Message Security using Armstrong Numbers and Authentication using Colors

Mrs. G.V. Sowmya

Assistant Prof. Information Science and Engineering Dept, JNNCE, Shimoga, Karnataka, India

---***---

Abstract: In present 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 security data transmission there are several techniques being followed. One among them is cryptography which is the practice and study of hiding information. Data security has a major impact for securing data when it comes to accurately maintaining the confidentiality, authentication and integrity of the data.

Key words: *Encryption, Decryption, Armstrong number, colors, Authentication.*

1 INRTODUCTION

Cryptography, a word derived from Greek kryptos meaning "hidden", and verb graphein means "to write", is the process of making and using codes to secure the transmission of information. Cryptography is the art of secret writing. More generally, people think of cryptography as the art of mangling information into apparent unintelligible in a manner allowing a secret method of un-mangling. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. Here mainly concentrated on the kind of cryptography that is based on representing information as numbers and mathematically manipulating those numbers. This kind of cryptography can provide other services, such as Integrity checking— reassuring the recipient of a message that the message has not been altered since it was generated by a legitimate source. Authentication—verifying someone's (or something's) identity but back to the traditional use of cryptography. A message in its original form is known as plaintext or clear text. The mangled Information is known as ciphertext.

The process for producing ciphertext from plaintext is known as encryption. The reverse of encryption is called decryption.

Cryptography is the art and study of hiding information i.e. technique to convert plain text into ciphertext. Ciphertext is the message or data in unreadable format. Transformation of plain text into ciphertext is done with the help of key it can be secret key or public key. This process is nothing but an encryption process. Decryption is the reverse process of encryption in which cipher text is converted back into plain text (Original message) again with the help of key.

Cryptography is a branch of cryptology dealing with the design of algorithms for encryption and decryption, intended to ensure the secrecy or authenticity of messages. In modern times, cryptography is considered to be a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering. Cryptography is used in many applications in everyday life which includes the security of ATM cards, computer passwords and electronic commerce, all of which depends on cryptography.

2 LITRATURE SURVEY

S. Belose et.al., [1] proposed "Data Security Using Armstrong Number". In proposed approach they have maintained server database with following fields-Unique name and id of sender and receiver, and encrypted key (Armstrong Number). Now, if sender "A" wants to send data to receiver "B", then he encrypts that data using randomly generated Armstrong number. That encrypted data is identified by unique timestamp given to it and sent to receiver. At the same time key (Armstrong Number) of encrypted data is sent to server with receiver "B" id and file name. Whenever receiver get that encrypted data he simply request for key to server. Now actual authentication is done by server, Server takes request from receiver with file name and receivers self id, and compare it with senders key name and receiver id. If both match then only that key is send to the receiver. Whenever receiver gets key now he can decrypt that data easily.

T. Udepal Singh, et.al., [2] "An ASCII value based text data encryption System" paper proposes an algorithm to encrypt and decrypt the data base on symmetric key encryption technique. The proposed system is generating very good results. In future, the system can be further improved by using variable length key.

Priyanka Vora, et.al., [3] presented "Data Security using colors and Armstrong Numbers". The system uses divide and conquer strategy to exploit distributed processing. A divide and conquer algorithm works by recursively breaking down a problem into two or more sub-problems of the same (or related) type (divide), until these become simple enough to be solved directly (conquer). The solutions to the sub problems are then combined to give a solution to the original problem.

3 CRYPTOGRAPHICAL TECHNIQUES - A REVIEW

Cryptography is the art and study of hiding information that is technique to convert plain text into cipher text. Ciphertext is the message or data in unreadable format. Transformation of plain text into cipher text is done with the help of key it can be secret key or public key. This process is nothing but an encryption process. Decryption is the reverse process of encryption in which ciphertext is converted back into plain text again with the help of key.

RGB color model: The RGB color model is an additive color model in which red, green and blue light are added together in various ways to reproduce a broad array of colors. The name of the model comes from the initials of the three additive primary colors red, green and blue. The main purpose of the RGB color model is for the sensing, representation and display of images in electronic systems, such as televisions and computers, though it has also been used in conventional photography.

