International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 2 | ISSN : 2456-3307
DOI : 10.32628/CSEIT1952196

User Authentication Using Color and Secure Message Transmission Using Armstrong Number

Dr. S. W. Mohod[1], Rohit V. Kakde[2], Payal S. Munjewar[2], Ruchita N. Hatwar[2], Harsha R. Rothe[2]

[1]Assistant Professor, Department of Computer Engineering, Bapurao Deshmukh College of Engineering, Wardha, Maharashtra, India

[2]BE Scholar, Department of Computer Engineering, Bapurao Deshmukh College of Engineering, Wardha, Maharashtra, India

ABSTRACT

These days data security assumes a crucial job where confidentiality, authentication, and integrity are given real significance. Every single overall programmer is ending up progressively dynamic. Along these lines, it is quickly ending up increasingly essential to secure our data. There are various techniques used to make data transmission with insurance and Cryptography is one of them. The worldwide mechanism for serving the confidentiality of transmitted data is Cryptography. This undertaking gives an application to scramble the data subsequently joining Armstrong numbers and shading codes to produce mystery key as the secret word thus to decode the record which is encoded utilizing AES calculation.

Keywords: Data Security, Confidentiality, Authentication, Integrity, Cryptography, Color Code, Armstrong Number, AES Encryption

I. INTRODUCTION

Data security has a noteworthy effect for verifying data with regards to precisely keeping up the confidentiality, authentication, and integrity of data. Transmission of data at more elevated amounts is extremely troublesome because of the nearness of programmers. The primary objectives of cryptography are getting to control and non-revocation. It comprises the procedure of encryption and decoding. Regarding encryption and decoding, there's a need of some mystery data which is ordinarily alluded to as a key called as the mystery key. This mystery key is utilized for both encryption and decoding relying upon the cryptography component. While for various systems, the keys utilized for encryption and decoding might be totally unique. The arranged framework gives calculations, for example, AES for encryption and decoding procedure and 2 distinct methods i.e Armstrong number and shading code for producing mystery key. Since the recently proposed framework gave single calculation which was utilized for encryption yet it gave low security and consequently, our framework hopes to give security including two calculations for encryption. Likewise, the expanded length of the Armstrong number gives high security making it troublesome for programmers to unscramble the data.

II. LITERATURE REVIEW

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.

III. EXISTING APPROACH

A) Security Using Colors and Armstrong Numbers [1]

The existing techniques involve the use of keys involving prime numbers. There are two techniques, Armstrong number and color code for generating a symmetric key which will be additionally used to perform coding of data in this system. The sender is conscious of the specified receiver to whom the information ought to be sent. The set of three key values are added to the native color values and encrypted at the sender's side. The actual data is encrypted using Armstrong numbers. At the receiver's side, the receiver is aware of his own color and other key values. The encrypted color from the sender is decrypted by subtracting the key values from the obtained set of color values. It is then experimented for a match with the color stored at the sender's database. Only when the colors are united the actual data can be decrypted using Armstrong numbers.

2. Secure Data Communication using AES Algorithm, Palindrome Number & Color Code [2]

In this paper, a modern encryption technique that uses AES algorithm using color code and palindrome numbers for encrypting any type of file which provides more security is implemented. In this system a new encryption technique that uses AES algorithm using color code and palindrome numbers for encrypting any type of file which gives more security than other approach. This paper presents a technique to transmit data over the network in set of three keys i.e. palindrome number, alphanumeric random key and ASCII value of color code. Crypt-analyst can easily find out the key but however in this approach, a mixture of palindrome number and color code which is used for encrypting the data. In the same way, decryption will also be done at receiver's side by using inverse of encryption process.

IV. IMPLEMENTATION

A) System Architecture

The proposed system comprises of admin and users. The admin has to login to get authenticated to the system. Once logged in, the sender has the ascendancy to add users to the system to whom information can be shared whenever required. Figure 1 shows the detailed architecture of our approach.

