IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 10, October 2015.
www.ijiset.com
ISSN 2348 – 7968

Security of data based on Color and Armstrong number

Puja Maruti Lad[1], Yallawa Shivaji Vhankade[2],Ashwini Jagannath Khandagale[3] and Prajakta Ram Bhalerao[4]

Computer Science and Engineering,Pune University
H.S.B.P.V.T'S COE Kashti,
Tal:-Shrigonda,Dist:-Ahmednagar
Maharashtra,India.

[1] pujalad1994@gmail.com
[2] vhankaderence1992@gmail.com
[3] ashwinikhandagale123@gmail.com
[4] prajakta.bhalerao69@gmail.com

Abstract
Now a day's data security is the main issue. Confidentiality, integrity, non-repudiation, authentication, mainly comprises by the data security. The universal technique for contribute confidence of transmitted data is cryptography. I have implemented a novel approach to provide security and encryption of the data using a colors as the password and key involving Armstrong numbers. Secure data transmission are provided by the three set of keys with the as vital security element acted by the colors thereby providing authentication.

Keywords: *Armstrong numbers, data security, authentication, cryptography.*

1. Introduction

Today, different methods are used to make secure data transmission. One of the techniques is Cryptography. In Cryptography, the simple data is converted into in decipherable form and again get back it in original form using the encryption and decryption process. In existing system is the Security Using Armstrong Numbers with Color. In that the first step is to authorize a different color for each recipient. Set of three values represented with each color. For example In RGB format (238, 58,140) is represented by violet red color. In the next step a set of three key values are assign to each receiver. At Sender and Receiver ends the data is pre-sent. The sender know about the required receiver to which the data will have to send. So as the password, the receiver's unique color is used.
In the color value the set which has three key values are added and encrypted at the sender's side. As a password use this encrypted color. Using Armstrong numbers the actual data is encrypted. The receiver known his own color and key value. At the receiver's side, the key values are subtracted from actual color value and decrypt the encrypted color. Then receiver send that decrypted color send to the sender for matching. If that color match with senders color then using Armstrong number the actual data decrypted.
Cryptography, to most of people, is concerned with keeping communications private. The transforming the content into indecipherable form is the encryption. Its intension is to keep the information hidden from anyone which gives surety of privacy. The reverse process of encryption is the decryption; it is get the original information from the encrypted information. The secret information are used for both of these processes, usually called as a key. The plain text is the data to be encrypted. As a result of encryption process the encrypted data is obtained is called as cipher text. The same key is used for encryption as well as decryption, depending on the encryption mechanism, there may be different keys are used for encryption and decryption.
In this technique assign a unique color for each receiver is the first step. A set of three key values are represented with each color. i. e. RGB format as (238, 58,140) is represented by violet red color. In the next step to each receiver, assign a three key value's set.
The sender is known about the required receiver which has to send the data. So that as a password use the receiver's unique color. In the original color values the set of three col-or values are added and which are encrypted at the sender's side. Then as a password this encrypted color is use. Using Armstrong numbers the actual data is encrypted.
The receiver is familiar with his own color and also with other key values, at the receiver's side. Receiver subtract the key values from the color values to decrypt the encrypted color by sender. Then send that decrypted color for match to the sender. If the color get matched at sender side then only the actual data can be decrypted by using the Arm-strong number. The data providing authentication, use the color as a password to get the surety of some re-security. This is because the actual data could be

ISSN 2348 – 7968

accessed only when the colors at these receiver's side match with each other.

1.1. Types of Cryptographic Algorithms

The cryptographic algorithms classified by several ways. Depending on the number of keys are occupied for encryption as well as decryption, they are classified, and further describe by their application, there are three types of algorithms which are

1. Secret Key Cryptography (SKC)

In this algorithm for both encryption and decryption uses a single key.

Ex. Advanced Encryption Standard (AES), Data Encryption Standard (DES) .

2. Public Key Cryptography (PKC)

In this algorithm, uses different keys for encryption and decryption.

Ex. RSA (Rivest, Shamir, Adleman) algorithm.

3. Hash Functions:

To irreversibly "encrypt" information uses a mathematical transformation.

Ex. MD (Message Digest) algorithm.