An Armstrong number is an n-digit base m number such that the sum of its (base m) digits raised to the power n is the number itself. Hence 371 is an Armstrong number because 33+73+13 =1 + 343 + 27 = 371.

4 SYSTEM ARCHITECTURE

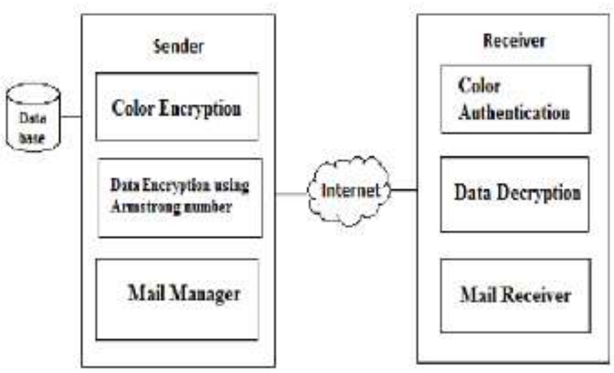

Figure 1 System Architecture

The overview of the system architecture is given below which is as shown in Fig.1

Sender: is the one who wishes to send the information to another person or group of person. Here the sender needs to enter his name and select the color for the receiver. The sender must also enter the secret key value. A database is a collection of information that is organized so that it can be easily accessed, managed and updated. It is maintained to save all the sender's name and the color values.

Color Encryption To encrypt the color, two values are needed.

Color value: The RGB values of the color, here the sender picks the color to be sent to the receiver.

Secret key: Secret key is the number that is given by the sender. The secret key can be any number positive or negative. The secret key values are added with the respective values of the RGB, this process encrypts the color. This encrypted color value is later on sent to the receiver.

5 IMPLEMENTATION

Encryption: The sender selects the color for the receiver and then encrypts the color value by adding it with the secret key. The message to be sent is chosen from the file and is then encrypted using Armstrong number. The cipher text thus generated and the encrypted color value is mailed to the receiver. Fig.2 illustrates the encryption program flow.

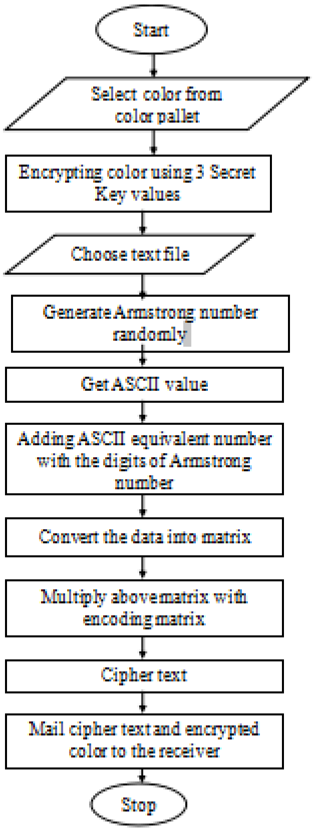
Start
Select color from color pallet
Encrypting color using 3 Secret Key values
Choose text file
Generate Armstrong number randomly
Get ASCII value
Adding ASCII equivalent number with the digits of Armstrong number
Convert the data into matrix
Multiply above matrix with encoding matrix
Cipher text
Mail cipher text and encrypted color to the receiver
Stop

Figure 2 Flow chart for Encryption

Decryption : The receiver receives the mail containing the ciphertext and encrypted color value. The encrypted color value is subtracted with the secret key which is entered by the receiver which he/she obtained through private channel communication. The color so obtained is compared with the actual color value. If there is a match then the user is an authenticated user else he/she is not a valid user. If the user is a valid user then it is possible to decrypt the message by using Armstrong number. This process is illustrated in Fig.3.

Color Authentication It is the act of confirming the truth of an attribute of a single piece of data claimed true by an entity. In this process the receiver is required to enter the sender's name and the encrypted color value which he receives through the e-mail. The receiver must also enter the secret key value which he receives through the private channel communications. The encrypted color value is then subtracted with the secret key value, this gives the color value. The value so obtained is compared with the actual color value which is retrieved from the database. If there is a match then the receiver is an authenticated user and is allowed to decrypt the message. If there is no match then the receiver is not allowed to decrypt the message.