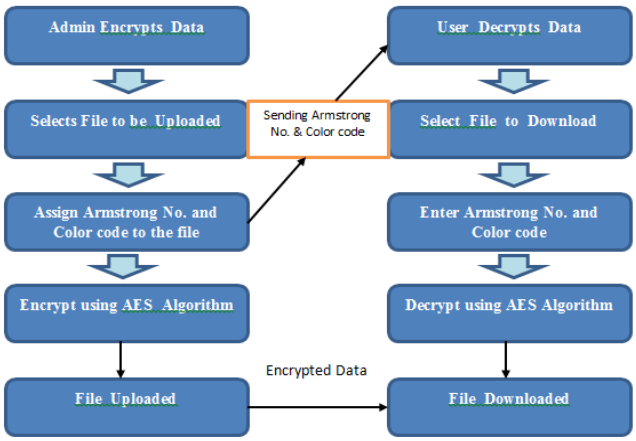

Figure 1. System Architecture

On adding new user, system produced password for user will be created and sent to user on their email address. Now for uploading file the admin will first select the Armstrong number according to his preference and concatenate with system generated color code. This will result in generation of secret key which will be provided for encryption and decryption of the data. The admin will further select an appropriate file to upload. The admin can select one or more users to whom the file has to be sent. the resulting output will be further provided as input to AES algorithm. Henceforth the file will be uploaded and the previously generated key is sent to the receiver's email address as provided. Now the receiver has to log in to the system to download the appropriate file. Once logged in, user will pick out the file to be downloaded. The user will enter the key received on his email and decryption of file will be done using AES algorithm.

B) Algorithm

1. Cryptography

Cryptography is the study of masking information i.e. a 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 which can be a secret key or a public key. This entire process is entirely an encryption process. Decryption is the reverse or the opposite process of encryption in which cipher text is again converted back to plain text with the help of the secret key.

2. Color Code

Any available color is the combination of three colors i.e. Red, Green and Blue in preset quantities. The figure below depicts RGB representation. Here the values of Red, Green and Blue represent each pixel and any color can be solely represented via 3-dimensional RGB cube. RGB model uses total of 24 bits allocating 8 bits for each color. Henceforth the colors are used as identification for authentication purpose.

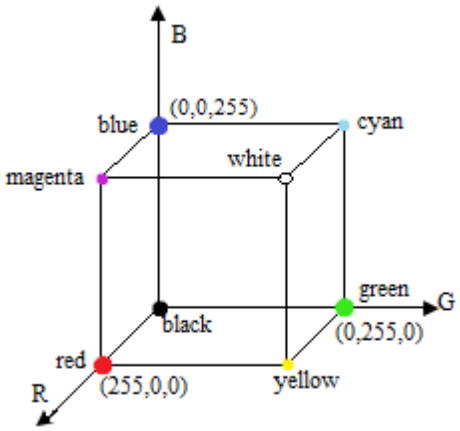

Figure 2. RGB Model

3. 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.

4. AES

AES stands for Advanced Encryption Standard algorithm which is a block cipher that uses an encryption key and performs several iterations of encryption. It is an encryption algorithm that works on single block of data at a time. In case of standard AES encryption, the block is of 128 bits or 16 bytes in length. The term "iterations" refers to the way in which the encryption algorithm stirs the data re-encrypting it ten to fourteen times depending on the length of the key. AES encryption uses a single key as a part of the encryption process. The key can be 128, 192 or 256 bits in length. The term "128-bit encryption" refers to the use of a 128-bit encryption key. With AES both encryption and the decryption are performed using the same key and hence it is called a symmetric encryption algorithm.

AES algorithm Steps:

1. Attain the set of round keys from the cipher key.
2. Initialize the state array with block data (plaintext).
3. Add the initial round key to the rise of state array.
4. Conduct nine rounds of state manipulation.
5. Perform the tenth and final round of state.

