Cryptography Mechanisms Using Colors Steganography and Armstrong Number in Data Transmission

Nilima Patil[1], Shruti.B.Kurup[2], Nirali Arora[3], Smita.A.Mali[4]
1Assistant Professor, [2,3,4] BE Student, Department of Computer Engineering ,
KC College of Engineering and Management Studies and Research , Thane(E),India
[1]nilima.patil7@gmail.com,[2]shrutikurup.sk@gmail.com,[3] niralikaur2@gmail.com, [4]smita.171192@gmail.com

ABSTRACT

In real world, data security plays an important role where confidentiality, authentication, integrity, non repudiation are given importance. 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. 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. 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. Now 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.

Keywords

Self-destructing data, active storage, data privacy, cloud computing**.**

I. INTRODUCTION

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, to most people, is concerned with keeping communications private. Indeed, the protection of sensitive communications has been the emphasis of cryptography all through much of its history. 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, even those who can see the encrypted data. Decryption is the reverse of encryption; it is the transformation of encrypted data back into some intelligible form. Today governments use sophisticated methods of coding and decoding messages. One type of code, which is extremely difficult to break, makes use of a large matrix to encode a message. The receiver of the message decodes it using the inverse of the matrix. This first matrix is called the encoding matrix and its inverse is called the decoding matrix An Armstrong number is an n-digit base b number such that the sum of its (base b) digits raised to the power n is the number itself. Hence 153 because 13 + 53 + 33 = 1 + 125 + 27= 153.Much more information can be found at the site of Lionel Deimel. The most principal information is that the number of Armstrong numbers for a particular base is finite.

II. LITERATURE SURVEY

There are various types of Cryptographic algorithms. In general they are categorized based on the number of keys that are employed for encryption and decryption[2] The three types of algorithms are depicted as follows:

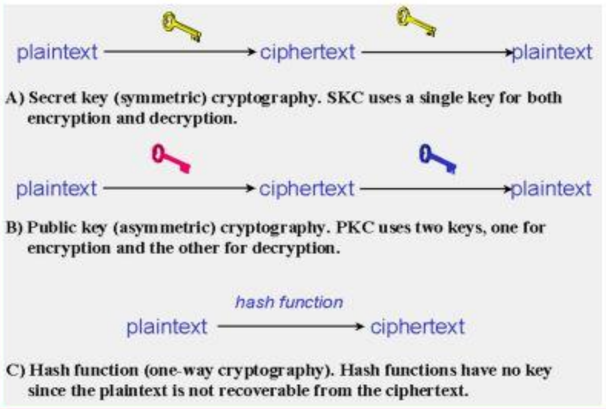
1) Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption. The most common algorithms in use include Data Encryption Standard (DES), Advanced Encryption Standard (AES).

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 The existing techniques involve the use of keys involving prime numbers and the like (RSA)[1].

Fig. 1 Types of Cryptographic Algorithms

III. RGB COLOR FORMAT



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.

III. PROPOSED SYSTEM

In this technique the first step is to assign a unique color for each receiver. So the receiver's unique color is used as the password. The set of four color values are added to the original color values and encrypted at the sender's side. This encrypted color actually acts as a password. Further we also use a combination, substitution and permutation methods to ensure data security. It performs the substitution process by assigning the ASCII equivalent to the characters.

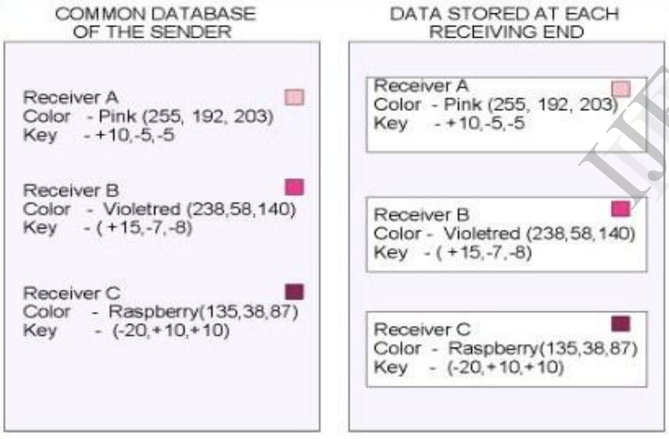

COMMON DATABASE OF THE SENDER
Receiver A
Color - Pink (255, 192, 203)
Key - +10,-5,-5
Receiver B
Color - Violetred (238,58,140)
Key - (+15,-7,-8)
Receiver C
Color - Raspberry(135,38,87)
Key - (-20,+10,+10)
DATA STORED AT EACH RECEIVING END
Receiver A
Color - Pink (255, 192, 203)
Key - +10,-5,-5
Receiver B
Color - Violetred (238,58,140)
Key - (+15,-7,-8)
Receiver C
Color - Raspberry(135,38,87)
Key - (-20,+10,+10)

Fig 2: Data at Sender and Receiver ends.

Permutation process [1] is performed by using matrices as in and Armstrong number. The reverse is performed by the receiver. And the receiver is validated by the use of his unique color. 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.

