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. 3, March 2015, pg.451 – 458

RESEARCH ARTICLE

Secured and Reliable Transmission using RGB Colors and Prime Numbers

T.Mugilan
Assistant Professor
Department of Computer Science and Engineering
IFET College of Engineering
mugipdy@gmail.com

S.Kiruthika
UG Student
Department of Computer Science and Engineering
IFET College of Engineering
skiruthika55@gmail.com

M.Elakkiya
UG Student
Department of Computer Science and Engineering
IFET College of Engineering
elakkiyamgn@gmail.com

Abstract: The common technique for providing Cryptography is the key to pledge data security. This proposal provides various factors to encrypt and decrypt the data using a key such as prime numbers and RGB colors as the password. There are three keys used to afford secure and reliable data transmission with the RGB colors which is a most important security element which provides substantiation. In real world, data security plays an important role where privacy, substantiation, reliability, non-refutation are given importance. This paper provides a technique to encrypt the data using a key involving prime numbers in Fibonacci and colors as the password. Three set of keys are used to provide safe data transmission with the colors acting as vital security element thereby providing substantiation.

Keywords- prime numbers, Fibonacci, data security, authentication, cryptography

I. INTRODUCTION

Information security is the process of protecting information. It protects its availability, privacy and integrity. Access to stored information on computer databases has increased greatly. More companies store business and individual information on computer than ever before. Much of the

Information stored is highly confidential and not for public viewing. The main feature of the encryption/decryption program implementation is the generation of the encryption key. Now a day, cryptography has many commercial applications. If we are protecting confidential information then cryptography is provide high level of privacy of individuals and groups.

II. 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.

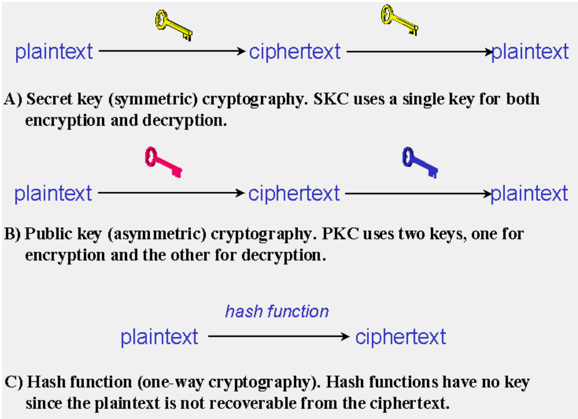
A. Types of Cryptographic Algorithms

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 as in [1]. 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, Adleman) algorithm is an example.

3. ***Hash Functions:***
   Uses a mathematical transformation to irreversibly "encrypt" information. MD (Message Digest) algorithm is an example.



A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

Fig. 1 Types of Cryptographic Algorithms

III. RGB COLOR FORMAT

A. 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.

IV. PROPOSED APPROACH

A. Introduction

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 prime numbers under the Fibonacci concepts 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 [2] and prime numbers in Fibonacci .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.

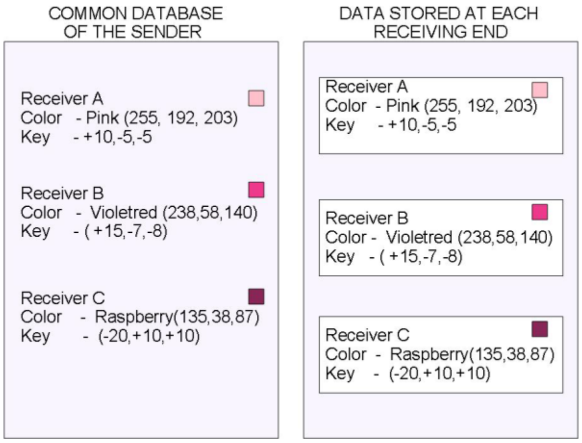


Fig 2: Data at Sender and Receiver ends.

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 acts as a password. The actual data is encrypted using Prime 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 received set of color values. It is then tested for a match with the color stored at the sender's database. Only when the colors are matched the actual data can be decrypted using Prime numbers. Usage of colors as a password in this way ensures more security to the data providing authentication. This is because only when the colors at the sender and receiver's side match with each other the actual data could be accessed.

