IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-2, Issue-12 E-ISSN: 2347-2693

Data Security Through Armstrong Number and Colors

[1*]Ajisha John, [2]Keerthy.K.B, [3]Meenu Manoharan and [4]Diana Davis

[1*,2,3,4] Department of Information Technology
Jyothi Engineering College, Cheruthuruthy, Thrissur, Kerala, India

www.ijcaonline.org

Received: Nov/21/2014 Revised: Dec/02/2014 Accepted: Dec/16/2014 Published: Dec/31/ 2014

***Abstract*—**Data Security is the science and study of methods of protecting data from unauthorized disclosure and modification. As the technology advanced, there is need to secure data, transmitted over the network. To make secure data transmission, different methods are used. One of the techniques is Cryptography. Cryptography is the universal technique for secure data communication with the presence of third parties. In this method, encryption and decryption process is used to hide simple data from unauthorized users by converting it into unreadable form and again retrieve it in original form. This method not only protect data from theft, but also used for user authentication. Encryption and decryption have need of some secret information, called key.

***Keywords*—** Armstrong Numbers, Data Security, Authentication, Cryptography

I. INTRODUCTION

In this age of universal electronic connectivity, of viruses and hackers there is indeed no time at which security does not matter. The explosive growth in computer systems and their inter connections via networks has increased the dependence of both organisations and individuals on the information stored and communicated using these systems. This in turn, led to an awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages and to protect systems from network based attacks. The requirements of data security within an organisation have undergone drastic changes in the last several decades.

II. CRYPTOGRAPHY

Cryptography is the art and study of hiding information. It is a technique to convert plain text into cipher text. Cipher text is the message or data in unreadable format. Transformation of plain text into cipher text is done with the help of key. This process is called encryption process. Decryption is the reverse process of encryption [1]. The purpose of Encryption is to ensure privacy by keeping the information hidden from anyone for whom it is not intended. Encryption and decryption require the use of some secret information, called as key[1],[3].

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. There are various types of Cryptographic algorithms in use. They are categorized based on the number of keys used for encryption and decryption. The three types of algorithms used are:

Corresponding Author: Ajisha John, ajisha101@gmail.com

1. ***Secret Key Cryptography (SKC):*** Uses a single key for both encryption and decryption. The most common algorithms in use include Data Encryption Standard (DES),Advanced Encryption Standard (AES).

2. ***Public Key Cryptography (PKC):*** Uses one key for encryption and another for decryption. RSA (Rivest, Shamir, Adleman) algorithm is an example.

3. ***Hash Functions:*** Uses a mathematical transformation to irreversibly "encrypt"information. MD Message Digest[3]

III. PROPOSED SYSTEM

The existing techniques involve the use of keys involving prime numbers. In the proposed system, Armstrong numbers and colors are used. We can also use a combination of substitution and permutation methods to ensure data security. The substitution process is performed by assigning the ASCII equivalent to the characters. Permutation process is performed by using matrices and Armstrong number.

In this technique, the first step is to assign a unique color to each receiver. Each color is represented with a set of three values. For example violet red color is represented in RGB format as (238, 58,140). The next step is to assign a set of three key values to each receiver. The sender is aware of the receiver to whom the data has to be sent. So the receiver's unique color is used as the password[4]. The set of three key values are added to the original color values and encrypted at the sender's side. This encrypted color acts as a password. This is the authentication mechanism. The actual

data is encrypted using Armstrong numbers in the encryption process[1]-[3].

At the receiver's side, the receiver is aware of his own color and other key values(the sender sends it to the receiver). The encrypted color from the sender is decrypted by subtracting the key values from the received set of color values. Then it is tested for a color match, stored at the sender's database. Only when the colors are matched the actual data can be decrypted using Armstrong numbers. Using colors as a password ensures more security to the data providing authentication. Because only when the colors at both the sender and receiver's side match with each other the actual data can be accessed[3],[6].

