SECURITY USING COLORS AND ARMSTRONG NUMBERS FOR DATA STORAGE AND RETRIEVAL

KOLAPARTHI DIVYANAGA SATYA [#1], B.SURYANARAYANA MURTHY [#2]

[#1] MCA Student, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Associate Professor, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

Abstract

In real world, data security plays an important role in each and every aspect. The universal technique for providing confidentiality of transmitted data is cryptography. This project provides a new 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. So in this project we have used color as a major part for providing security for the data to be hidden as well as integrating Arm Strong number for that RGB pattern in order to give more security for the data. By Conducting various experiments and simulations on this new approach, we finally prove that this is the technique which was implemented for the first time to give more security for the sensitive data.

1. INTRODUCTION

In today's world, electronic media become a necessity. Cryptography is a way to make secure that electronic media. Data security plays an important role. Day by day hackers is becoming more powerful. So it is increasingly becoming more important to protect our valuable data Basically cryptography is used to protect valuable information resources on intranets, extranets and internet. 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

Most people are concerned with keeping communications private[4]. Encryption and decryption process is used to hide simple data from unauthorized users by converting it into unreadable form and again retrieve it in original form. Its purpose is to ensure privacy by keeping the data hidden from anyone for whom it is not intended. 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 the 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. Security is one of the major concerns of all the users irrespective of the domain in which they work. There are various ways by which one can ensure the security of the data which is present in different files on the computer.

Encryption-Decryption is one of those techniques which is quite popular[3]. Cryptography is the art and study of hiding information i.e. technique to convert plain text into cipher text i.e. encryption. Decryption in which cipher text is converted back into plain text with the help of the key. To maintain privacy and to prevent an unauthorized person from extracting information from the communication channel. 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 the three types of algorithms are depicted as follows

1) Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption.

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.[1][2]

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.

In the proposed system we use a new technique by integrating 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. 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 main objective of this present application is design a secure application by taking color and arm strong numbers as main parameters and then try to encrypt the sensitive data and send to the receiver under no attacks.

2. LITERATURE SURVEY

INRODUCTION

Literature survey is the most important step in software development process. Before developing the tool, it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, then next steps are to determine which operating system and language used for developing the tool. Once the programmers start building the tool, the programmers need lot of external support. This support obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

RELATED WORK

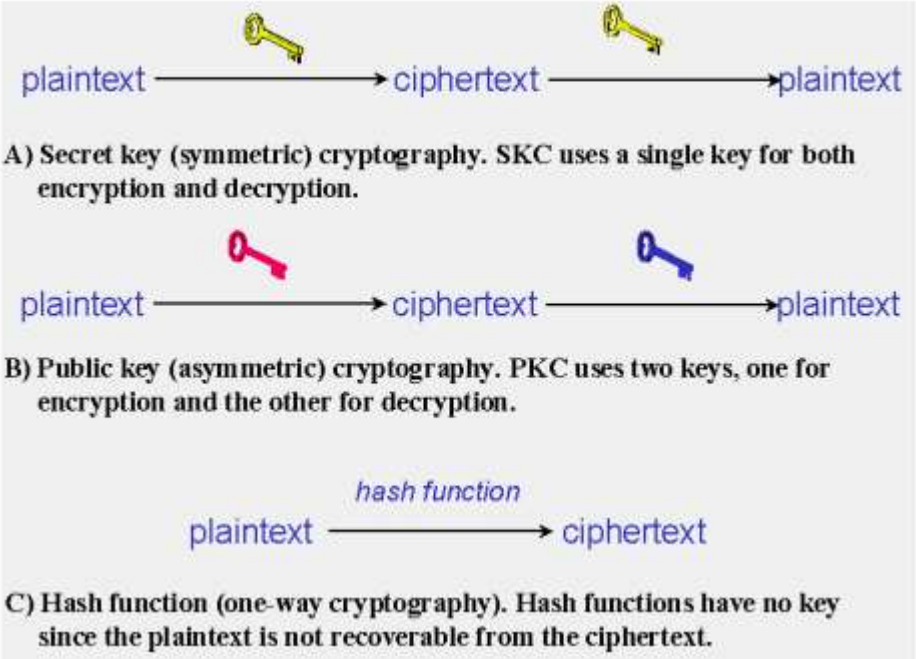
In the present world scenario it is difficult to transmit data from one place to another with security. This is because hackers are becoming more powerful nowadays. To ensure secured data transmission there are several techniques being followed. One among them is cryptography which is the practice and study of hiding information.

