

Security Using Colors and Armstrong Numbers

S. Pavithra Deepa^{#1}, S. Kannimuthu^{#2}, V. Keerthika^{#3}

^{#1,3}UG Student, Department of IT, Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India

^{#2}Assistant Professor, Department of IT, Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India

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.

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

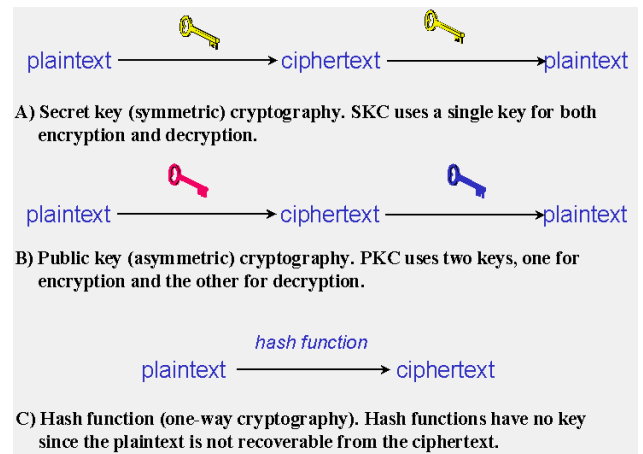
1) *Secret Key Cryptography (SKC)*: Uses a single key for both encryption and decryption. The most common algorithms in use include Data Encryption Standard (DES), Advanced Encryption Standard (AES).

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.

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 consider 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 [2] 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.

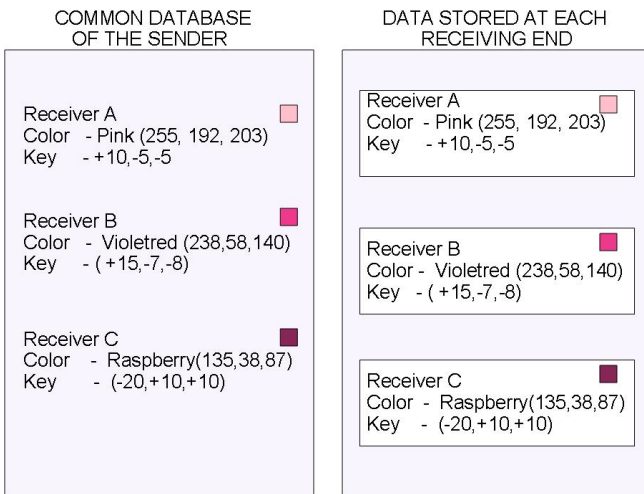


Fig 2: Data at Sender and Receiver ends.

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 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 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

Armstrong 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.

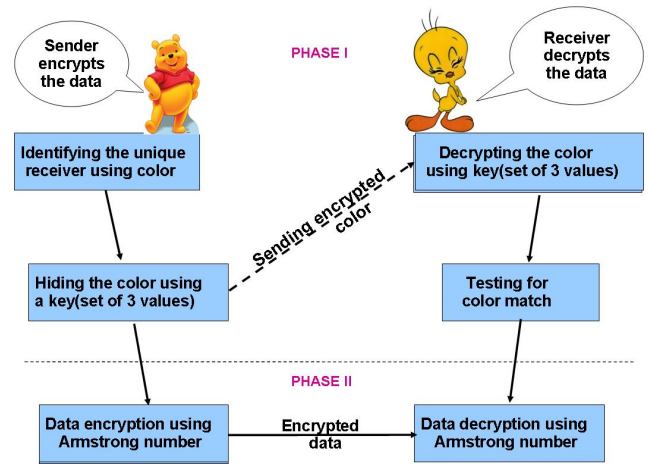


Fig 3 .Layout of the proposed technique

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 Armstrong number used for data encryption be 153.

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: Now add these numbers with the digits of the

Armstrong number as follows

$$\begin{array}{r}
 67\ 82\ 89\ 80\ 84\ 79\ 71\ 82\ 65\ 80\ 72\ 89 \\
 (+)1\ 5\ 3\ 1\ 25\ 9\ 1\ 125\ 27\ 1\ 5\ 3 \\
 \hline
 68\ 87\ 92\ 81\ 109\ 88\ 72\ 207\ 92\ 81\ 77\ 92
 \end{array}$$

Step 4: Convert the above data into a matrix as follows

A =

$$\begin{bmatrix}
 68 & 81 & 72 & 81 \\
 87 & 109 & 207 & 77 \\
 92 & 88 & 92 & 92
 \end{bmatrix}$$

Step 5: Consider an encoding matrix...

B =

$$\begin{bmatrix}
 1 & 5 & 3 \\
 1 & 25 & 9 \\
 1 & 125 & 27
 \end{bmatrix}$$

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

C =

$$\begin{bmatrix}
 779 & 890 & 1383 & 742 \\
 3071 & 3598 & 6075 & 2834 \\
 13427 & 16082 & 28431 & 12190
 \end{bmatrix}$$

The encrypted data is...

779, 3071, 13427, 890, 3598, 16082, 1383, 6075, 28431, 742, 2834, 12190

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.

$$\begin{array}{r}
 125\ 43\ 92\ \text{(Received data)} \\
 (-)\ -10\ 5\ 5\ \text{(Key values)} \\
 \hline
 135\ 38\ 87
 \end{array}$$

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

$$(-1/240) * \begin{bmatrix}
 -450 & 240 & -30 \\
 -18 & 24 & -6 \\
 100 & -120 & 20
 \end{bmatrix}$$

D =

Step 3: Multiply the decoding matrix with the encrypted data

$$\begin{bmatrix}
 68 & 81 & 72 & 81 \\
 87 & 109 & 207 & 77 \\
 92 & 88 & 92 & 92
 \end{bmatrix}$$

(D X C) we get

Step 4: Now transform the above result as given below

$$68\ 87\ 92\ 81\ 109\ 88\ 72\ 207\ 92\ 81\ 77\ 92$$

Step 5: Subtract with the digits of the Armstrong numbers as follows

$$\begin{array}{r}
 68\ 87\ 92\ 81\ 109\ 88\ 72\ 207\ 92\ 81\ 77\ 92 \\
 (-)1\ 5\ 3\ 1\ 25\ 9\ 1\ 125\ 27\ 1\ 5\ 3 \\
 \hline
 67\ 82\ 89\ 80\ 84\ 79\ 71\ 82\ 65\ 80\ 72\ 89
 \end{array}$$

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 Armstrong 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 Armstrong 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 Armstrong number is used differently in each step. The key can be hacked only if the entire steps involved in the encoding process is 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 Armstrong 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 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>