A Review on Cryptography Using Armstrong Numbers And Colors

Mrunali vaidya[#1], Vaibhav Bansod[#2], Mangesh manwar[#3].

Department Of Computer Engineering, B.D.C.E.Sevagram,Wardha, India
mrunalivaidya16@gmail.com, bansodv04@gmail.com, mangeshmanwar@gmail.com

Abstract-Data Security is the science and study of methods of protecting data from unauthorized disclosure and modification. As per the technology upgraded, there is need to secure data which is transmitted over the network. Unsecured networks can be hacked into easily, and hackers can do lots of things in short amounts of time. A hacker can search the hard drive of the average PC user in less than a minute. In this short time period a search can be conducted on spread sheets or databases that contain user names and passwords. This paper provides a technique to encrypt the data using a key involving Armstrong numbers. Central server system is used to provide secure intended Authentication between users. So here two way security is given to key as well as data.

Keywords—Armstrong numbers, data security, authentication, cryptography.

I. INTRODUCTION

Now a day, to make secure data transmission different methods are used. One of the techniques is Cryptography, in this encryption and decryption process is used to hide simple data from unauthorized users by converting it into unreadable form and again retrieve it in original form. Security is one ofthe major concerns of all the users irrespective of the domain in which they work. There are various ways by which one can ensure the security for the data which is present in different files in the computer. Encryption-Decryption is one of those techniques which is quite popular. But, the complexity which is involved in this technique doesn't allow its users to apply it in a simpler way. Cryptography is the practice and study of techniques for secure communication in the presence of third parties. More generally, it is about constructing and analyzingprotocols that overcome the influence of adversaries and which are related to various aspects in information securitysuch as data confidentiality, data integrity, authentication, and non-repudiation. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended. Decryption is the reverse of encryption; it is the transformation of encrypted data back into some intelligible form. Encryption and decryption require the use of some secret information, Usuallyreferred to as a key. The data to be encrypted is called as plain text. The encrypted data obtained as a result of encryption process is called as cipher text. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different. This minimum key length reduces the efforts taken to encrypt the data. The key length can be increased if needed, with increase in character length. Tracing process becomes difficult with this technique, because the Armstrong number is used differently in each step. The key can be hacked only if the entire step involved in the encoding process is known earlier. Simple encryption and decryption techniques may just involve encoding and decoding the actual data, but in this proposed technique the password itself is encoded for providing more security to the access of original data.

II. LITERATURE SURVEY

Gayatrikulkarni and pranaligujar developed a technique in which Armstrong number and color are used to provide security in communication. In that Armstrong number is used instead of prime number to provide more security.

Ajay bansode and kirangosavi provided a technique in which it makes use of Armstrong number for encryption and decryption. They used Diffie-hellman algorithm and Armstrong number and proved to be

the more efficient and reliable technique for data exchange between two parties.

Author	Title	Year	Techniques
GayatriKulkarni , PranjaliGujar, Madhuri Joshi, ShilpaJadhav	Message Security Using Armstrong Numbers and Authentication Using Colors	Jan-2014	Armstrong number is used for encryption of messages, color is important in authentication process as it act as a password.
Ajay Bansode, Amit Joshi, Awanish Singh, KiranGosavi.	Data security in message passing using Armstrong number	Mar-Apr-2014	Especially this technique makes use of Armstrong numbers while encryption and decryption data.
ShakeraShaikh, VeenaGulhane	User Authentication using Colors and data security using Armstrongnumbers for Wireless Sensor Networks	June-2012	User authentication for WSNs. Proposed system is not only secure but also increased speed of communication.
S.Belose, M.Malekar , G.Dharmawat	Data Security Using Armstrong Numbers	Mar-2012	Encryption and decryption process uses Armstrong numbers which is referred as a secret key.
S.PavithraDeepa, S.Kannimuthu, V,Keerthika	Security using color and Armstrong numbers	Feb-2011	Makes use of technique to encrypt data using key involving Armstrong number and color as a password.
Madhuri Joshi, ShilpaJadhav, et al	Secure Message Using Armstrong Number and Authentication Using Colors	Mar-2014	Armstrong number and color codes are the use for providing security.

Madhuri Joshi and ShilpaJadhav 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 sheikh and veenagulhane proposed a user authentication scheme for wireless sensor network named RGB based authentication scheme. This scheme provides sufficient security for sensor nodes having less processing capability

S.PavithraDeepa and S.Kannimuthu provided a technique which provides more security with increase in key length of the Armstrong number. Usage of three set of keys namely colors, additional set of key values and Armstrong number ensures that the data is transmitted securely and accessed only by authorized only.

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.

III. COMPARISON OF DIFFERENT TECHNIQUES

Table 1 Comparison of different techniques

IV. PROPOSED WORK

In this technique the first step is to assign a unique color foreach receiver. Each color is represented with a set of three values and assigns a set of three key values to each receiver. The sender is aware 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 and encrypted at the sender's side. This encrypted color actually actsas a password. As a step further ahead let us considers atechnique in which we use Armstrong numbers and colors. Further we also use a combination, substitution and permutation methods to ensure data security. It performs the substitution process by assigning the ASCII equivalent to the characters. Permutation process is performed by using matrices as in and Armstrong number. The reverse is performed by the receiver. And the receiver is validated by the use of his unique color.