Step 1 Sender wishes to send the data, first have to encrypt the color using following method. Now sender is aware about receiver's color and to whom he wants to send the data. If receiver's color values are (120, 35, 20) and key values are (10, 3, 4) So at the time of encryption we add key values to original color values

$$\begin{array}{rl} & 120\ 35\ 20 \\ (+) & 10\ 3\ 4 \\ \hline & 130\ 38\ 24 \end{array}$$

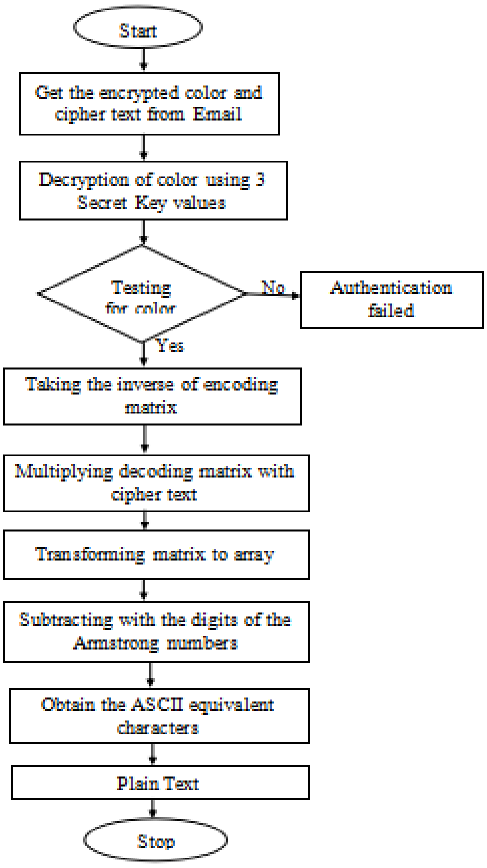
Start
Get the encrypted color and cipher text from Email
Decryption of color using 3 Secret Key values
Testing for color
No
Authentication failed
Yes
Taking the inverse of encoding matrix
Multiplying decoding matrix with cipher text
Transforming matrix to array
Subtracting with the digits of the Armstrong numbers
Obtain the ASCII equivalent characters
Plain Text
Stop

Figure 3 Flowchart of Decryption

Step 2 (Encryption of the actual data) Let the message to be transmitted be "SECURITYTECH First ASCII equivalent are taken of the above characters.

S E C U RI TY T E C H

83 69 6785 82 73 84 89 84 69 67 72

Step 3

Add ASCII equivalent numbers with the digits of the Armstrong number as follows,

$$\begin{array}{rl} & 83\ 69\ 67\ 85\ 82\ 73\ 848984\ 69\ 67\ 72 \\ (+) & 3\ 7\ 1\ 9\ 49127\ 343\ 1371 \\ \hline & 86\ 7668\ 94\ 131\ 74\ 111\ 432\ 85\ 7274\ 73 \end{array}$$

Step 4

Convert the above data into matrix as follows,

$$A= \begin{bmatrix} 86 & 94 & 111 & 72 \\ 76 & 131 & 492 & 74 \\ 68 & 74 & 85 & 73 \end{bmatrix}$$

Step 5

Encoding matrix is as follows,

$$B= \begin{bmatrix} 3 & 7 & 1 \\ 9 & 49 & 1 \\ 27 & 3431 & \end{bmatrix}$$

C=B X A

$$C= \begin{bmatrix} 858 & 1273 & 3442 & 807 \\ 4566 & 7339 & 22252 & 4347 \\ 28458 & 47545 & 151258 & 27399 \end{bmatrix}$$

The encrypted data is as follows,

858,4566,28458,1273,7339,47545,3442,22252,151258,807,4347,27399

Decryption process starts here,

Step 1

Authenticating the receiver color is used for authentication purpose only. When receiver want to read the data then he must be authenticated user and for that he have to decrypt the encrypted color using following method by subtracting key values.

$$\begin{array}{rl} & 130\ 38\ 24 \\ - & 10\ 3\ 4 \\ \hline & 120\ 35\ 20 \end{array}$$

