Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.92 – 98

SURVEY ARTICLE

A Survey on Different Techniques for Message Security and Authentication in Offline Chatting

[1]Neha Khodke, [2]Shivangi Deshpande, [3]Payal Tote, [4]Trupti Ghumade

Department of Computer Engineering, B.D.C.O.E., R.T.M.N.U., Wardha, India

[1] nehakhodke77@gmail.com, [2] shivangideshpande111@gmail.com, [3] payaltote20@gmail.com, [4] truptig002@gmail.com

Abstract— In today's world scenario, data security plays an important role where importance is given to authentication, confidentiality, integrity and non repudiation. The universal technique to providing confidentiality of transmitted data is cryptography. Here we use group key management (GKM) in mobile communication where it is important to enable access control for a group of users. In GKM, a major issue is how to minimize the communication cost for group rekeying. While designing the optimal GKM, researchers have assumed that all group members have the same leaving probabilities and that the tree is balanced and complete to simplify analysis. These assumptions are impractical and may lead to a large gap between the impractical analysis and the measurement in real-life situations, thus allowing for GKM schemes to incorporate only a specific number of users. A new GKM framework supporting more general cases that do not require these assumptions. In which Armstrong number is used for cryptography process. In authentication process color is important which acts as password.

Keywords- Armstrong Numbers, Authentication, Batch Rekeying Cryptography, Data Security, Group Dynamics, Group Key Management, Integrity, Logical Key Hierarchy, Multicast, Non-Repudiation

I. Introduction

In next-generation mobile communication, multicast Service will be a key application for supporting a large group of subscribers simultaneously. As multicast transmits data to the group simultaneously, it reduces the communication cost significantly. However, since multicast may be vulnerable to an overhearing attack, this efficiency can be achieved only when security or access control is guaranteed; i.e., only authorized group members can read the data. Many commercial applications such as Pay TV, vehicular ad hoc network (VANET), and group signature require that only legal users have access authority. Nowadays, Smart phones are becoming popular; many mobile applications which need group communication such as DMB, video conference, and online game have emerged. For both security and efficiency Cryptography is the universal technique for providing security to confidential data. Cryptography is the science and art of transforming messages to make them secure and immune to attack. Cryptography has many commercial applications. Suppose we are protecting confidential information, cryptography provides high level of privacy of individuals and groups. There are two main steps involved in cryptography such as encryption and decryption. Encryption is the transformation of plain text into some unreadable form. Decryption is the reverse process of encryption that is transformation of encrypted data back into some readable form. The encrypted data is called as plain text. Then the encrypted data obtained as a result of encryption process is called as cipher text. Then the transmitted message can be decrypted by only group members having the GK. However, the GK is updated whenever the group membership changes for

forward and backward secrecy, which can cause a serious problem with rekeying overhead. Hence, many researchers have proposed variations of group key management(GKM), and have attempted to reduce the overhead for group rekeying.