Here, Encryption and Decryption process applies to both data as well as its key. So that two way security is provided to the application. After successful authentication, data is encrypted by random Armstrong number and at the same time that Armstrong number is get encrypted. For both these encrypted data and key, we can also attach current system timestamp(optional). So whenever receiver gets both the data he can easily recognize which key is for which data. The encrypted key is send to the receiver through any ways like Bluetooth, mail system etc[2]-[5].

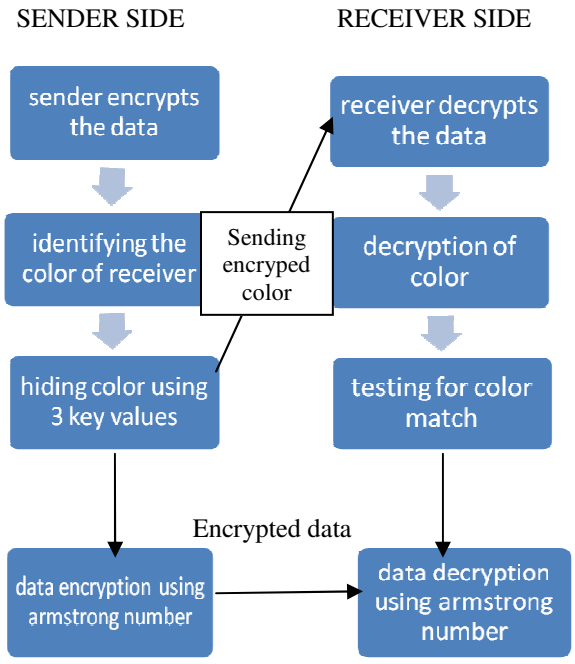

Fig 1: layout of proposed system

IV. ILLUSTRATION

ENCRYPTION

- Once the user is authenticated, now the sender sends the requested data to the receiver.
- Initially ASCII value for each character is found. Then Armstrong number is added to this ASCII value in an iterative manner until each character is assigned with the number.
- The resultant sum value is now converted into a matrix. Consider an encrypted matrix (Armstrong number), multiply it with the resultant sum matrix.
- The resultant matrix value consists of the encrypted data.

If we want to send the data, first we have to encrypt the color using following method.

STEP 1:

Now the sender is aware about receiver's color and to whom he wants to send the data. If receiver's color values are (238,58,140) and key values are (10,3,4) , at the time of encryption we add key values to original color values.

238 58 140 +
10 3 4

248 61 144

STEP 2:

Let the message to be transmitted is "TECSECURE".
First ASCII equivalent of TECSECURE is taken.
ie; 84 69 67 83 69 67 85 82 69.

STEP 3:

Add ASCII equivalent numbers with the digits of the Armstrong number as follows:

84 69 67 83 69 67 85 82 69+
3 7 1 9 49 1 27 343 1

87 76 68 92 118 68 112 425 70

STEP 4:

Convert the above data into matrix as follows:

$$A=\begin{pmatrix} 87 & 92 & 112 \\ 76 & 118 & 42 \\ 68 & 68 & 70 \end{pmatrix}$$

Step 5:

Encoding matrix is as follows:

$$B=\begin{pmatrix} 3 & 7 & 1 \\ 9 & 49 & 1 \\ 27 & 343 & 1 \end{pmatrix}$$

C=B * A

$$C=\begin{pmatrix} 861 & 1170 & 3381 \\ 4575 & 6678 & 21903 \\ 28485 & 8726 & 148869 \end{pmatrix}$$

The encrypted data is as follows:
861, 4575, 28485, 1170, 6678, 8726, 3381, 21903, 148869.

DECRYPTION

- The data which is encrypted and hidden is received at the receiver side. The data is now extracted.
- The inverse of the encoding matrix (Armstrong number) is found, and it is the decoding matrix.
- On receiving the encrypted data, the data is rearranged to the original order, which gives the correct order of the encrypted data.
- This data is arranged in matrix format and it is multiplied with the decoding matrix. The resultant value gives the ASCII value of the characters. Thus the data is decrypted and original data is found out.