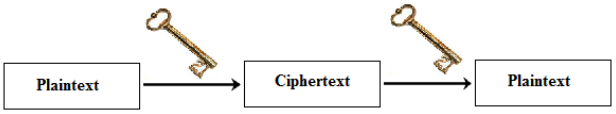


Figure 1. Secrete key (symmetric) cryptography

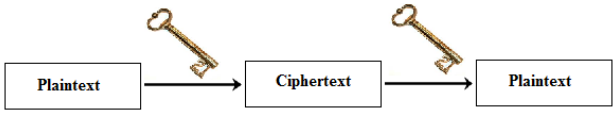


Figure 2. Public key (asymmetric) cryptography

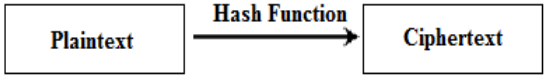


Figure 3. Hash Function (One way cryptography)

1.2. RGB Color Format

The red Green and Blue are the primary colors. And any color is formed by the combination of these three primary colors. Which are in fixed quantities. In a computer color is stored in the form of Red, Green and Blue by representing their quantities which is known as RGB representation. In the computer for storing the image in PDF, JPEG or BMP formats, the RGB representation is use. Values for Red, Green and Blue is represented by each pixel. Thus in the three dimensional RGB cube, any color can be uniquely represented as values of Red, Green and Blue.

To produce other colors, the values of Red, Green and Blue are merge together in different ways in the RGB color model. Many colors can be represented by using convenient merging of Red, Green and Blue intensities. Typically, to store a color pixel 24 bits are used in which 8 bits each for red, green and blue. For each hue, all these colors are presents in the range of 256 possible values. 16 777 216 (256^ 3 or 2^24) various combinations of intensity and hue can be specified with this system. acceptable.

2. Literature Survey

In the information protection the use of public-key cryptography is persistent and privacy areas. The prime numbers are a crucial part of the public key systems so that the prime numbers utilizes by public key cryptography algorithms broadly. This technique ensures that data transfer can be performed with protection using two main steps. In that first step is the convert the data into ASCII form, then by adding it with the Armstrong numbers digits. Second step is to generate the required encrypted data, encode it using a matrix. With this technique the tracing process becomes difficult. Because in each step by different ways the Armstrong number is used. Three different keys are used which are Armstrong numbers, key values added with the colors and the colors. If all the three key values along with this technique is known then only data can be retrieved. Encoding and decoding the actual data involve by Simple encryption and decryption techniques. But in this proposed technique to provide maximum security for accessing the initial information, the password itself is encoded. Armstrong numbers and colors are used in this technique. To whom the message has to be sent, the sender is known about the required receiver [1], [5]-[7].

3. Existing System

In today's world, Data security while transferring data from one place to other is major issue. To protection of data from unintended user Data security mainly refers. At senders and receiver side this technique uses encryption and decryption respectively. Especially while encrypting and decrypting the data this technique makes use of Armstrong number. For exchanging key between sender and receiver this technique also makes use of Diffie-Hellman key exchange algorithm. The proposed Algorithm is simple, flexible and making both hardware and software implementation easier.

To both data as well as its key, Encryption and Decryption process applies. So that to the application two way

ISSN 2348 – 7968

security is provided. After successful authentication, by random Armstrong number data is encrypted and Armstrong number gets encrypted at the same time. Now current sys-tem timestamp is attached, for both these encrypted data and key. So receiver can easily recognize which key is for which data whenever he gets both the data. Then by sender's public key encrypted key is decrypted and to decrypt actual data, that resulted Armstrong number is used.
So to hack the data it is difficult and steal it. Hacker must have key by which that data is encrypted with its timestamp once he steals the data. To retrieve both key and data, if hackers get both data and key then he must know the decryption algorithm which is very difficult.

3.1. Disadvantages

- Diffie-Hellman key exchange algorithm involves expensive exponential operations. The only way to break into this system is by Brute force attack, which also can take up to two or three years.
- The speed of execution is slow because the file size after encryption is much larger than original file.

4. Proposed System

All paragraphs must be indented. All paragraphs in the existing techniques there is the use of prime number and like for involving keys. Then the further step ahead in that we use Armstrong numbers and colors. For surety of information security, we also use a merging of permutation and substitution methods.

4.1. System Architecture

We assign the ASCII equivalent to the characters, this is the substitution process. Using matrices and Armstrong number the permutation process is complete. The first step of this technique is to appoint a different color for each and every receiver. Set of three values are represented with each color. For example in RGB format as (238, 58,140) is represented by violet red color. In the next step a set of three key values assign to each receiver. Common Database Of The Sender Data Stored At Each Receiving End.

Table 1.Data at sender and receiver ends.

Common Database Of The Sender	**Date Stored At Each Receiving End**
Receiver A Color-Pink(255, 192, 203) Key- (+10, -5, -5)	Receiver A Color-Pink(255, 192, 203) Key- (+10, -5, -5)
Receiver B Color-Violet red(238, 58, 140) Key- (+15, -7, -8)	Receiver B Color-Violet red(238, 58, 140) Key- (+15, -7, -8)
Receiver C Color-Raspberry(135, 38, 87) Key- (-20, +10, +10)	Receiver C Color-Raspberry(135, 38, 87) Key- (-20, +10, +10)

The sender is known about the required receiver. So that as a password use the receiver's unique color. The original color values are added with the set of three key values and then encrypted at the sender's side. Then as a password use this encrypted color. Then using Armstrong numbers actual data is encrypted.
The receiver is known his own color and also other key values at the receiver's side. At receiver side the receiver decrypt the color which is encrypted by the sender by subtracting the key values from the color value. Then it is matched with the color which is stored at the sender's database. The certain information decrypted with the help of Armstrong numbers only when the colors are matched.