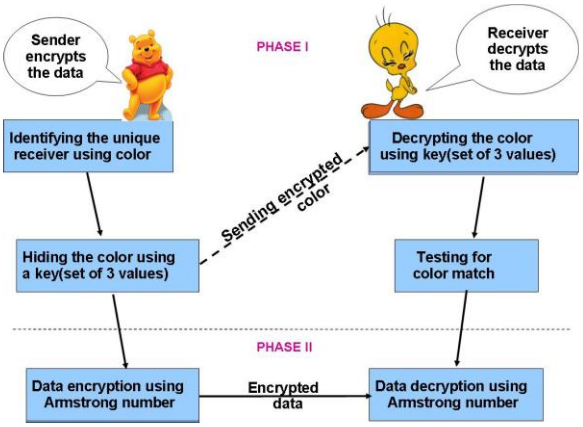

Sender encrypts the data
PHASE I
Receiver decrypts the data
Identifying the unique receiver using color
Decrypting the color using key(set of 3 values)
Sending encrypted color
Hiding the color using a key(set of 3 values)
Testing for color match
PHASE II
Data encryption using Armstrong number
Encrypted data
Data decryption using Armstrong number

Fig 3 .Layout of the proposed technique

B. Illustration

1) Encryption:

As an illustration let us assume that the data has to be sent to a receiver (say A) who is assigned the color raspberry (135, 38, 87). Let the key values to be added with this color value be (-10, +5, +5). Let the Prime numbers used for data encryption be 153.

Triple DES algorithm:

Triple DES uses a "key bundle" that comprises three DES keys, K_1, K_2 and K_3, each of 56 bits (excluding parity bits). The encryption algorithm is:

ciphertext = $E_{K3}(D_{K2}(E_{K1}(\text{plaintext})))$

I.e., DES encrypt with K_1, DES *decrypt* with K_2, then DES encrypt with K_3.

Decryption is the reverse:

plaintext = $D_{K1}(E_{K2}(D_{K3}(\text{ciphertext})))$

I.e., decrypt with K_3, *encrypt* with K_2, then decrypt with K_1.

Each triple encryption encrypt on block of 64 bits of data.

In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying options 2, and provides backward compatibility with DES with keying option 3.

Keying options

The standards define three keying options:

- Keying option 1: All three keys are independent.
- Keying option 2: K_1 and K_2 are independent, and $K_3 = K_1$.
- Keying option 3: All three keys are identical, i.e. $K_1 = K_2 = K_3$.

Keying option 1 is the strongest, with 3 × 56 = 168 independent key bits.

Keying option 2 provides less security, with 2 × 56 = 112 key bits. This option is stronger than simply DES encrypting twice, e.g. with K_1 and K_2, because it protects against meet in the middle attacks

Keying option 3 is equivalent to DES, with only 56 key bits. This option provides backward compatibility with DES, because the first and second DES operations cancel out.

Each DES key is nominally stored or transmitted as 8 bytes, each of odd parity, so a key bundle requires 24, 16 or 8 bytes, for keying option 1, 2 or 3 respectively.

Step 1: (Creating password)

Initially the sender knows the required receiver to be A. So the key values are added with the color values assigned for receiver A.

```
     135    38    87

      -10     5     5

  -----------------------------

     125     43    92
```

Now a newly encrypted color is designed for security check.

Step 2: (Encryption of the actual data begins here)
Let the message to be transmitted be "CRYPTOGRAPHY". First find the ASCII equivalent of the above characters.

C R Y P T O G R A P H Y

67 82 89 80 84 79 71 82 65 80 72 89

Step 3: Prime numbers under Fibonacci as follows:

Prime :

2 3 5 7 11 13 17 19 23 29 31 37 41

43 47 53 59 61 67 71 73 79 83 89 97

In Fibonacci values:

2 5 10 17 28 41 58 77 100 129 160

197 238 281 328 381 440 501 568 639

712 791 874 963 1060

Now take the even numbers on Fibonacci values:

2 10 28 58 100 160 238 328 440 568 712

874 1060.

