Volume 4, Issue 1, January 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Message Security Using Armstrong Numbers and Authentication Using Colors

Gayatri Kulkarni*, Pranjali Gujar, Madhuri Joshi, Shilpa Jadhav
Computer Department
Pune University, India

Abstract— We are living in the information age. Hence data security plays an important role. Hackers are becoming more active nowadays. Hence it is increasingly becoming more important to protect our data. There are some techniques used to make data transmission with protection. Cryptography is one of them. This paper provides a technique in which Armstrong number is used for encryption of message. Color is important in authentication process as it acts as password. Using this technique, message is hidden from unauthorized people and accessible to an authorized individual when required.

Keywords— Data security, Armstrong numbers, Authentication, Cryptography, Colors, Unimodular matrix

I. INTRODUCTION

In real world, data security is very important where importance is given to the confidentiality, authentication and integrity. Secure data transmission is really difficult because of the hackers. Cryptography is the universal technique for providing security to confidential data. The main goals of cryptography are access control and non- repudiation. It consists of encryption and decryption processes. Encryption and decryption have need of some secret information, usually referred to as a key. The same key might be used for both encryption and decryption depending on the encryption mechanism. While for other mechanisms, the keys used for encryption and decryption might be different.

A. RGB representation

Any color is the mixture of three colors RGB (Red, Green and Blue) in preset quantities. This is nothing but a RGB representation. Here values for Red, Green and Blue represent each pixel. So any color can be individually represented with the help of three dimensional RGB cube. RGB model uses 24 bits, 8 bits for each color. Hence colors are used as a password for authentication purpose. Then encryption or decryption process takes place.

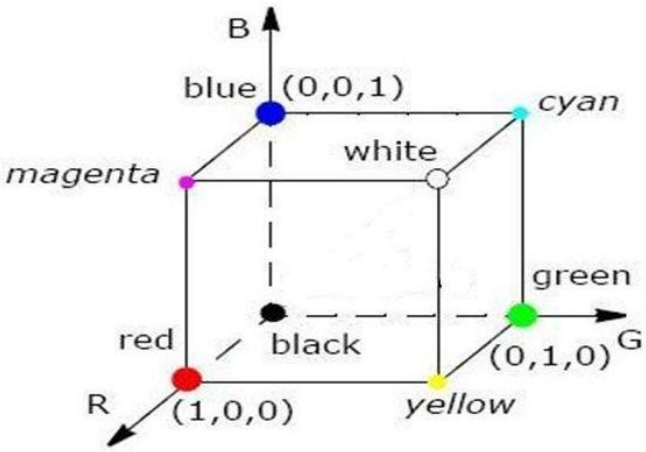

Fig 1 RGB Color Model

B. *Armstrong number*

An Armstrong number is an n-digit base m number such that the sum of its (base m) digits raised to the power n is the number itself. Hence 371 is an Armstrong number because $3^3+7^3+1^3 = 1 + 343 + 27 = 371$. [2],[4]

II. CRYPTOGRAPHY

Cryptography is the art and study of hiding information i.e. 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 it can be secret key or public key. This process is nothing but an encryption process. Decryption is the reverse process of encryption in which cipher text is converted back into plain text (Original message) again with the help of key. [8]