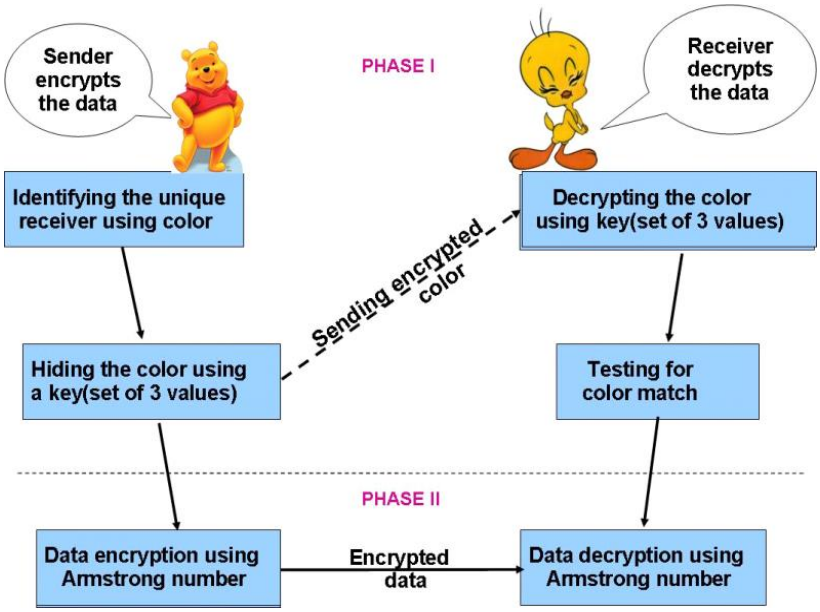

Fig 1. Layout of the proposed technique

II. LITERATURE SURVEY

Pranjali Gujar and Gaytri Kulkarni provided a technique in which Armstrong number was used for encryption of message. Color was important in authentication process as act as password.

Ajay Bansode and Amit Joshi provided use of Armstrong number while encrypting and decrypting the data. This also made the use of Diffie-Hellman key exchange algorithm for exchanging key between sender and receiver.

Madhuri Joshi and Shilpa Jadhav provided a technique in which Armstrong number was used for encryption of message.

Three set of keys provides more security when data is transmitted.

Shakera Shaikh and Veena Gulhane provided a User Authentication (UA) scheme for Wireless Sensor Networks (WSNs), which employed RGB color cube Algorithm and Armstrong number for data security.

M. Renuga Devi, S. Christobel Diana provided a technique to encrypt the data using a key involving Armstrong numbers and colors as the password. The key was passed between the Sender and the receiver by using Diffie Hellman key exchange algorithm.

S. Pavithra Deepa and S. Kannimuthu provided a technique to encrypt the data using a key involving Armstrong numbers and colors as the password. Three set keys were used to provide secure data transmission with the colors acting as vital security element thereby providing authentication.

A. Revathi and Dr. Paul Rodrigues addressed the growth of secure group communications over a decade.

Sr. No.	Name of Title	Name of Author	Year	Descriptions
I.	Message Security Using Armstrong Numbers and Authentication Using Colors	Gayatri Kulkarni, Pranjali Gujar, et al.	Jan-2014	Armstrong and RGB Color
II.	Data security in message passing using Armstrong number	Ajay bansode, amit joshi, et al.	Mar-Apr-2014	Diffie-Hellman key exchange algorithm
III.	Secure Message Using Armstrong Number and Authentication Using Colors	Madhuri Joshi, Shilpa Jadhav, et al	Mar-2014	Armstrong number and Color.
IV.	Survey on Secure Group Communication and Applications	A. Revathi Dr. Paul Rodrigues	June-2014	Forward Secrecy Backward Secrecy Collision Resistance
V.	User Authentication using Colors and data security using Armstrong numbers for Wireless Sensor Networks	Shakera Shaikh, Veena Gulhane	June-2012	RGB color cube Algorithm and Armstrong Number
VI.	Enhancing Security in Message Passing Between Sender and Receiver Using Colors and Armstrong Numbers	M. Renuga Devi, S. Christobel Diana	April-2012	Diffie Hellman key exchange algorithm
VII.	Security Using Colors and Armstrong Numbers	S. Pavithra Deepa, S. Kannimuthu	Feb-2011	Three set of keys are used to provide secure data transmission

Table I. Comparison of different techniques

III. PROPOSED WORK

In proposed system Armstrong numbers are used for encryption purpose while existing system uses prime number. Color is used for authentication purpose. Main 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, where encrypted color acts as a password. Then this data is encrypted using Armstrong numbers. When the receiver enters secret key at the receiver's side, decryption of color takes place. Then that decrypted color is 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. 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 converts that data into matrix form and it performs permutation process by using matrices. Receiver will perform in reverse manner. Our framework consists of two algorithms: one for initial construction of a basic key-tree and another for optimizing the key-tree after membership changes. The first algorithm enables the framework to generate an optimal key-tree that reflects the characteristics of users' leaving probabilities, and the second algorithm allows continual maintenance of communication with less overhead in group rekeying. Through simulations, we show that our GKM framework outperforms the previous one which is known to be the best balanced and complete structure.