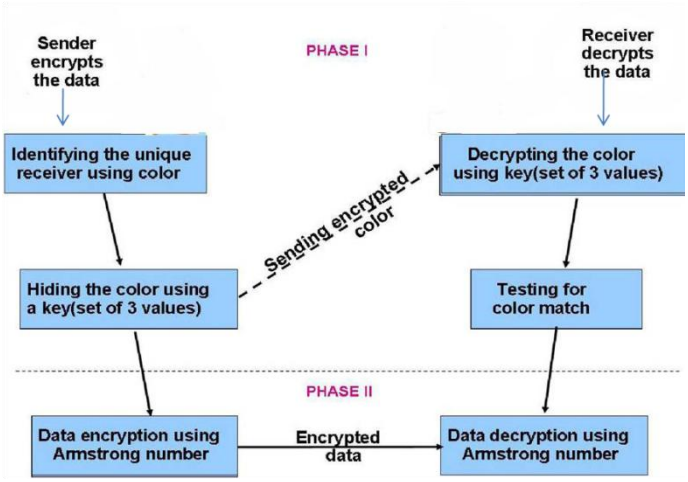

Fig 1 Architecture of proposed system

A. *RGB Model*

The proposed scheme includes two phases: Registration, Authentication.

1) User registration:

user module selects on RGB color value for the user and then find the position of this RGB in the cube and send request with its ID and POS to the base station for registration in WSNs. Base station generate a random number Which is termed as seed Also the base station module scales the seed value with the Armstrong number and multiply it with the POS it received from the user. It performs MD5 on this product and generate 128 bit key which is used for data security in AES algorithm. Base station send the key and seed to user and store the values in its database.

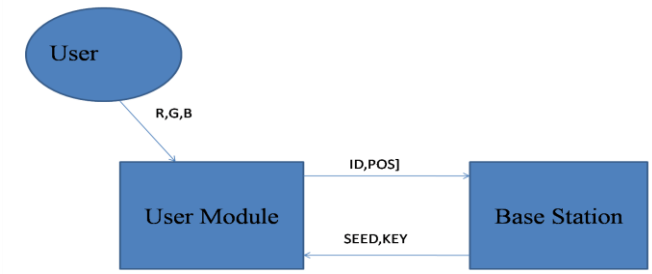

Fig 1.1 User registration

2) User Authentication on Login:

In this phase user find out the new position of RGB using RGB color cube and PRNG in which the user module generate next random number using PRNG in which it uses the seed received from the base station in the registration phase and then offsets its previous RGB POS to NEW_POS with this new SEED_NEW and login with its ID and H[POS_NEW] to the base station. Upon Login request base station also generate the SEED_NEW using PRNG and find out the POS_NEW1 in the RGB cube. If the POS_NEW matches POS_NEW1 the user is authentic.

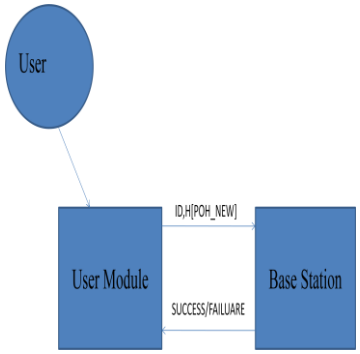

Fig 1.2 User authentication

The three primary colors of the additive color model are red, green, and blue. This RGB color cube displays smooth transitions between these colors. It has 8 bits per components. 256 * 256 * 256 number of possible colors Each color represented by a number in the cube(POS): POS = r + (g*256) + (b*256*256)

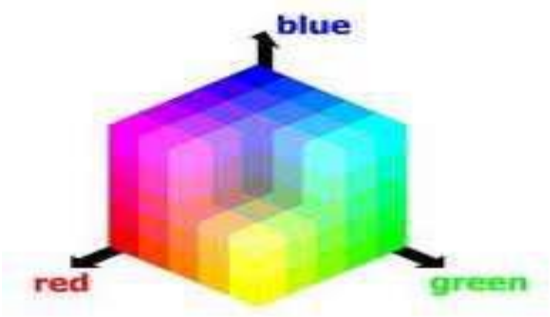

Fig 1.3 RGB color cube

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.

For example 153 is an Armstrong number because cube of 1 is 1(1x1x1=1) + cube of 5 is 125(5*5*5=125) + cube of 3 is 27(3*3*3=27). Now add all the cubes 1+125+27=153 which is equals to number itself

V. DIFFERENT ALGORITHMS

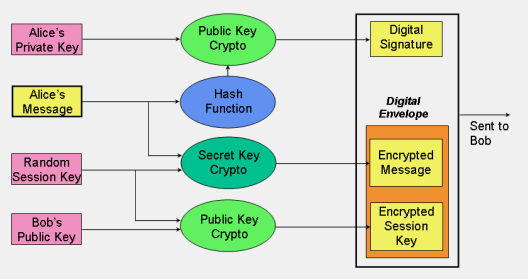

Fig 2.1 Types of Cryptographic Algorithm

There are several ways of classifying cryptographic algorithms. The three types of algorithms are depicted as follows

A. Secret Key Cryptography (SKC):
Uses a single key for both encryption and decryption. The most common algorithms in use include Data Encryption Standard (DES), Advanced EncryptionStandard (AES).

B. Public Key Cryptography (PKC):
Uses one key for encryption and another for decryption. RSA (Rivest, Shamir, Adleman) algorithm is an example.

C. Hash Functions:
Uses a mathematical transformation to Irreversibly"encrypt" information. MD (Message Digest) Algorithm is an example.

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.

References:

[1] S. PavithraDeepa,S. Kannimuthu, V. Keerthika., "*Security Using Colors and Armstrong Numbers*", Proceedings of the National Conference on Innovations in Emerging Technology, 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.ISSN 2250-2459, Volume 2, Issue 4, April 2012.

[4]ChavanSatish, LokhandeYogesh, ShindePravin, YewaleSandeep, 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.

[5]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

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

[7] AtulKahate, "*Cryptography and Network Security*", Tata McGraw Hill Publications