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. 4, Issue. 5, May 2015, pg.512 – 515

RESEARCH ARTICLE

A Novel Approach for Security using Colors and Armstrong Numbers

1st T. Ravi Kiran, 2nd M. Divya, 3rd N. Vinay, 4th M. Shiva Shankar, 5th G. Siva Kamal

[1]Assistant Professor, Dept. of CSE, VITS College of Engineering, Vizag
[2]B.Tech Student, VITS, Vizag
[3]B.Tech Student, VITS, Vizag
[4]B.Tech Student, VITS, Vizag
[5]B.Tech Student, VITS, Vizag

ABSTRACT: In real world, data security plays an important role where confidentiality, authentication, integrity, non repudiation are given importance. The universal technique for providing confidentiality of transmitted data is cryptography. This paper provides a technique to encrypt the data using a key involving Armstrong numbers and colors as the password. Three set of keys are used to provide secure data transmission with the colors acting as vital security element thereby providing authentication.

Keywords— Armstrong numbers, data security, authentication, cryptography

I. INTRODUCTION

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.

Cryptography

Cryptography, to most people, is concerned with keeping communications private. Encryption is the transformation of data into some unreadable form. 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, 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. 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.

Types of Cryptographic Algorithms

There are several ways of classifying cryptographic algorithms. In general they are categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms are depicted as follows

1) 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 Encryption Standard (AES).
2) Public Key Cryptography (PKC): Uses one key for encryption and another for decryption. RSA (Rivest,Shamir, Adelman) algorithm is an example.
3) Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information. MD (Message Digest) algorithm is an example.

RGB Color Model

Any color is the combination of three primary colors Red, Green and Blue in fixed quantities. A color is stored in a Computer in form of three numbers representing the quantities of Red, Green and Blue respectively. This representation is called RGB representation which is used in computers to store images in BMP, JPEG and PDF formats. Here each pixel is represented as values for Red, Green and Blue. Thus any color can be uniquely represented in the three dimensional RGB cube as values of Red, Green and Blue. The RGB color model is an additive model in which Red, Green and Blue are combined in various ways to produce other colors. By using appropriate combination of Red, Green and Blue intensities, many colors can be represented. Typically, 24 bits are used to store a color pixel. This is usually apportioned with 8 bits each for red, green and blue, giving a range of 256 possible values, or intensities, for each hue. With this system, 16 777 216 (256^ 3 or 2^24) discrete combinations of hue and intensity can be specified.

II. Related Work

Existing System:

Description of the Problem:

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. 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.

Demerits of Existing System:

1. More space is required on server side because of RSA.
2. The speed of execution is slow because the file size after encryption is 8 times the original size.
3. The only way to break into this system is by Brute force attack, which also can take up to two or three years.
4. To protect the encryption, the minimum number of bits in n(n in RSA) should be 2048.

Proposed System:

Problem Solution:

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. Further we also use a combination of substitution and permutation methods to ensure data security. We perform the substitution process by assigning the ASCII equivalent to the characters. 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. Each color is represented with a set of three values. For example violet red color is represented in RGB format as (238, 58,140). The next step is to assign 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. At the receiver's side, the receiver is aware of his own color and other key values.

Merits of the proposed system:

1. 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.
2. This technique could be considered as a kind of triple DES algorithm since we use three different keys namely the colors, key values added with the colors and Armstrong numbers.
3. Unless all the three key values along with the entire encryption and decryption technique is known the data cannot be obtained. So hacking becomes difficult mainly because of the usage of colors.
4. 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.

III. MODULES

User Authentication:

- In this technique, we use RGB color model for user authentication, were a discrete and unique set of colors, i.e., 16 777 216 (256^ 3) combinations of colors can be defined.
- The sender assigns unique color for each user and this detail is stored in a database. The sender is aware of the required receiver to whom the data has to be sent.
- A set of three key values are added to the original color values and encrypted at the sender's side. This encrypted color actually acts as a password.
- The sender sends the key value to the receiver.
- The receiver is aware of the color assigned to him. The receiver decrypts the color by subtracting the key values from the encrypted color values.
- If the decrypted color value matches with the color value stored in the database, then the user is an authenticated user.
- Usage of colors helps to enhance security of data; this is because only if the color at receiver side matches the color on the sender side, original data can be accessed.

