International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 04 | April -2020 ISSN: 2582-3930

Secure Data with Color Code and Armstrong Number

A.D.Janani

Assistant.Prof. Mr. S. SathishKumar ., MCA., M. Phil.,

Assistant Professor

Department of Computer Application

Krishnasamy college of Engineering and Technology,Cuddalore.

ABSTRACT

In real world ,data security plays on important role where confidentialty, authentication,integrity,non reputation are given importance.This paper provides a technique for data security which encrypt the data using a key involving Armstrong numbers and colours as the password. Three set of keys is used to provide secure data transmission with the colours acting as vital security element thereby providing authentication.

1.Introduction

In today's world, electronic media become a necessity. Cryptography is a way to make secure that electronic media. Data security plays an important role. Day by day hackers is becoming more powerful. So it is increasingly becoming more important to protect our valuable data Basically cryptography is used to protect valuable information resources on intranets, extranets and internet. To ensure secured data transmission, there are several techniques being followed. One among them is cryptography which is the practice and study of hiding information.

2. Existing System

In the present world scenario, it is difficult to transmit data from one place to another with security. This is because hackers are becoming more powerful nowadays. To ensure secured data transmission there are several techniques being followed. One among them is cryptography which is the practice and study of hiding information

Encryption and decryption require the use of some secret information, usually referred 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

3.Proposed System

The existing techniques involve the use of keys involving prime numbers and the like. As a step further ahead let us considers a technique in which we use Armstrong numbers and colors. Permutation process is

performed by using matrices as in and Armstrong number. In this technique the first step is to assign

a unique color for each receiver. The next step is toassign a set of three key values to each receiver. Thesender 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. At the receiver's side, the receiver is aware of his own color and other key values.

4.Cryptography

Most people are concerned with keeping communications private[4]. 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. Its purpose is to ensure privacy by keeping the data hidden from anyone for whom it is not intended. Encryption and decryption require the use of some secret information, usually referred to as a key. The data to be encrypted is called as plain text. The encrypted data obtained as a result of the 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. Security is one of the 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 of the data which is present in different files on the computer. Encryption-Decryption is one of those techniques which is quite popular[3].

Cryptography is the art and study of hiding information i.e. technique to convert plain text into cipher text i.e. encryption. Decryption in which cipher text is converted back into plain text with the help of the key. To maintain privacy and to prevent an unauthorized person from extracting information from the communication channel.

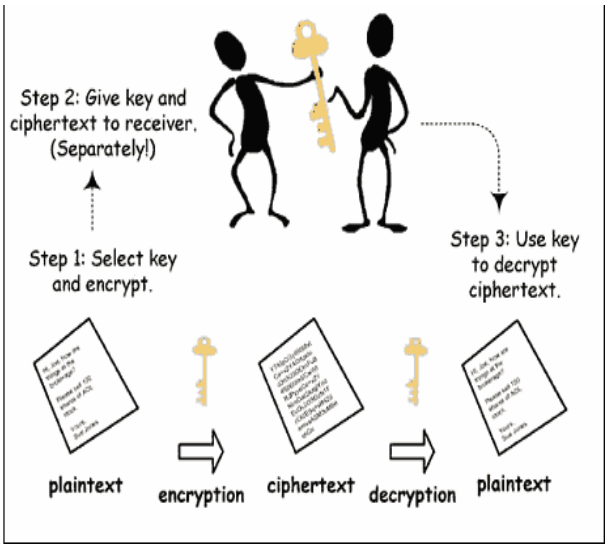


Figure 1- Cryptography

4.1 Advanced Encrytion Standard

In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard adopted by the U.S. government. The standard comprises three blockciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originallypublished as Rijndael. Each of these ciphers has a 128-bit block size, with key sizes of 128,192 and 256 bits, respectively. The AES ciphers have been analysed extensively and are nowused worldwide. AES was announced by National Institute of Standards and Technology (NIST) asU.S. FIPS PUB 197 (FIPS 197) on November 26.

There are three versions of AES with 10,12 and 14 rounds.The key size can be 128,12, 256 bits depending on the number of rounds.Generaldesign