A. *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 153 is an Armstrong number because $1^3+5^3+3^3=1+125+27=153$

B. *RGB Representation*

Any color is the mixture of three colors RGB (Red, Green and Blue) in fixed quantities. This is nothing but a RGB representation. It represents values for Red, Green and Blue represent each pixel. Therefore any color can be individually represented with the help of three dimensional RGB cube and RGB model uses 24 bits, 8 bits for each color. Therefore, in our approach we make use of colors whose values serve as a password for initial authentication and encryption decryption process.

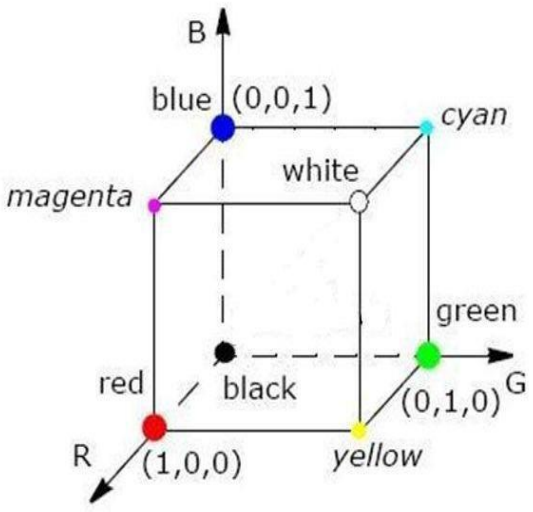

Fig. 2 RGB Color Model

This figure shows the architectural diagram of proposed system which consist of various parts such as Group Controller, Server and Mobile users.

Fig .3 Model of Multicast Environment

IV. DIFFERENT ALGORITHMS

There are many algorithms for encryption decryption process like DES, AES, RSA in which encryption is done with the help of substitutions and transformations on the plaintext, which 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, and Adleman (RSA) algorithm.

C. *Hash Functions:*

To preserve the integrity of message, the message is passed through the algorithm called a hash function. It uses mathematical transformation for encryption which is not recoverable from the cipher text.