Step 2

Decryption of encrypted data to get original message is as follows, First obtain the inverse of encoding matrix, $D=B^{-1}$.

$$D=\begin{pmatrix} -7/24 & 1/3 & -1/24 \\ 1/56 & -1/42 & 1/168 \\ 7/4 & -5/6 & 1/12 \end{pmatrix}$$

Step 3

Multiplication of the decoding matrix with the encrypted data is as follows,

$$D\ X\ C=\begin{pmatrix} -7/24 & 1/3 & -1/24 \\ 1/56 & -1/42 & 1/168 \\ 7/4 & -5/6 & 1/12 \end{pmatrix} X \begin{pmatrix} 858 & 1273 & 3442 & 807 \\ 4566 & 7339 & 22252 & 4347 \\ 28458 & 47545 & 151258 & 27399 \end{pmatrix}$$

$$=\begin{pmatrix} 86 & 94111 & 72 \\ 76 & 131\ 492 & 74 \\ 68 & 74\ 85 & 73 \end{pmatrix}$$

Step 4

Now transform the above result as given below,

86 76 68 94 131 74 111 432 85 72 74 73

Step 5

Subtracting with the digits of the Armstrong numbers.

$$\begin{array}{rl} & 86\ \ 76\ 68\ 94\ 131\ 74\ 111\ 432\ 85\ 7274\ 73 \\ (-) & 3\ 7\ 1\ 949\ 1\ 27\ 343\ 1\ 3\ 7\ 1 \\ \hline & 83\ 69\ 67\ 85\ 82\ 73\ 84\ 89\ 84\ 69\ 67\ 72 \end{array}$$

Step 6

Obtain the ASCII equivalent characters of above data.

83 69 67 85 82 73 84 8984 6967 72

S E C U R I TY T E C H

6 RESULT AND ANALYSIS

The different operations of the project include encrypting the color value, encrypting the data , authenticating the user and decrypting the data. All these operations are included as shown in Fig. 4 The sender needs to enter the name and select the color for the receiver from the color pallet which is as shown in Fig. 5After selecting the color the sender needs to select the input file to be encrypted. When the sender clicks the plain text button a file chooser appears from which the file is selected.

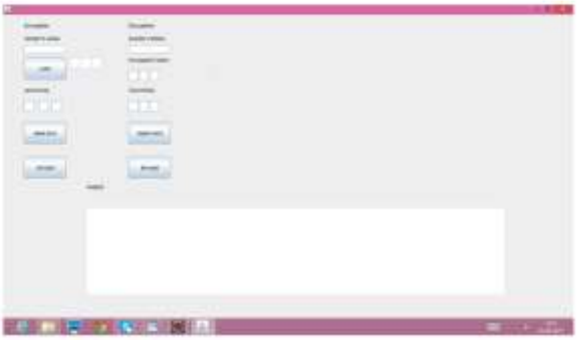

Figure 4

contents of the file is shown in the text area named as output. This is shown in Fig. 6.When the sender clicks the encrypt button, the message is encrypted and the resultant ciphertext is displayed in the output area. Email id of the receiver needs to be entered. This is shown in Fig. 7.