Data Encryption:

- Once the user is authenticated, now the sender sends the requested data to the receiver.
- Initially ASCII value for each character is found. Then Armstrong number is added to this ASCII value in an iterative manner until each character is assigned with the number.
- The resultant sum value is now converted into a matrix. Consider an encrypted matrix (Armstrong number), multiply it with the resultant sum matrix.
- The resultant matrix value consists of the encrypted data.

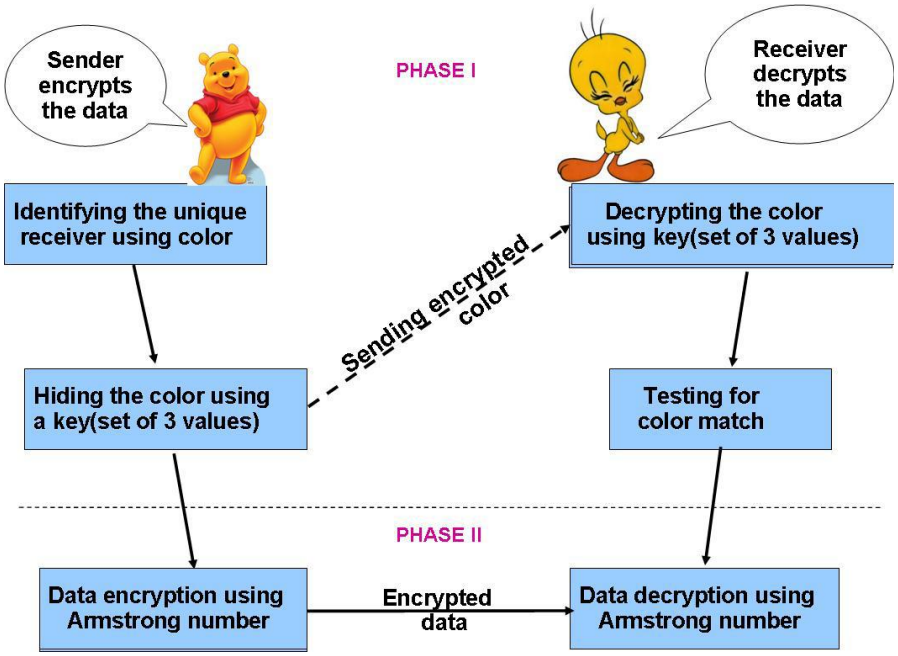
Receiver:

- The receiver of this module will receive encrypted code and they have to decrypt it also to decrypt a message.

Data Decryption:

- The data which is encrypted and hidden is received at the receiver side. The data is extracted now.
- The inverse of the encoding matrix (Armstrong number) is found, and it is the decoding matrix.
- On receiving the encrypted data, the data is rearranged to the original order, which is gives the correct order of the encrypted data.
- Now this data is arranged in matrix format and it is multiplied with the decoding matrix. The resultant value gives the ASCII value of the characters. Thus the data is decrypted and original data is got back.

Proposed Architecture:



IV. CONCLUSION

The 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.

REFERENCES

1. Atul Kahate, "Cryptography and Network Security ", Tata McGraw Hill Publications
2. http://aix1.uottawa.ca/~jkhoury/cryptography.htm
3. http://www.scribd.com/doc/29422982/Data-Compression-and-Encoding-Using-Col
4. JAVA Complete Reference, Herbert schildt, standard edition 7, McGraw-Hill Education, 2011
5. HTML Black Book, Holzner, standard edition 2, Dreamtech Press, 2000
6. The Unified Modeling Language User Guide, 2nd edition, Pearson Education 1999
7. Software Engineering By Somerville 8th edition, Pearson education

