Undergraduate Academic Research Journal

Volume 1 | Issue 1 Article 19

July 2012

Data Security Using Armstrong Numbers

S. Belose
Department of Computer, Dnyanganga College of Engineering and Research; Pune, Maharashtra, India, shaileshbelose@gmail.com

M. Malekar
Department of Computer, Dnyanganga College of Engineering and Research; Pune, Maharashtra, India, mangesh7718@yahoo.com

S. Dhamal
Department of Computer, Dnyanganga College of Engineering and Research; Pune, Maharashtra, India, dhamal@yahoo.com

G. Dharmawat
Department of Computer, Dnyanganga College of Engineering and Research; Pune, Maharashtra, India, ganesh.dharmawat@gmail.com

N.J. Kulkarni
Department of Computer, Dnyanganga College of Engineering and Research; Pune, Maharashtra, India, nikitajkulkarni@yahoo.com

Data Security Using Armstrong Numbers

S.Belose, M.Malekar, S.Dhamal , G.Dharmawat & N.J.Kulkarni

Department of Computer, Dnyanganga College of Engineering and Research; Pune, Maharashtra, India
E-mail : shaileshbelose@gmail.com, mangesh7718@yahoo.com, sameer.dhamal@yahoo.com, ganesh.dharmawat@gmail.com, nikitajkulkarni@yahoo.com

Abstract **-** In the real world, it is difficult to transmit data from one place to another with security. To ensure secured data transmission, universal technique called cryptography is used, which provides confidentiality of the transmitted data. In this paper Encryption and decryption process uses Armstrong number which is referred as a secret key. To make the Authentication between two intended users along with the security, server is used. With the help of server, both sender and receiver will get validated. Then actual data could be transmitted by any of the means.

Keywords—*Armstrong numbers, data security, authentication, cryptography*

I. INTRODUCTION

Now days, to make secure data transmission different methods are used. One of the techniques is Cryptography, in this 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.

In existing system "Security Using Colors and Armstrong Numbers"[1] the first step is to assign a unique color for 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.

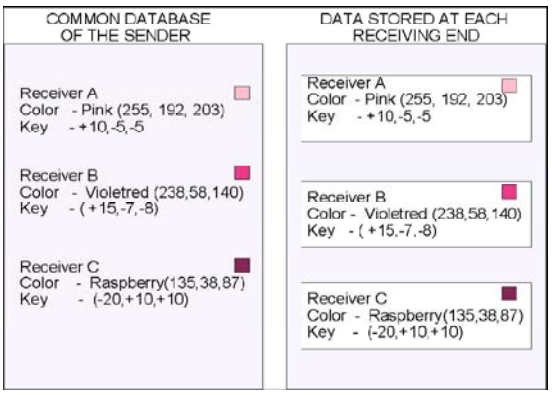

Fig 1: Data at Sender and Receiver ends.

The sender is aware of the required receiver to whom the data has to be sent. So the receiver's unique color is used as the password. The set of three key values are added to the original color values and encrypted at the sender's side. This encrypted color actually acts as a password. The actual data is encrypted using Armstrong numbers.

At the receiver's side, the receiver is aware of his own color and other key values. The encrypted color from the sender is decrypted by subtracting the key values from the received set of color values. It is then tested for a match with the color stored at the sender's database. Only when the colors are matched the actual data can be decrypted using Armstrong numbers. Usage of colors as a password in this way ensures more security to the data providing authentication. This is because only when the colors at the sender and receiver's side match with each other the actual data could be accessed.

In this paper, 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. Now for both these encrypted data and key current system timestamp is attached. So whenever receiver gets both the data he can easily recognize which key is for which data. Then encrypted key is decrypted by sender's public key and that resulted Armstrong number is used to decrypt actual data.

Here encrypted key is send to receiver through server and data is sent by any ways like Bluetooth, mail system etc.

So it is difficult to hack the data and steal it. Once hacker steals the data, then he must have key by which that data is encrypted with its same timestamp. If hackers get both data and key then he must know the decryption algorithm to retrieve both key and data which is very difficult.

II. CRYPTOGRAPHY

Cryptography, to most people, is concerned with keeping communications private. Encryption is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended. Decryption is the reverse of encryption; it is the transformation of encrypted data back into some intelligible form. Encryption and decryption require the use of some secret information, usually referred to as a key. 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. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different.

A. Types of Cryptographic Algorithms

There are several ways of classifying cryptographic algorithms. In general they are categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use as in [1]. The three types of algorithms are depicted as follows

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)

Algorithm is an example.

III. SERVER ARCHITECTURE

A Server is a computer or device on a network that manages network resources. For example, a file server is a computer and storage device dedicated to storing files Any user on the network can store files on the server.

Servers are often dedicated, meaning that they perform no other tasks besides their server tasks. On multiprocessing operating systems however, a single computer can execute several programs at once. A server in this case could refer to the program that is managing resources rather than the entire computer.

A. What is Server Platform?

A term often used synonymously with operating system. A platform is the underlying hardware or software for a system and is thus the engine that drives the server.

B. Types of server

1] FTP-Servers

One of the oldest of the Internet services, File Transfer Protocol makes it possible to move one or more files securely between computers while providing file security and organization as well as transfer control.