of an AES encryptioncipher is given in **Figure 2.**

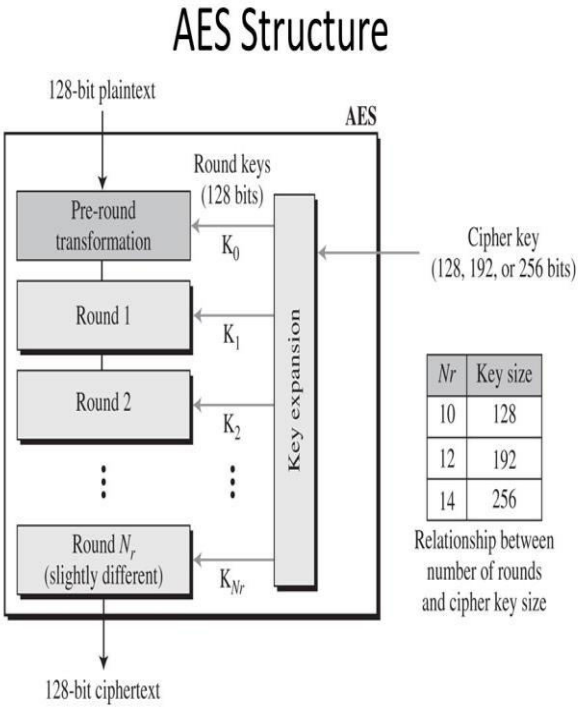


Figure 2- Structure of AES

5.Secure Data With Color Code

In real world ,data security plays on important role where confidentialty, authentication,integrity,non reputation are given importance.Data security plays an important role. Day by day hackers is becoming more powerful. So it is increasingly becoming more important to protect our valuable data Basically cryptography is used to protect valuable information resources on intranets, extranets and internet.To ensure secured data is hiding the information and receivers has unique color code password,so the hackers don't access from information.

5.1 Modules

- Color encryption
- Data encryption
- Color decryption
- Data decryption

Color Encryption

Step 1: Select random image

Step 2: Click on any pixel of an image. If we click on image pixel then we get RGB colour values of that pixel. Consider RGB value is (107, 55, 57)

Step 3: Divide that RGB values by 10. We get key (10, 5, 5)

Step 4: Add this key (10, 5, 5) to the receivers unique colour. Consider the colour is pink (255,192,203).

255 192 103

+ 10 5 5

265 197 108

If the encoded value is greater than 255 then change the sign of the key values like (- 10, 5, 5) and the new encoded values are (245, 197, 108).

Step 5: Finally sender sends this encoded colour values to the receiver.

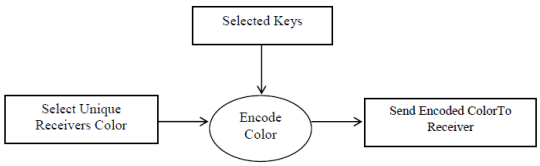


Fig1: color encryption

Data Encryption :

Step 1: Select Armstrong number randomly which is not contain the zero digit.

Step 2: Convert plaintext into ASCII equivalent.

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

Step 4: Convert result produce by this operation is converted into the matrix.

Step 5: Convert Armstrong number into the matrix

Step 6: Multiply the above two matrices and finally get the encrypted value.Encrypted values converted into the form of message like (779, 3071, 135, 742…)

Step 7: Send this message to the receiver.

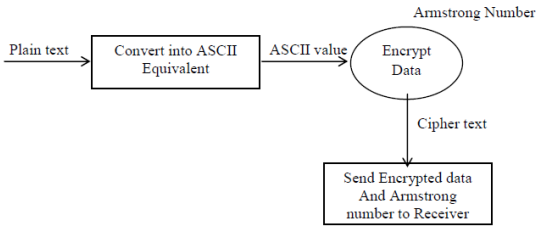


Fig2:Data Encryption

Data Decryption

Step 1: convert the cipher text into the matrix.

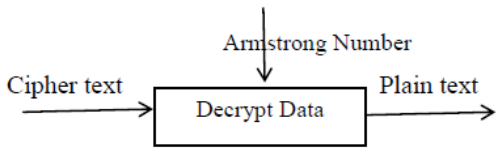
Step 2: take the inverse of cipher text matrix.

Step 3: multiply inverse matrix with the cipher text matrix

Step 4: The result produce by this operation is converted into equivalent values like (779, 3071, 135, 742…)*Data Security Using Colours and Armstrong Numbers*

Step 5: subtract Armstrong number from this resulted values.

Step 6: Convert this values into character i.e receiver get the original plain text.



6.Advantages

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. The combination of substitution and permutation process increases the data security. To increase the strength of algorithm 9 digits, Armstrong number is used for encryption and decryption, a length of an Armstrong number can be increased if necessary for security purpose.

7.Conclusion

The above combination of secret key and public key cryptography can be applied mainly in military where data security is given more importance. This technique provides more security with increase in key length of the Armstrong numbers. Thus usage of three set of keys namely colors, additional set of key values and Armstrong numbers in this technique ensures that the data is transmitted securely and accessed only by authorized people.

9.References

[1]http://www.aix1.uottawa.ca/~jkhoury/cryptography.html.

[2]http://www.scribd.com/doc/29422982/Data-Compression-and Enciding-Using-Col.

[3]“Cryptography and Network Security” By AtulKahate TMH.

[4] Higher Algebra(Abstract and Linear) – S.K.Mapa , Sarat Book House.

[5]S.PavithraDeepa,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.

[6] Gordon L. Miller and Mary T. Whalen, "Armstrong Numbers", University of Wisconsin, Stevens Point, WI 54481 (Submitted October 1990).

[7] 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).

[8] M.F.Armstrong "A brief introduction to Armstrong Numbers" .