Cryptography, 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.

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.



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.

3. EXISTING SYSTEM

In the existing system for providing security for the data, user need to choose normal cryptography algorithms such as encryption and decryption by using general algorithms such as public key cryptography, private key cryptography and secret key cryptography. But all these algorithms take lot of effort and time to convert plain text into cipher and cipher text to plain text.

LIMITATION OF EXISTING SYSTEM

The following are the limitation of existing system. They are as follows:

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. There was no mechanism in the existing system to provide security using colors as the input paramenters.

4. PROPOSED SYSTEM

In the proposed system we use a new technique by integrating 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. 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.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system. They are as follows:

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.

The proposed system try to use color as one of the main parameter to provide security from the attacker and this will greatly increase the security from hackers

5. SOFTWARE PROJECT MODULES

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. We have implemented the proposed concept on Java programming language with JEE as the chosen language in order to show the performance this proposed novel IPath protocol. The front end of the application takes JSP,HTML and Java Beans and as a Back-End Data base we took My-SQL Server. They are totally 4 modules present in this project. They are as follows:

1. User Authentication
2. Receiver
3. Data hiding
4. Data decryption

Now let us discuss about each and every module in detail as follows:

5.1 User Authentication Module

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. 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.

4.8.2 Data Encryption Module

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.

5.2 Receiver Module

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

5.3 Data Decryption Module

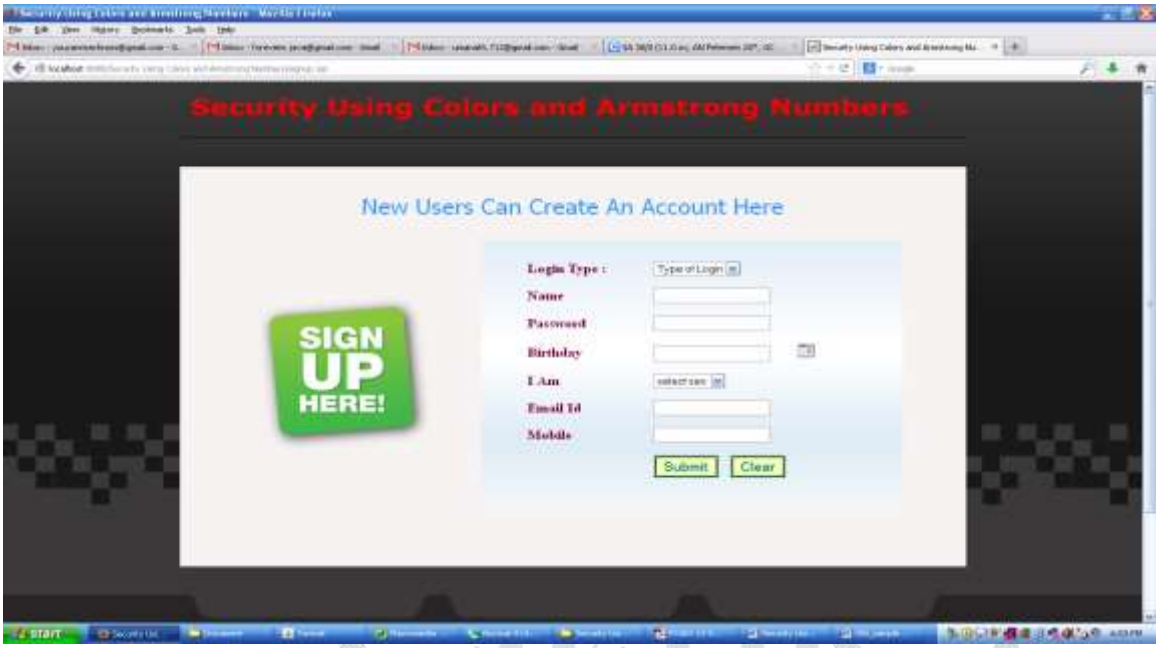
The data which is encrypted and hidden is received at the receiver side. The data is extracted now. The inverse of the encoding matrix (Armstrong number) is found, and it is the decoding matrix. On receiving the encrypted data, the data is rearranged to the original order, which is gives the correct 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.