STEP 1:
When the receiver want to read the data then he must be an authenticated user and for that he have to decrypt the encrypted color by subtracting the key values.

248 61 144 –
10 3 4

238 58 140

STEP 2:
Decryption of encrypted data to get original message is as follows: First obtain the inverse of encoding matrix.

$D=B^{-1}$

$$D=\begin{pmatrix} -7/24 & 1/3 & -1/24 \\ 1/56 & -1/42 & 1/168 \\ 7/4 & -5/6 & 1/12 \end{pmatrix}$$

STEP 3:
Multiplication of the decoding matrix with the encrypted data is as follows:

$$D*C=\begin{pmatrix} 87 & 92 & 112 \\ 76 & 118 & 425 \\ 68 & 68 & 70 \end{pmatrix}$$

Step 4:
Now transform the above result as given below.
87, 76, 68, 92, 118, 68, 112, 425, 70

Step 5:
Subtracting with the digits of the Armstrong numbers, we get:

87 76 68 92 118 68 112 425 70 –
3 7 1 9 49 1 27 343 1

84 69 67 83 69 67 85 82 69

V. ADVANTAGES OF PROPOSED SYSTEM

- This minimum key length reduces the efforts taken to encrypt the data. The key length can be increased if needed, with increase in character length.
- This technique could be considered as a kind of triple DES algorithm since we use three different keys namely the colors, key values added with the colors and Armstrong numbers

VI. HARDWARE AND SOFTWARE REQUIREMENTS

Processor	Pentium 3
Operating system	Windows 95/98/2000/XP
Front end	HTML, Java, Jsp
Application Server	Tomcat 5.0/6.X
Hard Disk	20 GB

VI.COMPARISON OF EXISTING AND PROPOSED SYSTEM

Parameters	Existing System	Proposed System
Numbers used for encryption	Prime numbers are used (AES, Triple DES etc.)	Armstrong numbers are used.

Authentication	Password	Color is used. Unique color acts as password.
Valid receiver	No validation after log in for message.	Validation after log in for message.
Security	Encoding and decoding the actual data.	The password itself is encoded for providing more security.
Encryption and Decryption	Encryption and Decryption with 1 or 2 digits Armstrong/prime number.	Encryption and Decryption with 3 digits Armstrong number

Fig 2: Comparison Table

ACKNOWLEDGMENT

We express our gratitude and thank to our Head of our Department Ms. Divya M Menon who have helped us a lot in the successful completion of initial phase of our project. We extend our gratitude and sincere thanks to our project coordinator Ms. Sabna AB who has always given her valuable time for us and also for her moral support. We remember the invaluable support offered by Ms.Diana Davis, our project guide and for her good suggestions and constant encouragement.

REFERENCES

[1] Gayatri Kulkarni , Pranjali Gujar, Madhuri Joshi, Shilpa Jadhav, "Message Security Using Armstrong Numbers and Authentication Using Colors" International Journal of Advanced Research in Computer Science and Software Engineering, January 2014

[2] S. Pavithra Deepa,S. Kannimuthu, V. Keerthika, "Security Using Colors and Armstrong Numbers", Proceedings of the National Conference on Innovations in Emerging Technology, February, 2011.

[3] S.Belose, M.Malekar, G.Dharmawat,"Data Security Using Armstrong Numbers", International Journal of Computer science and Engineering, April 2012

[4] Gordon L. Miller and Mary T. Whalen, "Armstrong Numbers", University of Wisconsin, Stevens Point, WI 54481,October 1990.

[5] M.Renuga Devi, S.Christobel Diana, "Enhancing Security in Message Passing Between Sender and Receiver Using Colors and Armstrong Numbers", International Conference on Computing and Control Engineering(ICCCE 2012) April 2012.

[6] Chavan Satish, Lokhande Yogesh, Shinde Pravin, Yewale Sandeep, Sardeshpande S. A, "Secure Email using Colors and Armstrong Numbers over web services", International Journal Of Research In Computer Engineering And Information Technology VOLUME 1 No. 2, March 2010.