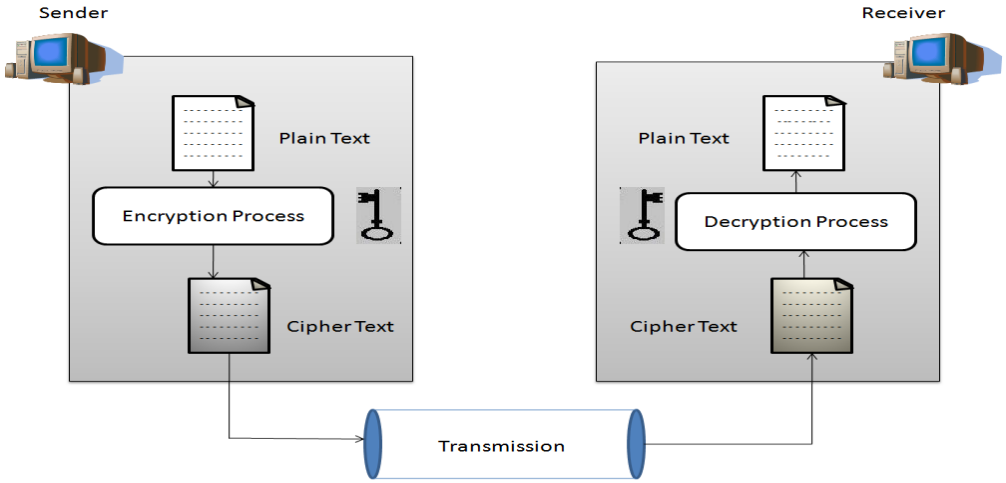

Fig 2 Cryptographic Technique

III. LITERATURE SURVEY

The use of public-key cryptography is persistent 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 protection. First step is to convert the data into ASCII form, then by adding with the digits of the Armstrong numbers. Second step is to encode using a matrix to generate the required encrypted data. Tracing process becomes difficult with this technique. This is because in each step the Armstrong number is used in different way. Three different keys are used namely the colors, key values added with the colors and Armstrong numbers. Data can be retrieved only if all the three key values along with this technique is known. Simple encryption and decryption techniques may just involve encoding and decoding the actual data. But in this 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. The sender is attentive of the required receiver to whom the message has to be sent. [1],[5]-[7]

IV. EXISTING SYSTEM

There are many algorithms for encryption decryption process like AES, DES, RSA in which encryption is done with the help of substitutions and transformations on the plaintext. It uses prime numbers for encryption process.

A. *Cryptography using secret key (SKC):* Secret key is a value independent of a plaintext and of the algorithm. Single key is used for both encryption and decryption by an algorithm. It includes Data Encryption Standard (DES) and Advanced Encryption Standard (AES).

B. *Cryptography using Public Key (PKC):* Two different keys are used in this. One key is used for encryption and another for decryption. It includes Rivest, Shamir, Adleman (RSA) algorithm.

C. *Hash Functions:* It uses mathematical transformation for encryption which is not recoverable from the cipher text.

V. PROPOSED SYSTEM

In proposed system Armstrong numbers are used for encryption purpose while existing system uses prime number. Color is used for authentication purpose. Basic concept is that unique color is assigned to each receiver. This unique color acts as password. The sender knows required receiver to whom the data has to be sent. There can be N numbers of receivers who can access the encrypted data if they are authorized ($N \leq 2^{24}$). Firstly, encryption of color is done by adding key values to the original color values at sender's side. This encrypted color acts as a password. Then data is encrypted using Armstrong numbers. At the receiver's side when the receiver enters secret key, decryption of color takes place. The decrypted color is then matched with color assigned by sender i.e. original color stored at the sender's database. Without the secret key, there is no way for user to access the data.

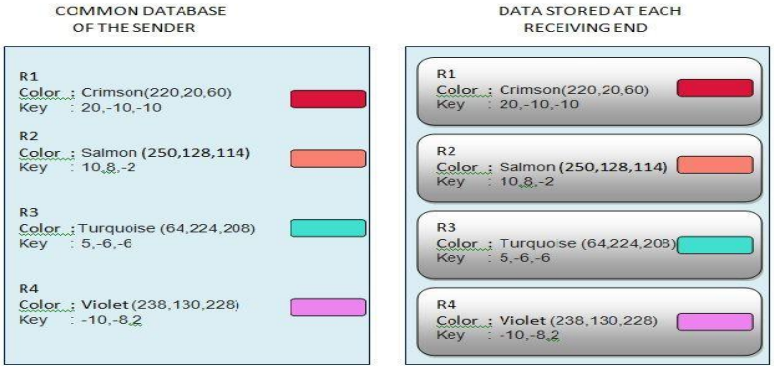

Fig 3 Data At Sender And Receiver's End

Further a combination, substitution and permutation methods are used with Armstrong number to ensure data security. S For encryption it converts each letter to its ASCII equivalent by substitution method and permutation is done with the help of Armstrong number. Later it convert that data into matrix form.It performs permutation process by using matrices [9]. Receiver will perform in reverse manner.