6. RESULTS (OUTPUT SCREENS)

1) HOME PAGE

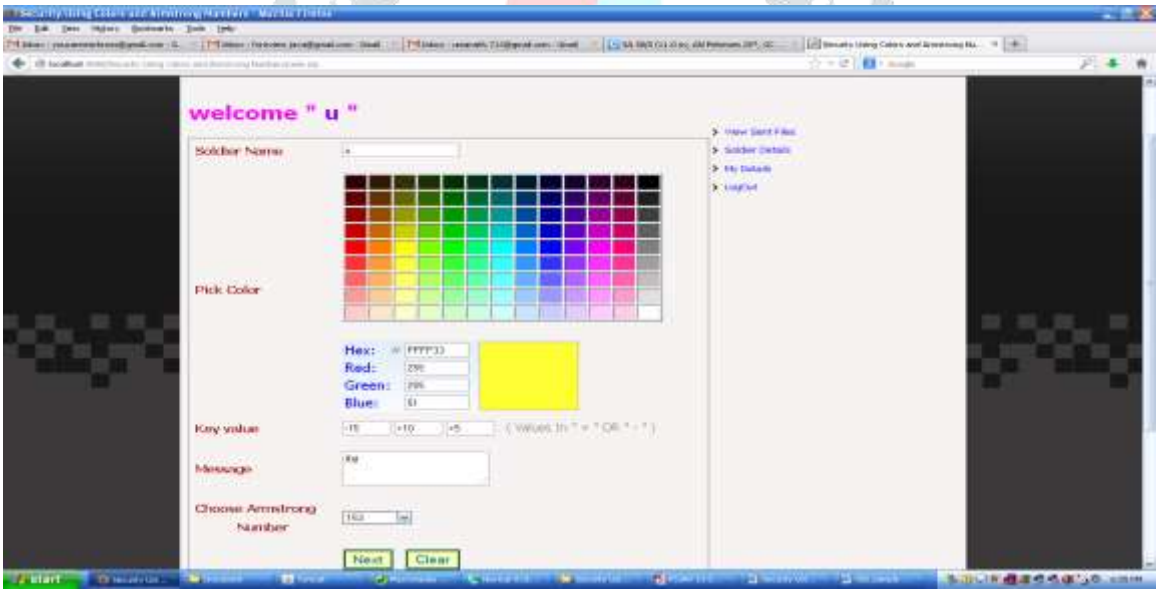
Represents the Home Page

USER REGISTRATION NEEDS THE FOLLOWING



Represents the Data User Registration

3) User choose Color Pattern While Registration



