# Survey of Cryptography Techniques for Data Security

[1]Sonali B. Pawar, [2]Lina L. Tandel , [3]Priyanka K. Zeple,[4]Sachin R Sonawane
*[1 2 3]Department of Computer, Atharva College of Engineering Mumbai, Maharashtra, India*
*[4]Assistant Professor,Department of Computer Engineering, Atharva College of Engineering Mumbai, Maharashtra, India*
E-mail :sona.pawar14@gmail.com, lina.tandel123@gmail.com , zeple.priyanka@gmail.com

***ABSTRACT:*****Web has been converted into one complicated world. For Information transmission, internet is widely used, But Data Security is also concern in that case. While sending any sensitive data one must ensure about its integrity , confidentiality , authenticity. Cryptography is one Encryption technique. In his paper , Armstrong Numbers are used to provide more security to transmitted data. And for increasing password strength, color is used for authentication which is associated with set of 3 key values; hence authenticated persons only able to communicate in secure manner and also lowers the risk of data theft.**

***Keywords:*****Cryptography, Armstrong number, Color, Authentication, Data Security.**

## I. INTRODUCTION

Now days, to make secure data transmission different methods are used. Cryptography is the technique in this encryption and decryption process is used to hide simple data from unauthorized users by converting into unreadable form and again retrieve it in original form.

The main goal of Cryptography is access control and non-repudiation. 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. So it is difficult to hack the data.

### *A. RGB Representation-*

Any color is the combination of three primary colors Red, Green and Blue. A color is stored in acomputer in form of three numbers representing the quantities of Red, Green and Blue. RGB model uses 24 bits where each color uses 8 bit. Hence colors are used as a password for authentication purpose. There are about 16.7 million colors which are formed using the RGB.

### *B. Armstrong Number-*

Armstrong Number is n-digit number that is equal to the sum of the N th Power of its digits.
Example-

3^3+7^3+1^3 =1 + 343 + 27 = 371.[1]

## II. CRYPTOGRAPHY

Cryptography is the study of hiding data. Cryptography can be explained as hidden writing or secret writing. It is the process of sending and receiving a data in secret manner i.e. one person sends secret message to another person; the third person should not be able to read the data.

Cryptography can provide the service like integrity of the message and authenticity of the sender or receiver. The original data which is encrypted is known as plaintext whereas the encrypted data is known as cipher text.Applications of Cryptography: ATM cards, Computer Password, E-commerce.

## III. LITERATURE SURVEY

The use of public-key cryptography is in the information protection and privacy areas. Public key cryptography algorithms utilize prime numbers broadly because prime numbers are a crucial part of the public key systems.

This technique ensures that using two main steps data transfer can be performed with protected. In first step toconvert thegiven data into ASCII format, then add this ASCII numbers with Armstrong number digit.

Second step is to encode using a matrix to generate the required data encrypted. Tracking process becomes difficult with the help of this technique. This is because in each step the Armstrong number is used in different way.

Three different keys are used name as colors, a key value is adding with the colors and Armstrong numbers. Data can be retrieved when 3 key values along with known this technique.

Simple encryption and decryption techniques may just involve encoding and decoding the given data. But in the proposed technique the password itself is encoded to provide more security to the access of original data. Armstrong numbers and colors are used in this technique.[1], [7]

## IV. EXISTING SYSTEM

In the present world it is difficult to transmit data from one place to another with the help of security. This is important because of the hackers are becoming more powerful. To ensure securely transmission of the datathere are several techniques.

One of them is cryptography which is the study and practice of hiding information Encryption and decryption require the use of some secret information, referred to as a key. The data is to be encrypted is called as plain text.

The encrypted data get obtained as a result of encryption process is called cipher text. It depend on the encryption mechanism used, the same key is used for both encryption and decryption process. [4]

*Disadvantages of Existing System:*

1. More space is required on server side because of RSA.

2. As file size after encryption is 8 times by its actual size, hence execution speed decreases

3. The Brute force attack only way to break into this system, which also can take up to two or three years.

4. To protect the encryption, the minimum number of bits in n (n in RSA) should be 2048.

## V. PROPOSED SYSTEM

The existing techniques involve the use of keys involving prime numbers and the like. Hence in our proposed system we are using colors and Armstrong numbers. Further to ensure data security, we also use a combination of substitution and permutation methods. In the substitution process we perform assigning the ASCII equivalent to the characters. In Permutation process uses matrices as in and Armstrong number.

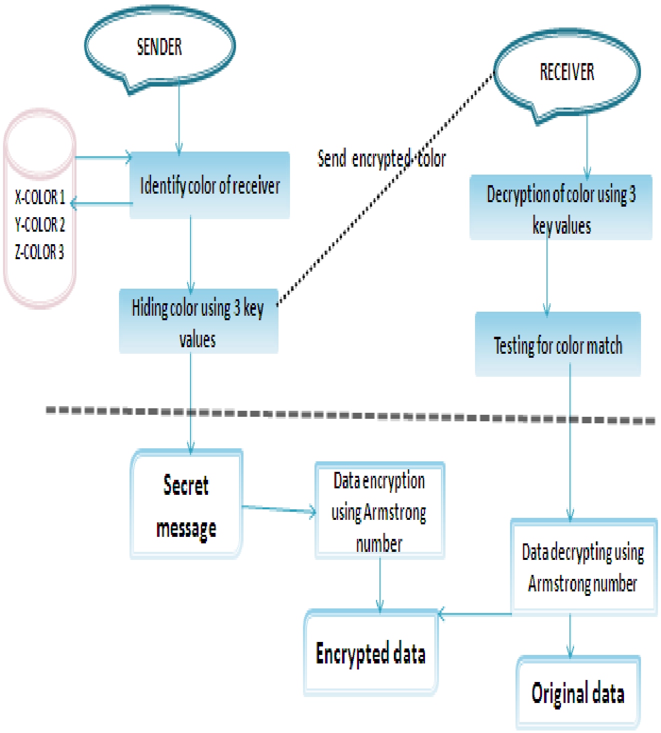
SENDER
RECEIVER
X-COLOR 1
Y-COLOR 2
Z-COLOR 3
Identify color of receiver
Send encrypted color
Decryption of color using 3 key values
Hiding color using 3 key values
Testing for color match
Secret message
Data encryption using Armstrong number
Data decrypting using Armstrong number
Encrypted data
Original data