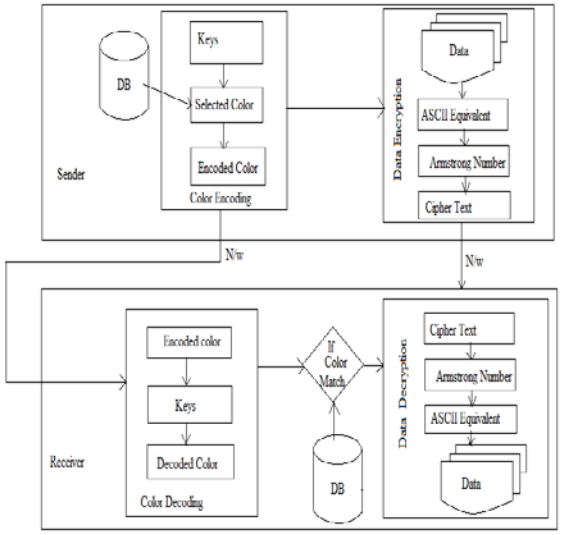


Figure 4. System Architecture

For surety of maximum security to the information providing, for authentication usage of colors as a password. This is because the actual data could be accessed after matching the colors at sender and receiver's side with each other.

4.2. Illustration

1. Encryption:
Assume that the information has to be sent to a receiver (say A) which the color (120, 35, 20) is assigned. Let with

ISSN 2348 – 7968

this color value the key value (10,3,4) to be added. And let the Armstrong number 153 be used for data encryption.

Step 1: (Password creation)

Initially the sender knows about the required receiver which is to be A. So that the some color values are appoint for receiver A, and the key values are added.

```
 120  35  20
+10   3   4
 ----------
 130  38  24          (1)
```

Now for security check, a newly encrypted color is designed.

Step 2: (Actual data Encryption)

Let the transmitted message be "SECURITYTECH". Then find ASCII equivalent values of the above all characters.

```
S  E  C  U  R  I  T  Y  T  E  C  H
83 69 67 85 82 73 84 89 84 69 67 72      (2)
```

Step 3: Now perform addition of the digits of the Armstrong number with these numbers as follows

```
 83  69  67  85 82 73 84  89 84 69 67 72
(+) 3   7   1   9  49  1  27 343  1  3  7  1
 ------------------------------------------------------------
 86 76 68 94 131 74 111 432 85 72 74 73      (3)
```

Step 4: Then, convert the above data into a matrix form as follows

$$A=\begin{bmatrix} 86 & 94 & 111 & 72 \\ 76 & 131 & 492 & 74 \\ 68 & 74 & 85 & 73 \end{bmatrix} \quad (4)$$

Step 5: Now, consider an encoding matrix...

$$B=\begin{bmatrix} 3 & 7 & 1 \\ 9 & 49 & 1 \\ 27 & 343 & 1 \end{bmatrix} \quad (5)$$

Step 6: Then, perform multiplication of two matrices (B X A) we get

$$C=\begin{bmatrix} 858 & 1273 & 3442 & 807 \\ 4566 & 7339 & 22252 & 4347 \\ 28458 & 47545 & 151258 & 27399 \end{bmatrix} \quad (6)$$

After multiplication, we get encrypted data which is,

858,4566,28458,1273,7339,47545,3442,22252,151258,807,4347,27399

The above values are the encrypted mode of original information.

2. Decryption:

The process retake original information back using decryption key is the decryption. Then sender's end data is matched with the data which is given by the receiver (the color). The receiver must be aware of the key values and his own color being assigned for this process.

Step 1: (The receiver Authentication)

The actual color being assigned is (120,35,20) for the receiver A (as assumed), the original color can get back by subtracting the key values from the color value.

The decryption process is as follow:

```
 130   38   24      Accepted data
-10    3    4      values of key
 ---------------------------------
 120   35   20                    (7)
```

The data stored at the sender's side, the above set of values (135, 38, 87) is compared. The original data can get back by performing following steps, only when they both match.