Represents the Data User Color Pattern

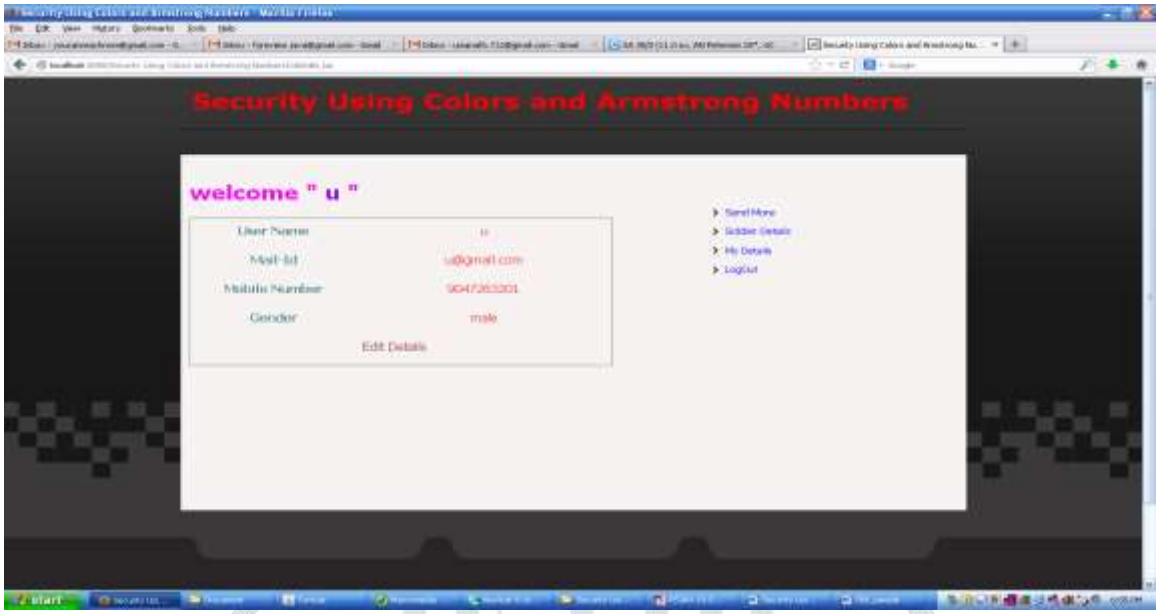
4) User Login and Home Page

Represents the Login and Home Page

5) Soldier Views the Message

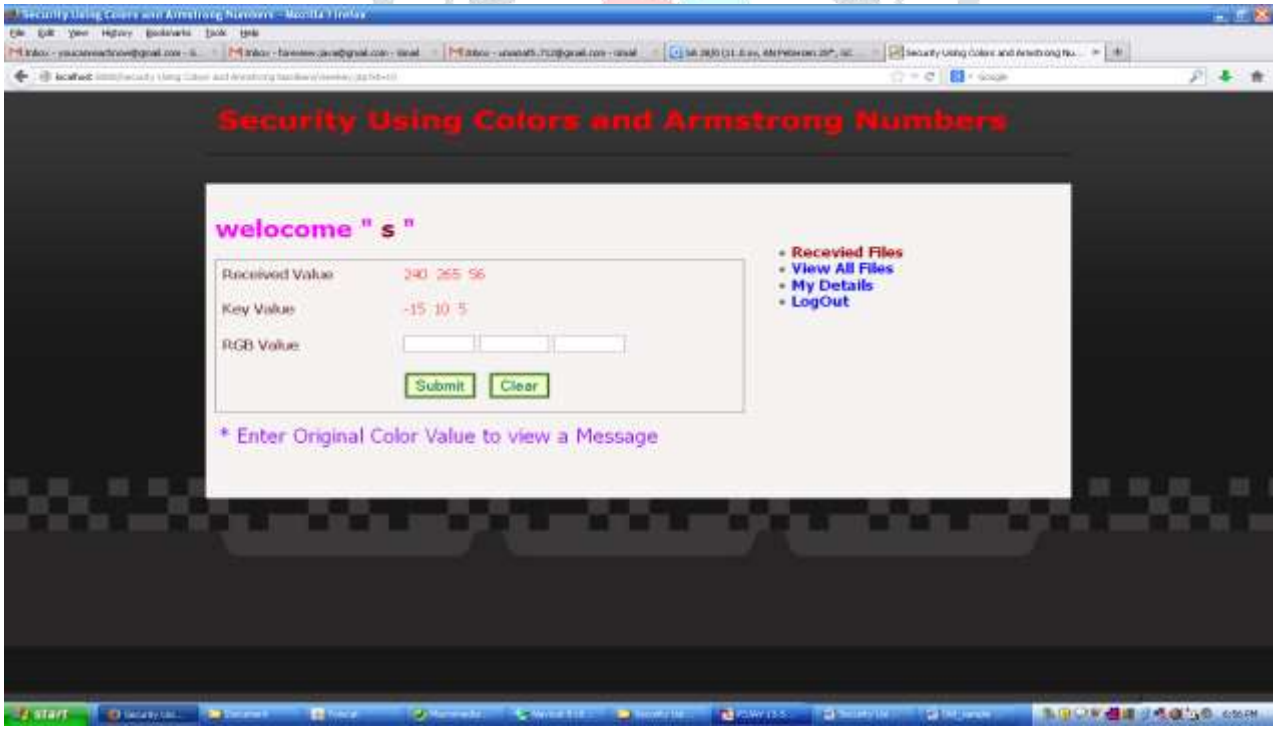
Represents the Soldier View Message In Encrypted Manner