Fig. 1 working of data in secure manner

In this technique the first step is for each receiver assign a unique color. Each color represented with a set of three values. For example brown color is represented in RGB format as (165, 42, 42). In next stepto each of the receiver assign a set of three key values. The sender is aware of the required receiver to whom the data has to be sent. So thereceiver's unique color is treating as the password. At the receiver's side, the receiver is aware of his own color and other key values.

A. *Illustration:*

Encryption Using Armstrong Numbers:Let the Armstrong number used for data encryption be 153.

Step 1: (Creating password)

User produces the key using Diffie-Hellman key exchange algorithm.

Step 2: (Encryption process begins here)

Let the message to be transmitted be "CRYPTOGRAPHY". Initially find the ASCII equivalent of the above characters.

C R Y P T O G R A P H Y
67 82 89 80 84 79 71 82 65 80 72 89

Step 3: Then add these numbers with the digits of the Armstrong number as follows

67 82 89 80 84 79 71 82 65 80 72 89
(+) 1 5 3 1 25 9 1 125 27 1 5 3
-------------------------------------------------------------------
68 87 92 81 109 88 72 20792 81 77 92

Step 4: Convert the data into a matrix as follows

$$A=\begin{pmatrix} 68 & 81 & 72 & 81 \\ 87 & 109 & 20 & 777 \\ 92 & 82 & 92 & 92 \end{pmatrix}$$

Step 5: Consider an encoding matrix

$$B=\begin{pmatrix} 1 & 5 & 3 \\ 1 & 25 & 9 \\ 1 & 125 & 27 \end{pmatrix}$$

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

$$C=\begin{pmatrix} 779 & 890 & 1383 & 742 \\ 3071 & 3598 & 6075 & 2834 \\ 13427 & 16082 & 28431 & 12190 \end{pmatrix}$$

The encrypted data is...

779, 3071, 13427, 890, 3598, 16082, 1383, 6075, 28431, 742, 2834, 12190

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

Decryption Using Armstrong Numbers: Decryption involves the process of getting back the original data using decryption key.

Step 1: (Authenticating the receiver) only when the keys from sender and receiver match, the following steps could be performed to decrypt the original data.

Step 2: (Decryption of the original data begins here) The inverse of the encoding matrix is

$$D= (1/240)*\begin{pmatrix} -450 & 240 & -30 \\ -18 & 24 & -6 \\ 100 & -120 & 2 \end{pmatrix}$$

Step3: Multiply the decoding matrix with the encrypted data

(D*C) we get

$$\begin{pmatrix} 68 & 81 & 72 & 81 \\ 87 & 109 & 207 & 77 \\ 92 & 88 & 92 & 92 \end{pmatrix}$$

Step 4: Now transform the result as given below

68 87 92 81 109 88 72 207 92 81 77 92

Step 5: Deduct with the digits of the Armstrong numbers as follows

68 87 92 81 109 88 72 207 92 81 77 92
(-) 1 5 3 1 25 9 1 125 27 1 5 3
-------------------------------------------------------------------
67 82 89 80 84 79 71 82 65 80 72 89

Step 6: Find the characters from the above ASCII equivalent

67 82 89 80 84 79 71 82 65 80 72 89
C R YP T O G R A P H Y

## VI. CONCLUSION

Thus, the issues related to security of messages are still a concern. There are several areas such as banking, military where data security has given more importance. Existing system includes combination of secret key and public key cryptography. Still more advanced cryptography techniques are needed for secure transmission of data.

## REFERENCE

[1] GayatriKulkarni, PranjaliGujar, Madhuri Joshi, Shilpa, " *Message Security Using Armstrong Numbers and Authentication Using Colors*", International Journal of Advanced Research in Computer Science and Software Engineering,1, January 2014

[2] S.Belose, M.Malekar, S.Dhamal ,G.Dharmawat&N.J.Kulkarni," *Data Security Using Armstrong Numbers*", Undergraduate Academic Research Journal (UARJ), 2012

[3] 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), 12 & 13 April, 2012

[4]S. PavithraDeepa, S. Kannimuthu, V. Keerthika," *Security Using Colors and Armstrong Numbers*', NATIONAL CONFERENCE ON INNOVATIONS IN EMERGING TECHNOLOGY, YEAR 2011

[5]PranjaliGujar,Madhuri Joshi,ShilpaJadhav,GayatriKulkarni,RanjeetsinghSuryawanshi," *Secure Message Using Armstrong Number and Authentication Using Colors*", International Journal of Innovative Research in Science,Engineering and Technology, march 2014

[6] Ajay Bansode, Amit Joshi, Awanish Singh,KiranGosavi," *Data Security in Message Passing using Armstrong Number*", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 2, Mar-Apr 2014

[7]G.Ananthlakshmi, S.Ramamoorthy "*A Multilevel Encryption Scheme for Secure Network Data Transfer*". International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012.