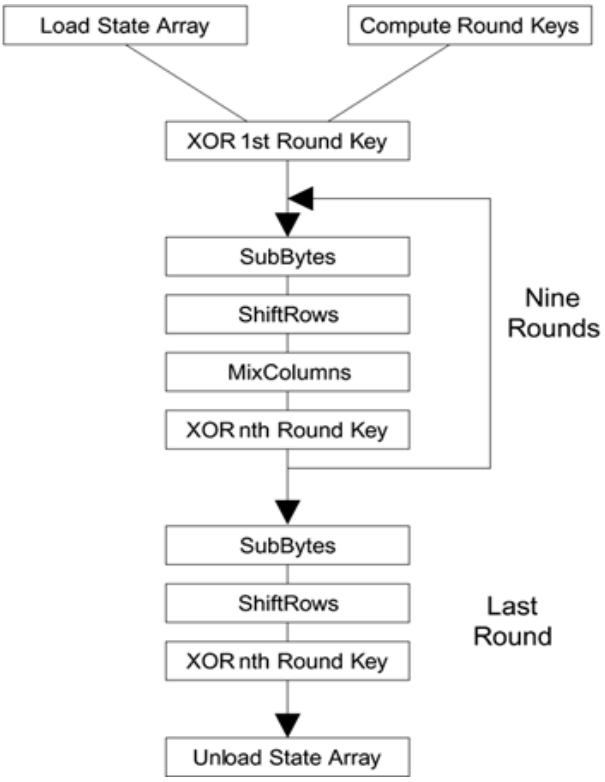

Figure 3. Working of AES Algorithm

V. CONCLUSION

In this paper, we tended to present the issue of security of secret message. Consequently, a system is proposed in which Armstrong numbers are utilized rather than prime numbers to give greater security. Hues are utilized for the authentication reason. The scope of shading is 2^0 to 2^24. RGB show utilizes 24 bits, 8 bits for each shading. To scramble the data set of three key values are added to the first shading qualities. This scrambled shading goes about like a secret key. To break this secret phrase assailant needs to check 256^3 conceivable qualities which are for all intents and purposes generally troublesome. The mix of substitution and change process expands the data security. To build the quality of calculation 9 digits, Armstrong number is utilized for encryption and unscrambling, a length of an Armstrong number can be expanded if essential for security reason. The secret zones like military, banking division, governments are focused by the framework where

data security is given more significance. Hues, key qualities and Armstrong numbers which are three arrangement of keys in this system ensure that there is verified message or data transmission and is accessible to the approved individual.

VI. REFERENCES

[1] Prof: Riya Qureshi, Shikha singh, Diksha Itankar Review on "Security Using Colours and Armstrong Numbers." International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 3, March 2016.

[2] Ajisha John, 2Keerthy.K.B, Meenu Manoharan and Diana Davis "Data Security Through Armstrong Number and Colors." International Journal of Computer Sciences and Engineering 2015.

[3] Message Security Using Armstrong Numbers and Authentication Using Colors-International Journal of Advanced Research in Computer Science and Software Engineering January 2014

[4] Data Security in Message Passing using Armstrong Number-International Journal of Computer Science Trends and Technology (IJCST)-Mar-Apr 2014

[5] Ajay Bansode, Amit Joshi, Awanish Singh, Kiran Gosavi, Prasad S.Halgaonkar, Vijay M.Wadhai " Data Security in Message Passing using Armstrong Number." International Journal of Computer Science Trends and Technology , Mar-Apr 2014.

[6] Data Security Using Armstrong Numbers-International Journal of Emerging Technology and Advanced Engineering April 2012

[7] Security Using Colors and Armstrong Numbers-NATIONAL CONFERENCE ON INNOVATIONS IN EMERGING TECHNOLOGY.

[8] 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).

[9] Atul Kahate, "Cryptography and Network Security ", Tata McGraw Hill Publications.

Cite this article as :

Dr. S. W. Mohod, Rohit V. Kakde, Payal S. Munjewar, Ruchita N. Hatwar, Harsha R. Rothe, "User Authentication Using Color and Secure Message Transmission Using Armstrong Number", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 2, pp. 570-574, March-April 2019.
Journal URL : http://ijsrcseit.com/CSEIT1952196