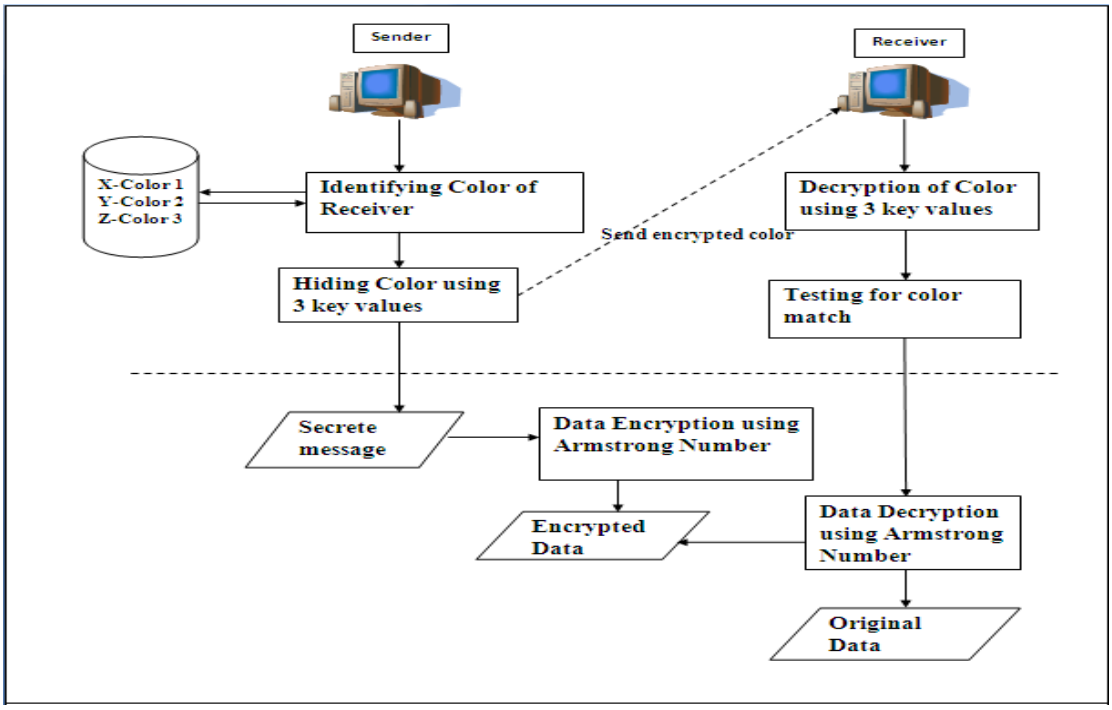

Fig 4 Layout of proposed technique

A. Illustration

(Color encryption)

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

Now sender is aware about receiver's color and to whom he wants to send the data. If receiver's color values are (120, 35 ,20) and key values are (10,3,4) So at the time of encryption we add key values to original color values

120 35 20
+10 3 4
130 38 24

Step 2: (Encryption of the actual data)

Let the message to be transmitted be "SECURITYTECH".

First ASCII equivalent are taken of the above 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

Step 3: Add ASCII equivalent numbers with the digits of the Armstrong number 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

step 4:Convert the above data into matrix as follows

$$A=\begin{pmatrix} 86 & 94 & 111 & 72 \\ 76 & 131 & 492 & 74 \\ 68 & 74 & 85 & 73 \end{pmatrix}$$

step 5:Encoding matrix is as follows

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

C=B X A

$$C=\begin{pmatrix} 858 & 1273 & 3442 & 807 \\ 4566 & 7339 & 22252 & 4347 \\ 28458 & 47545 & 151258 & 27399 \end{pmatrix}$$

The encrypted data is as follows

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

Decryption process starts here,

Step 1: Authenticating the receiver

Color is used for authentication purpose only. When receiver want to read the data then he must be authenticated user and for that he have to decrypt the encrypted color using following method by subtracting key values.

130 38 24
-10 3 4
---120 ----35 ----20 ----

Step 2: Decryption of encrypted data to get original message is as follows:

First obtain the inverse of encoding matrix.

$D=B^{-1}$

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

Step3: Multiplication of the decoding matrix with the encrypted data is as follows

D X C=

$$\begin{pmatrix} -7/24 & 1/3 & -1/24 \\ 1/56 & -1/42 & 1/168 \\ 7/4 & -5/6 & 1/12 \end{pmatrix} \begin{pmatrix} 858 & 1273 & 3442 & 807 \\ 4566 & 7339 & 22252 & 4347 \\ 28458 & 47545 & 151258 & 27399 \end{pmatrix}$$

$$= \begin{pmatrix} 86 & 94 & 111 & 72 \\ 76 & 131 & 492 & 74 \\ 68 & 74 & 85 & 73 \end{pmatrix}$$

Step 4:Now transform the above result as given below

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

Step 5: Subtracting with the digits of the Armstrong numbers

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

Step 6: Obtain the ASCII equivalent characters of above data

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

B. ***Special case***

There may occur a situation in which Armstrong number contains zero as one of the digit of number. In such case inverse of matrix cannot be found. In such case we can use Unimodular matrix. [3], [10]

VI. CONCLUSION

Thus we addressed the problem of security of secret message. Hence a technique is proposed in which Armstrong numbers are used instead of prime numbers to provide more security. The confidential areas like military, governments are targeted by the system where data security is given more importance. Colors, key values and Armstrong numbers which are three set of keys in this technique makes sure that there is secured message or data transmission and is available to authorized person.

ACKNOWLEDGEMENT

It is our pleasure to express our sincere gratitude to Trinity College of Engineering and Research, Pune for providing us an opportunity to do our work on Paper. We sincerely thank to our project guide Prof.Ranjeetsingh Suryawanshi for guidance and encouragement in carrying out this paper work. We will forever remain grateful for constant support by guide, in making this paper.

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.htm

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