Step 4: Now subtract these numbers with the digits of the Prime numbers in Fibonacci as follows:

67 82 89 80 84 79 71 82 65 80 72 89

(-) 2 10 28 58 2 38 3 28 10 40 2 10

65 72 61 22 82 41 68 54 55 20 70 79

Step 5: Convert the above data into a matrix as follows

$$A=\begin{pmatrix} 65 & 22 & 68 & 20 \\ 72 & 82 & 54 & 70 \\ 61 & 41 & 55 & 79 \end{pmatrix}$$

Step 5: Consider an encoding matrix

$$B=\begin{pmatrix} 2 & 10 & 28 \\ 58 & 28 & 10 \\ 60 & 4 & 40 \end{pmatrix}$$

Step 6: After multiplying the two matrices (B X A) we get

$$C=\begin{pmatrix} 1279 & 1006 & 1192 & 1496 \\ 3198 & 1991 & 3033 & 2535 \\ 3314 & 1664 & 3368 & 2920 \end{pmatrix}$$

Take mod 25,

$$\begin{pmatrix} 4 & 6 & 17 & 21 \\ 23 & 16 & 8 & 10 \\ 14 & 19 & 18 & 20 \end{pmatrix}$$

The encrypted data is...
4 23 14 6 16 19 17 8 18 21 10 20

The above values represent the encrypted form of the given message.

2) *Decryption:*

Decryption involves the process of getting back the original data using decryption key. The data given by the receiver (the color) is matched with the data stored at the sender's end. For this process the receiver must be aware of his own color being assigned and the key values.

Step 1: (Authenticating the receiver)

For the receiver A (as assumed) the actual color being assigned is Raspberry. (135, 38, 87), the key values (set of three values) are subtracted from the color being received to
get back the original color. The decryption is as follows.

```
         125      43    92 (Received data)

      (-) -10        5       5 (Key value)
--------------------------------------------------
         135      38     87
```

The above set of values (135, 38, 87) is compared with the data stored at the sender's side. Only when they both match the following steps could be performed to decrypt the original data.

Step 2: (Decryption of the original data begins here)

The inverse of the encoding matrix is

$$D = 1/320 \begin{bmatrix} -0.038 & 0.010 & 0.0246 \\ 0.061 & 0.057 & -0.057 \\ 0.052 & -0.02 & 0.018 \end{bmatrix}$$

Step 3: Multiply the decoding matrix with the encrypted data (D X C) we get

Step 4: Now transform the above result as given below

65 72 61 22 82 41 68 54 55 20 70 79

Step 5: Add with the digits of the Prime numbers as follows

```
    68  87 92 81 109 88 72 207 92 81 77 92

(+)  2  10 28 58     2 38   3   28 10 40   2 10
________________________________________________

      67 82 89 80  84 79 71   82 65 80 72 89
```

Step 6: Obtain the characters from the above ASCII equivalent

67 82 89 80 84 79 71 82 65 80 72 89

C R Y P T O G R A P H Y

C. Advantages

The above technique involves keys with a minimum length of 8 bits for Prime numbers. 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. This increases the complexity thereby providing increased security. This technique ensures that the data transfer can be performed with protection since it involves two main steps. First step is to convert the characters into another form, by adding with the digits of the Prime numbers. Second step is to encode using a matrix to form the required encrypted data. Tracing process becomes difficult with this technique. This is because the Prime numbers is used differently in each step. The key can be hacked only if the entire steps involved in the encoding process are known earlier.

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 prime numbers. 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. 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.

V. 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 prime numbers. Thus usage of three set of keys namely colors, additional set of key values and Prime 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]Yan Wang and Ming Hu “Timing evaluation of the known cryptographic algorithms “2009 International Conference on Computational Intelligence and Security 978 – 0 – 7695 – 3931 - 7/09

[5]T Morkel, JHP Eloff “ ENCRYPTION TECHNIQUES: A TIMELINE APPROACH” published in Information and Computer Security Architecture (ICSA) Research Group proceeding.

[6]Symmetric key cryptography using random key generator, A.Nath, S.Ghosh, M.A.Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas(USA) Vol-2,P-239-244.

[7]https://www.scribd.com/doc/15466855/Latest-Paper-on-Cryptography

[8]http://searchsecurity.techtarget.com/qna/0,289202,sid14_gci1077600,00.html

[9]https://users.cs.jmu.edu/abzugcx/public/Cryptology/Journal-Articles-on-Crypto-POSTED.pdf

[10]Prof. Mr. S. A. Saoji, Nikita B. Agarwal, Mrunal B. Bokil, Ashwini V. Gosavi, “Securing e- mails using colors and armstrong numbers”, IJSCER, vol 4, pp 1438 -1440, July 2013.

[11]Ayoub F, Singh K, “Cryptographic techniques and network security”, IEEE proceedings, vol. 131, pp. 684-694, Nov. 2008

[12]Majdi Al-qdah & Lin Yi Hui “Simple Encryption/Decryption Application ” public shed in International Neal Koblitz “A Course in Number Theory and Cryptography” Second Edition Published by Springer-Verlag