ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

Secure Message Using Armstrong Number and Authentication Using Colors

Pranjali Gujar[*1],Madhuri Joshi[*2],Shilpa Jadhav[*3],Gayatri Kulkarni[*4],Ranjeetsingh Suryawanshi[*5].

U.G.Student, Department Of Computer Engineering, Trinity College of Engg.& Research,Pune, Maharashtra,India [1]

U.G.Student, Department Of Computer Engineering, Trinity College of Engg.& Research,Pune,Maharashtra,India [2]

U.G.Student, Department Of Computer Engineering, Trinity College of Engg.& Research,Pune, Maharashtra,India[3]

U.G.Student, Department Of Computer Engineering, Trinity College of Engg.& Research,Pune, Maharashtra,India[4]

Assistant Professor, Department Of Computer Engg., Trinity College of Engg. & Research, Pune, ,Maharashtra,India [5]

Abstract: We are living in the information age. Information is an important asset, like other assets, it has value to various organization and need to be suitably protected. Hence data security plays an important role. Hackers are becoming more active nowadays. Hence it is increasingly becoming more important to protect our confidential data. There are some techniques for secure data communication with presence of third parties. Cryptography is one of them. This paper provides a technique in which Armstrong number is used for encryption of message. Three set of keys provide more security when data is transmitted. Color acts for the process of authentication.

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

I. INTRODUCTION

In real world, data security plays vital role where importance is given to the security goals- confidentiality, authentication and integrity. Secure data transmission is really difficult because of the hackers. Cryptography is the universal technique for secure data communication with the presence of third parties. This technique not only protect data from theft, but also used for user authentication. 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. [11]

II. BACKGROUND STUDY

The original message called plaintext is converted into random text called cipher text. The science and art of manipulating messages to make secure is called cryptography. Public key cryptography algorithms utilize prime numbers broadly because prime numbers are a crucial part of the public key systems. This paper considers a technique in which Armstrong numbers and colors are used. The sender is attentive 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. They are encrypted at the sender's side. [1],[5]-[7].

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

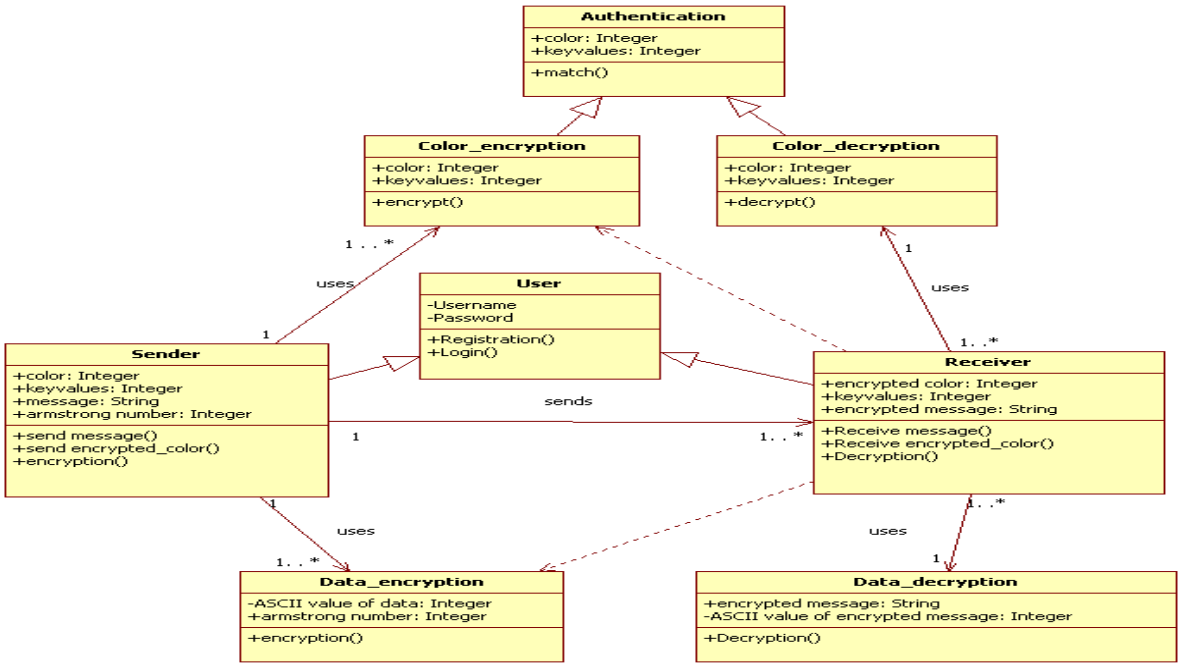

Fig.1 Schema

Steps of Algorithm

1) Encryption**:**

Let us assume that sender has to send a message to receiver.

1. Initially key values are added with the color values which are assigned for the receiver.
2. To encrypt the actual message, that message has to be converted into ASCII equivalent of those characters.
3. The digits of Armstrong numbers are added with the ASCII equivalents.
4. The above data is converted into matrix form.
5. This matrix is multiplied with the encoding matrix.
6. After multiplication we get the encrypted format of the message.

2) Decryption:

The original data gets back because of decryption process.

1. The authentication of the receiver is done.
2. The inverse of the encoding matrix is done to decrypt the original data.
3. The decoding matrix is multiplied with the encrypted data.
4. The numbers in above matrix are the digits of armstrong numbers.
5. The ASCII equivalents are obtained from the numbers.

III. IMPLEMENTATION

While creating account user has to enter valid username and password and select the color from color picker which is used for authentication purpose. The RGB values of that color will be shown. Then these values along with name are saved in sender's database.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

Fig.2 Form for creating account.

When sender wants to send the data to receiver, there is no need to remember RGB color of receiver. So at the time of sending system provides contact list of receiver along with their RGB values. So sender can able to recognize the user or receiver whom he wants to send the data. Following figure describe the GUI of contact list.

Fig.3 Form for list of receivers.

IV. RESULT

The comparative study between existing system and proposed system shown in following table specifies us the advantages of proposed system.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

Table 1

Parameters	Existing System	Proposed System
Number	Prime numbers are used for encryption purpose (AES, Triple DES etc.)	Armstrong numbers are used for encryption purpose.
Authentication	Password.	Color is used for authentication purpose. This unique color acts as password.
Valid receiver	No validation after log in for message.	Validation after log in for message.
Security	Encoding and decoding actual data.	The password itself is encoded for providing more security along with data.
Encryption and Decryption	Encryption and Decryption with 3 digits Armstrong number.	Encryption and Decryption with 4 digits Armstrong number.

Strength of Algorithm:

Colors are used for the authentication purpose. The range of color is 2^0 to 2^{24}. RGB model uses 24 bits, 8 bits for each color. To encrypt the data set of three key values are added to the original color values. This encrypted color acts as a password. To break this password attacker has to check 256^3 possible values which are practically most difficult. Combination of substitution and permutation process increases the data security. To increase the strength of algorithm 4 digits Armstrong number is used for encryption and decryption, length of an Armstrong number can be increased if necessary for security purpose.

V.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 Principal, H.O.D Computer Department, guide, project co-ordinator Prof.Anup Raut in making this paper.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

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

[11] 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. Website:www.ijarcsse.com (ISSN: 2277 128X,Volume 4, Issue 1, January 2014)