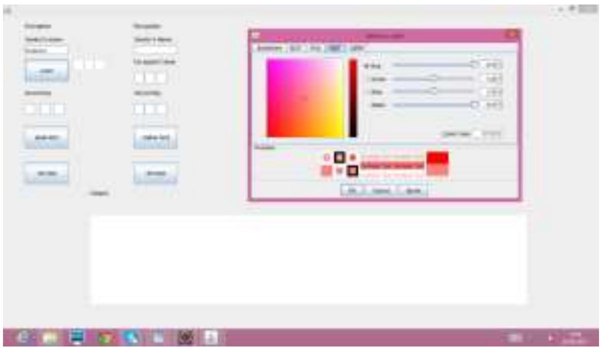

Figure 5

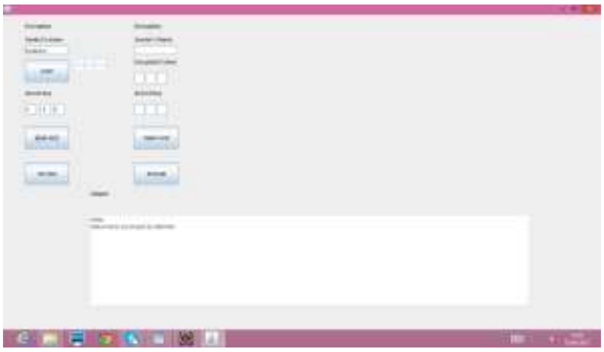

Figure 6

The receiver needs to enter the sender's name and the encrypted color value which is obtained through e-mail. The secret key value which is known through private communication is also entered. If there is a match between the entered value(encrypted value-secret key) and the color value stored in the database then the data is decrypted and the message is displayed in the output area. This is shown in Fig. 8.If the receiver enters wrong secret-key value or encrypted value then the receiver is not an authenticated user and decryption is denied which is shown in Fig.9 and Fig. 10.

Figure 7

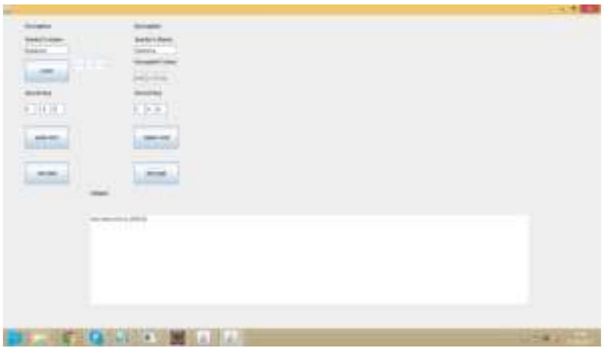

Figure 8

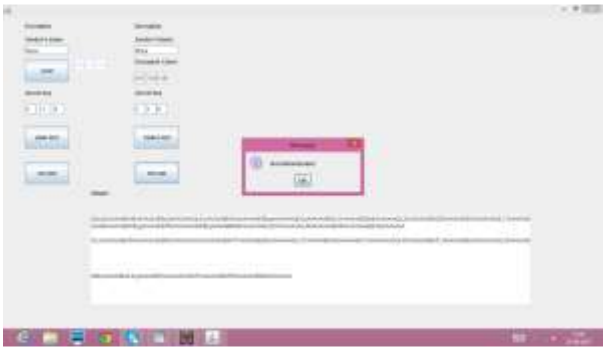

Figure 9

Figure 10

7 CONCLUSION AND FUTURE SCOPE

This Paper addressed the problem of security of the secret message. Hence a technique is proposed in which Armstrong numbers are used to provide more security. Colors, key values and Armstrong numbers which are three set of keys in this technique makes sure that there is secured message or data transmission and is available to authorized person. 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 that means in ASCII values, Second step by adding with the digits of the Encoding matrix to form the required encrypted data. Tracing process becomes difficult with this technique. This is because data is encrypted by key using Armstrong number and again this Armstrong number is encrypted by using as key so it is more secure.

Future Scope

In this Paper, range of Armstrong number is fixed to 3, but the range can be increased. The text is converted into ASCII equivalents this can be further extended to make use of Unicode for other languages.

REFERENCES

1. 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).

2. Udepal Singh, Upasna Garg, 'An ASCII value based text data encryption System',IJSRP , Volume 3, Issue 11, November 2013, ISSN 2250-3153.
3. Priyanka Vora, Kranti Sonawane,'Data Security Using Colours and Armstrong Number' International Journal of Electronics and Communication Engineering.ISSN 0974-2166 Volume 9, Number 1 (2016), pp. 13-18.
4. Gayatri Kulkarni, Pranjali Gujar, Madhuri Joshi, Shilpa Jadhav, "Message Security Using Armstrong Numbers and Authentication Using Colours" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014.
5. Mrunali Vaidya, Vaibhav Bansod, Mangesh Manwar, "A Review on Cryptography Using Armstrong Numbers and Colours", International Journal of Computer

Science and Mobile Computing, Vol.3 Issue.10, October- 2014.

6. Saleh Saraireh, "A Secure Data Communication System Using Cryptography And Steganography", International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013.