to prove that the sender really sends this message.

III.TYPES OF CRYPTOGRAPHIC ALGORITHMS

Secret Key Cryptography- It uses single key for encryption and decryption. Eg: DES and AES

Public Key Cryptography- It uses two keys for encryption and decryption. They are public and private keys. Both the sender and receiver have the keys. It provides message integrity and authentication. Eg: RSA algorithm

Hash Function- It is based on the mathematical transformation to encrypt information which is irreversible. MD (Message Digest) Algorithm is an example.

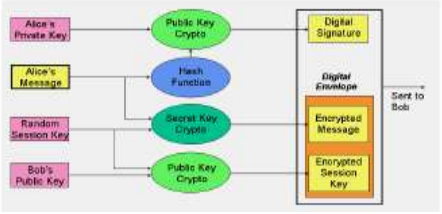

Figure 2: Types of Cryptographic Algorithms

I. Proposed System

In this system, we use strong number for encryption purpose. We define strong number as:

A strong number is the one in which it has the sum of the factorial of the individual digits is same as the original number. Eg: 145.

145 is strong number because: 1! +4! +5! =1+24+120=145.

We can have many receivers to whom the data can be sent. Initially each receiver is assigned a color value to identify the receiver by pre assigning a color.

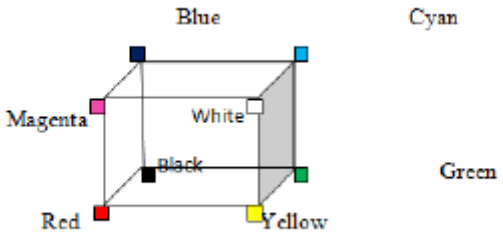

Figure 3: Color Model Representation

The following are the steps:

a. Encryption of the color is done by adding key values to the original color values at sender' side. This encrypted color acts as password.
b. Data is encrypted using strong number.
c. Decryption of the color takes place at receiver side when the receiver enters the private key.
d. The decrypted color is matched with the color assigned by the sender.
e. We find the ASCII values of the data which is added to the strong number used in matrix format (M).
f. Encoding matrix is formed (N).
g. Perform matrix multiplication of M and N matrices resulting in encrypted data.
h. Finally we have the decryption process.

Step 1: **Color Encryption**: Sender is aware about the receiver's color e.g. (110, 0,128). Let the key values (5,-2,-1) be added to the color which acts as password.

```
                    110   0    128
          +   5  -2      -1
              ------------------
              115   -2    127
              ------------------
```

The pair (115, -2, 127) acts a password.

Step 2**: Data encryption starts here as**:

Let the word be DATASECURITY which has to be encrypted. Take the ASCII values for each alphabet and add the strong number. Arrange the result in matrix format.

D	A	T	A	S	E	C	U	R	I	T	Y
68	65	84	65	83	69	67	85	82	73	84	89

Now add these numbers with the digits of
the strong number as follows:

Step 3: convert the above result into matrix format as:

$$M=\begin{bmatrix}69 & 66 & 68 & 74\\ 69 & 99 & 149 & 88\\ 89 & 94 & 207 & 94\end{bmatrix}$$

	68	65	84	65	83	69	67	85	82	73	84	89
+	01	04	05	01	16	25	01	64	125	01	04	05
	69	69	89	66	99	94	68	149	207	74	88	94

Step 4: Encoding matrix is as follows

$$N=\begin{bmatrix}1 & 4 & 5\\ 1 & 16 & 25\\ 1 & 64 & 125\end{bmatrix}$$

Step 5: perform the matrix multiplication as:

$$E=NxM=\begin{bmatrix}790 & 932 & 1699 & 896\\ 3398 & 4000 & 7627 & 3832\\ 15610 & 18152 & 35479 & 17456\end{bmatrix}$$

Now the encrypted data is sent to the receiver which is 790, 3398, 15610, 932, and 4000,18152,1699,7627,35479,896,3832,17456.

Step 6: Decryption process starts here by authenticating the receiver:

115 -2 127
- 5 -2 -1
---
110 0 128

Here the key value is subtracted from the pre-assigned password.

Step 7: decryption of encrypted data to get the original data as follows:

Decoded matrix Q= Inverse of encoded matrix N as N^{-1}

$$= \begin{bmatrix} 5/3 & -3/4 & 1/12 \\ -5/12 & 1/2 & -1/12 \\ 1/5 & -1/4 & 1/20 \end{bmatrix}$$

Step 8: Multiply the decoded matrix with the encrypted data as N^{-1} X E to get the original data.

$$M= \begin{bmatrix} 5/3 & -3/4 & 1/12 \\ -5/12 & 1/2 & -1/12 \\ 1/5 & -1/4 & 1/20 \end{bmatrix} X \begin{bmatrix} 790 & 932 & 1699 & 896 \\ 3398 & 4000 & 7627 & 3832 \\ 15610 & 18152 & 35479 & 17456 \end{bmatrix}$$

$$= \begin{bmatrix} 69 & 66 & 68 & 74 \\ 69 & 99 & 149 & 88 \\ 89 & 94 & 207 & 94 \end{bmatrix}$$

Step 9: Now read the values column wise as:

69, 69, 89, 66, 99, 94, 68, 149, 207, 74, 88, 94 and perform subtraction with the digits in the encoding matrix:

	69	69	89	66	99	94	68	149	207	74	88	94
-	1	4	5	1	16	25	1	64	125	1	4	5
	68	65	84	65	89	69	67	85	82	73	84	89

Now if we substitute the characters for the ASCII values we get our message.

IV.CONCLUSION

Cryptography has evolved from the ancient science to an important area of research to secure communications. It has evolved from substitution ciphers to quantum cryptography. This method provides a means and methods of hiding data, and establishing authenticity. Our proposed system uses three key values i.e., color key, receiver's key and strong number. We predict that this approach will be useful for secure data transmission.

REFERENCES

[1] AtulKahate ,"Cryptography and Network Security", Tata McGraw-Hill,2003.

[2] Higher Algebra(Abstract and Linear) – S.K.Mapa , Sarat Book House

[3] Duncan S. Wong, Hector Ho Fuentes and Agnes H. Chan, "The Performance Measurement of Cryptographic Primitives on Palm Devices",IEEE MILCOM 2001 Conference Proceedings, Oct 2001.

[4] AamerNadeem, Dr. M.Y.YounusJaved, "A Performance Comparison of Data Encryption Algorithms", 2005 IEEE.

[5] Gary C. Kessler," An Overview of Cryptography", McGrawHill, May 1998.

[6] Mathur, A., 2012. "A Research paper : An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms," 4(09): 1650-1657.

[7] Science, C. and S. Engineering, 2012. "Advance cryptography algorithm for improving data security, 1 1.,"

[8] Gitanjali, J., Dr.N. Jeyanthi, C. Ranichandra, M. Pounambal, 2014. "ASCII Based Cryptography Using Unique lD, Matrix Multiplication and Palindrome Number.".

[9] Singh, U. and U. Garg, 2013. "An ASCII value based text data encryption System," 3(11): 1-5

[10] Uddin, P., A. Marjan, N.B. Sadia and R. Islam, 2014. "Developing a Cryptographic Algorithm Based on ASCII Conversions and a Cyclic Mathematical Function," pp: 0-4.