Step 2:(Original data Decryption)

Take the inverse of the encoding matrix

$$D=B^{-1}$$

$$D=\begin{bmatrix} -7/24 & 1/3 & -1/24 \\ \frac{1}{56} & -1/42 & 1/168 \\ 7/4 & -5/6 & 1/12 \end{bmatrix} \quad (8)$$

Step 3: Now perform multiplication of decoding matrix and the encrypted data matrix i. e. (D X C), we get

$$D \times C=\begin{bmatrix} 86 & 94 & 111 & 72 \\ 76 & 131 & 492 & 74 \\ 68 & 74 & 85 & 73 \end{bmatrix} \quad (9)$$

Step 4: Then the above result transform as given below

86 76 68 94 131 74 111 432 85 72 74 73

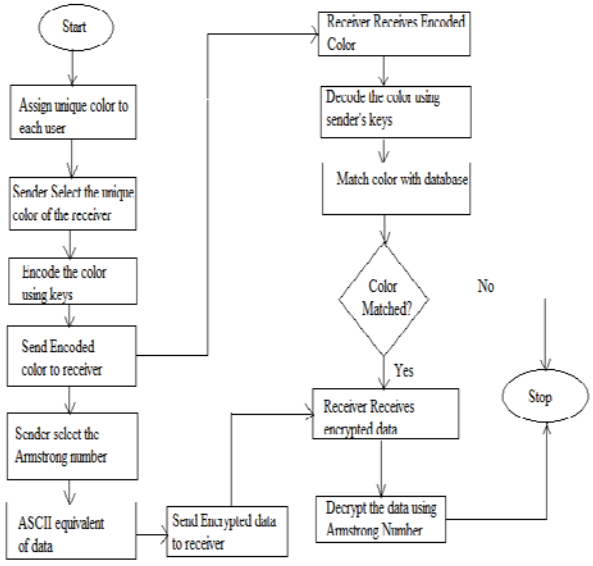
Step 5: Now, Subtract Armstrong numbers from the digits as follows

```
 86 76 68 94 131 74 111 432 85 72 74 73
(-) 3  7  1  9  49  1  27  343 1  3  7  1
 ------------------------------------------------------------
 83 69 67 85  82 73  84  89  84  69  67 72      (10)
```

Step 6: From the above ASCII equivalent obtain the characters

```
83 69 67 85 82 73 84 89 84 69 67 72
S  E  C U R  I  T  Y  T  E C  H.          (11)
```

4.3. Flowchart



ISSN 2348 – 7968

Figure 5. System Flowchart

4.4. Advantages

1. The above technique requires the minimum 8 bits of length key for Armstrong numbers. The efforts taken to encrypt the data are reduces this minimum key length. If needed the key length can be increased, with increase in the length of character. So that the complexity increases and hence, security gets increases.
2. This technique gives the surety that the data can be transfer with the protection since it consist of two main steps. First step is that, the character convert into another form after addition of it with the Armstrong numbers. In the second step, to form the required encrypted data, encode by using a matrix.
3. With this technique, tracing process becomes difficult. Because in each step the Armstrong number is used differently. If the total steps associated with the encoding process is known previous, then only key can be hacked.
4. We use three different keys which are key values added with the colors, Armstrong numbers and the colors, so that this technique could be treated as a kind of triple DES algorithm.
5. Until all the process of encryption and decryption as well as key values is not known the data cannot be obtained. So because of the usage of colors, hacking becomes difficult.
6. Encoding and decoding of the actual data involve by simple encryption and decryption techniques. But in this proposed technique for giving maximum security for original data access, the password itself is encoded.

4. Conclusions

In military, the above combination of public key and secrete key cryptography can be applied because, more importance is for security of data. When the length of the key of the Armstrong numbers increase, then this technique pro-vides more security. Thus by the use Armstrong numbers, additional set of key values and colors in this technique there is surety that the data is deliver securely and that only authorized peoples can access it contribution.

Acknowledgments

Authors would like to take this opportunity to express our profound gratitude and deep regard to our (Project Guide name), for his exemplary guidance, valuable feedback and constant encouragement throughout the duration of the project. His valuable suggestions were of immense help throughout our project work. His perceptive criticism kept us working to make this project in a much better way. Working under him was an extremely knowledgeable experience for us.

References

[1] S. Pavithra Deepa,S. Kannimuthu, V. Keerthika., “Security Using Colors and Armstrong Numbers”, Proceedings of the National Conference on Innovations in Emerging Technology-2011. India.17 & 18 February, 2011.pp.157-160.
[2] Gordon L. Miller and Mary T. Whalen, “Armstrong Numbers”, University of Wisconsin, Stevens Point, WI 54481 (Submitted October 1990).
[3] S.Belose, M.Malekar , G.Dharmawat, “Data Security Using Armstrong Numbers”, International Journal of Emerging Technology and Advanced Engineering. Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 4, April 2012).
[4] M.F.Armstrong “A brief introduction to Armstrong Numbers”
[5] 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.
[6] 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
[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.
[8] Atul Kahate, “Cryptography and Network Security”, Tata McGraw Hill Publications
[9] http://aix1.uottawa.ca/~jkhoury/cryptography.html