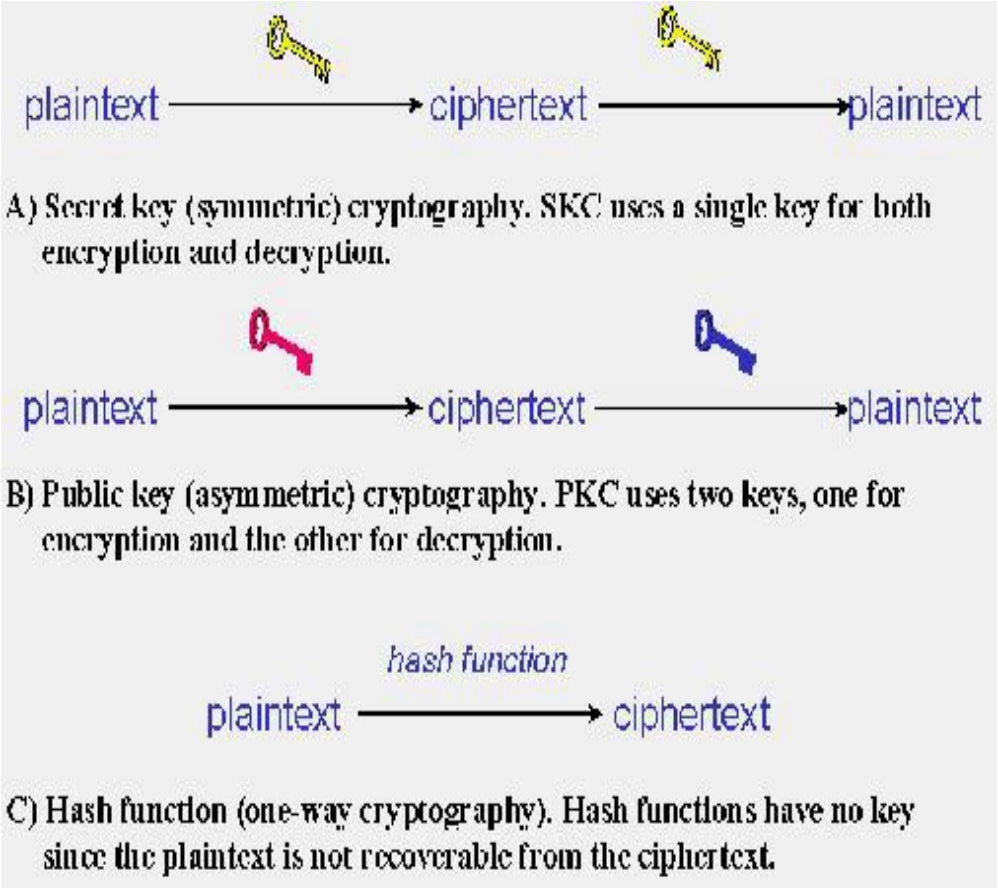

Fig. 4 Types of Cryptographic Algorithm

Recently, as the number of smart phones grows, various membership-based applications are developing. Many of these such as charged video streaming, online game and wireless access applications rely on paid service. Due to the increase of short-period of subscription, the group key is updated frequently, so that the communication overhead from rekeying grows. Hence, the efficient GKM scheme which can manage large and dynamic user group is necessary.

V. CONCLUSION

After the investigation of different algorithm such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Rivest, Shamir and Adleman (RSA), this used prime number only. So, for more efficiency we will use RGB color model and Armstrong number in proposed system by using three methods i.e., Substitution, Permutation and Combination. And the development of a new framework for optimal GKM with dynamic mobile subscribers. The proposed framework consists of cost-efficient key-tree generation and management. We also provide a new mathematical analysis methodology for quantifying the performance of key-trees.

REFERENCES

[1] 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 Vol. 4, Issue 1, pp.575-579, Jan 2014.

[2] Pranjali Gujar, Madhuri Joshi, Shilpa Jadhav, Gayatri Kulkarni, Ranjeetsingh Suryawanshi., "Secure Message Using Armstrong Number and Authentication Using Colors", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, Issue 3, pp. 10310-10314, March 2014.

[3] S.Belose, M.Malekar, G.Dharmawat, "Data Security Using Armstrong Numbers", Undergraduate Academic Research Journal (UARJ), Vol.-1, Issue-1, pp. 80-83, 2012.

[4] S.Belose, M.Malekar , G.Dharmawat, "Data Security Using Armstrong Numbers", International Journal of Emerging Technology and Advanced Engineering, Vol.2, Issue 4, pp. 125-127, April 2012.

[5] Ajay Bansode, Amit Joshi, Awanish Singh, Kiran Gosavi, Prasad S. Halgaonkar, Vijay M.Wadhai6., "Data Security Using Message Passing Using Armstrong Number", International Journal of Computer Science Trends and Technology, Vol. 2.Issue -2, pp.20-23, Mar-2014.

[6] Shakera Shaikh, Veena Gulhane, "User Authentication using Colors and data security using Armstrong numbers for Wireless Sensor Networks", International Journal of Innovative Technology and Exploring Engineering, Vol-1, Issue-1, pp. 34- 39, June 2012.

[7] 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), pp. 1-5, 12 & 13 April 2012.

[8] Sagar A. Dhanake, Umesh M. Korade, Chetan P. Shitole, Sagar B. Kedar, Prof. V. M. Lomte, "Authentication Scheme for Session Password using matrix Colour and Text", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. II, pp. 36-42, Jan. 2014.

[9] A. Revathi, Dr. Paul Rodrigues, "Survey on Secure Group Communication and Applications", International Journal of Advanced Research in Computer Science and Software Engineering,
Volume 4, Issue 6, pp.737-740 June 2014.

[10] Poonam Mandavkar, Gauri Patil, Chetna Shetty, Vishal Parkar, "SMS Security for Android Mobile Using Combine Cryptographic Algorithms", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3,pp.6221-6225 Issue 4, April 2014.