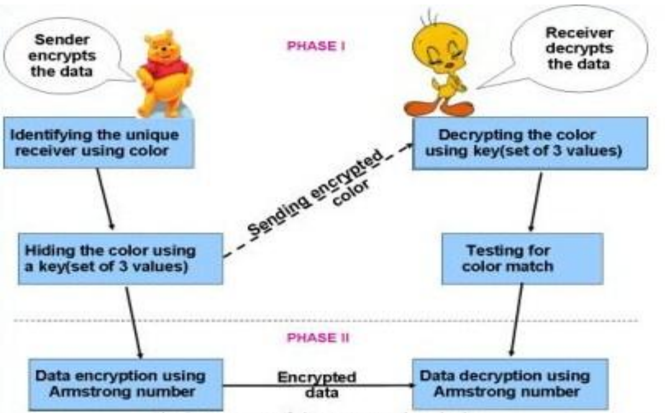

Sender encrypts the data
PHASE I
Receiver decrypts the data
Identifying the unique receiver using color
Decrypting the color using key(set of 3 values)
Sending encrypted color
Hiding the color using a key(set of 3 values)
Testing for color match
PHASE II
Data encryption using Armstrong number
Encrypted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

Fig 3 .Layout of the proposed technique

IV.ILLUSTRATION

A. 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)[3]. 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

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

1 5 3 1 25 9 1 125 27 1 5 3

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

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

A=□92 88 92 92

87 109 207 77

68 81 72 81

Step 5: Consider an encoding matrix...

B=1 125 27

1 25 9

1 5 3

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

C =

13427 16082 28431 12190

3071 3598 6075 2834

779 890 1383 742

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.

B. 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 .Decryption is exactly the reverse process which was involved in encryption.

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 values)

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

(1/ 240)* -450 240 -30□

18 24 6

100 -120 20

Step 3: Multiply the decoding matrix with the encrypted data

92 88 92 92

87 109 207 77

68 81 72 81

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

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

1 5 3 1 25 9 1 125 27 1 5 3

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

Step 6: Obtain the characters from the above ascii values

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

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

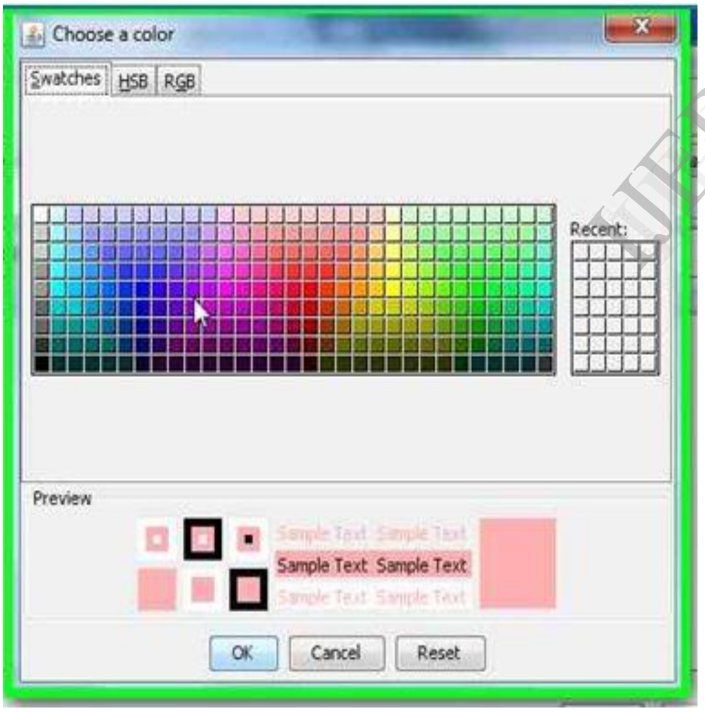
V. ADVANTAGES

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 require decrypted 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 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

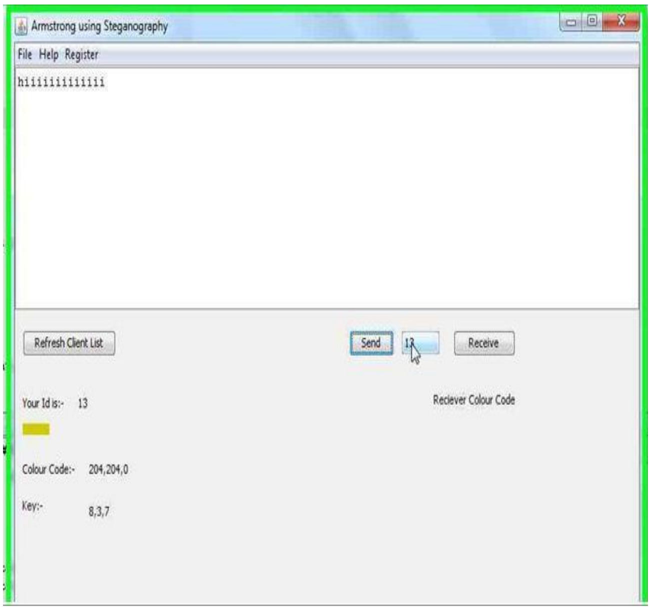
VI. RESULT

secret key cryptography and security inour project is achieved through the use of color codes. The colorcodes are used for authentication of the receiver. Only authentication of user using color codes & Encryption algorithms implemented. Output of the implantation shown in following snapshot. Implementation of decryption is still in working mode.

The below given snapshot depicts selection of colorcodes by the sender and the receiver.



The below given snapshot depicts the process after registration and color selection .Here the random keys are generated to facilitate the algorithm .Also the RGB values of the selected color codes is displayed .When we click on Send button the encryption algorithm starts executing at the backend.



hiiiiiiiiiiii

Your Id is:- 13

Colour Code:- 204,204,0

Key:- 8,3,7

VII. 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 McGrawHill

[2] "Security Using Colors and Armstrong Numbers" by S.Pavithra Deepa, S. Kannimuthu, V. Keerthika 1,3UG Student, Department of IT, Sri Krishna College of Engineering and Technology.

[3] "Introduction to algorithms" by Cormen, Leiserson, Rivest and Shamir

[4] http://aix1.uottawa.ca/~jkhoury/cryptography.htm