6) USER TRY TO DECODE THE MESSAGE



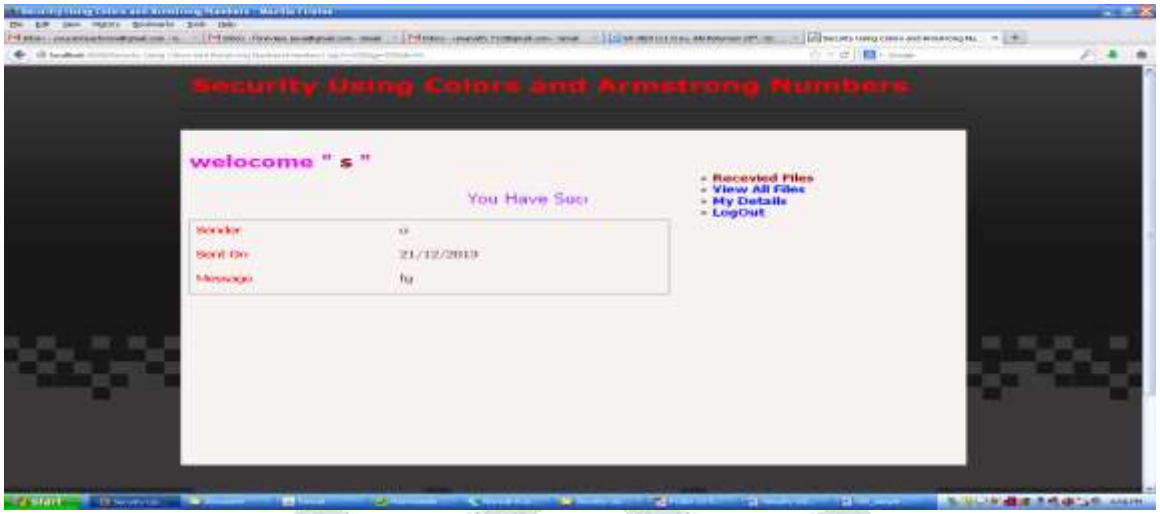
Represents the User Decode the Message

7) User is Asked to Match the Color Pattern



Represents the Color pattern Verification

8)PATTERN SUCCESS



7. 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.

8. REFERENCES

Good Teachers are worth more than thousand books, we have them in Our Department

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] http://java.sun.com

[5] http://www.sourcefordgde.com

[6] http://www.networkcomputing.com/

[7] http://www.roseindia.com/

[8] http://www.java2s.com/