2] Mail-Servers

Almost as ubiquitous and crucial as Web servers, mail servers move and store mail over corporate networks via LANs and WANs and across the Internet.

3] Print-server

It is a computer that manages one or more printers and a network server is a computer that manages network traffic.

There are so many servers according to requirement like Audio/video, Chat, Fax, News, Proxy, Web servers etc.

IV. PROPOSED SYSTEM

A. Introduction

In proposed system instead of keeping sender and receiver database as color and key value we keep unique number and name on single common server. Before sending data authentication is done between sender and receiver. Then after successful authentication we carry our encryption process of data and send that data to receiver. And encryption key as Armstrong number is send via server to receiver

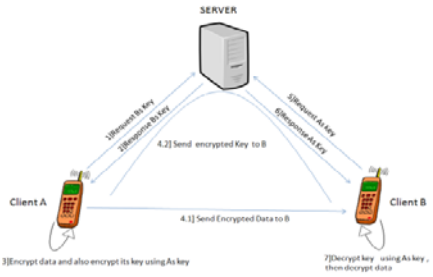

Fig 2. Server architecture

After getting encrypted key from server receiver decrypt that key using sender's key, and get original key using this key receiver decrypt actual encrypted data.

B. Illustration
1] Encryption:

Step 1 : Take random Armstrong Number and add its total digits like. (n=1+5+3=9). With the help of formula, form encoding matrix as below.

$$\begin{bmatrix} 8n^2+8n & 2n+1 & 4n \\ 4n^2+4n & n+1 & 2n+1 \\ 4n^2+4n+1 & n & 2n-1 \end{bmatrix}.$$

After calculation Encoding matrix is

720	19	36
360	10	19
361	9	17

Step 2: (Encryption of the actual data begins here)
Let the message to be transmitted be "ENCRYPT". First find the ASCII equivalent of the above characters.

E	N	C	R	Y	P	T	Extra	Extra
69	78	67	82	89	80	84	-25	-25

Step 3: Now add these numbers with the digits of the

Armstrong number Encrypted matrix as follows:

E	N	C	R	Y	P	T	Extra	Extra
69	78	67	82	89	80	84	-25	-25
+720	19	36	360	10	19	361	9	17
789	97	103	442	99	99	445	-16	-8

Step 4: Convert the above data into a matrix as follows:

A= 789	97	103
442	99	99
445	-16	-8

Step 5: Consider an encoding matrix...

B= 720	19	36
360	10	19
361	9	17

Step 6: After multiplying the two matrices (B * A) we get

C=54262	56951
48860	
27256	28495
24445	
27075	28534
24482	

The encrypted data is...

54262, 56951, 48860, 27256, 28495, 24445, 27075, 28534, 24482

The above values represent the encrypted form of the given message.

After storing this data into file it will be converted into byte array format as below:

-10, 119, -36, 120, 79, 125, -61, 118, -94.

2] Decryption:
Decryption involves the process of getting back the original data using decryption key.

Step 1:(Decryption of the original data begins here)
The inverse of the encoding matrix is:

D =	-1	1	1
	43363	-43508	-43216
	-21682	21755	21608

Step 2: Multiply the decoding matrix with the encrypted data

(C*D)

Step 3: Now transform the above result as given below:

789, 97, 103, -53830, -56733, -53405, 27581, 28400, 26872.

Step 4: Subtract with the digits of the Armstrong numbers as follows:

789	97	103	-53830	-56733	-53405	27581	28400	26872
+720	19	36	360	10	19	361	9	17
69	78	67	-54190	-56743	-53424	27220	28391	26855

Step 5: After converting the above data into byte array format and removing the extra parity bits we will get the original data.

69 78 67 82 89 80 84

Step 6: Obtain the characters from the above ASCII equivalent:

E	N	C	R	Y	P	T
69	78	67	82	89	80	84

V. ADVANTAGES

The above technique involves keys with a minimum key length which reduces the efforts taken to encrypt the data. The key length can be increased if needed, with increase in character length. This increases the complexity thereby providing increased security.

This technique ensures that the data transfer can be performed with protection since it involves two main steps. First step is to convert the characters into another form that means in ASCII values, Second step by adding with the digits of the Encoding matrix to form the required encrypted data.

Tracing process becomes difficult with this technique. This is because data is encrypted by key using Armstrong number and again this Armstrong number is encrypted by using As key. So it is more secure.

In this proposed technique encryption algorithm is to difficult to trace or hack externally.

REFERENCES

[1] "Security Using Colors and Armstrong Numbers" by S. Pavithra Deepa, S. Kannimuthu, V. Keerthika 1,3UG Student, Department of IT, Sri Krishna College of Engineering and Technology.

[2] "Introduction to algorithms" by Cormen, Leiserson, Rivest and Stein, Ch 28

[3] "ALGORITHM ANALYSIS AND COMPLEXITY CLASSES" Rayward-Smith, chapter 6), (Lewis & Papadimitriou, chapter 6)

[4] Public Key Cryptography Applications Algorithms and Mathematical Explanations Anoop MS, Tata Elxsi Ltd, India

[5] http://mathworld.wolfram.com/ UnimodularMatrix.html

❑❑❑