International Journal of Electronics and Communication Engineering.
ISSN 0974-2166 Volume 9, Number 1 (2016), pp. 13-18

http://www.irphouse.com

Data Security Using Colours and Armstrong Numbers

Priyanka Vora
Department of Electronics andTelecommunication
Bharati vidyapeeth's College of Engineering for women,
Dhankawadi, Pune 411043, India

Kranti Sonawane
Department of Electronics andTelecommunication
Bharati vidyapeeth's College of Engineering for women,
Dhankawadi, Pune 411043, India

Sneha Phulpagar
Department of Electronics andTelecommunication
Bharati vidyapeeth's College of Engineering for women,
Dhankawadi, Pune 411043, India

Prof.A.P.Ydav
Department of Electronics andTelecommunication
Bharati vidyapeeth's College of Engineering for women,
Dhankawadi, Pune 411043, India

Abstract

In real world, data security plays an vital role where security, privacy, validation, integrity, non-repudiation is given importance. There are some common techniques used for secure data transmission over network.This paper provides a technique for data security which encrypt the data using a key involving Armstrong numbers and colours as the password. Three set of keys is used to provide secure data transmission with the colours acting as vital security element thereby providing authentication.

Keywords: secure data transmission, Armstrong numbers, validation, Cryptography, Colors.

I.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]

II.PROPOSED SYSTEM

In our system, we are using 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. In this technique, we are using the some functions of a previous module into next module. In this system, the receiver side modules depend on the sender side modules. Until sender side modules are not developed, we cannot develop receiver side modules. So that, this system execute in distribute manner.

Modules:
Proposed system mainly consists of four modules,
- Color encryption
- Data encryption
- Color decryption
- Data decryption

SENDER MODULE:
This module is used to generate cipher text by applying colour encoding and data encryption. Every sender and receiver have a unique colour, which is selected by itself.

a) Colour Encryption Module:
Step 1: Select random image
Step 2: Click on any pixel of an image. If we click on image pixel then we get RGB colour values of that pixel. Consider RGB value is (107, 55, 57)
Step 3: Divide that RGB values by 10. We get key (10, 5, 5)
Step 4: Add this key (10, 5, 5) to the receivers unique colour. Consider the colour is pink (255,192,203).

255 192 103
+ 10 5 5
265 197 108

If the encoded value is greater than 255 then change the sign of the key values like (-10, 5, 5) and the new encoded values are (245, 197, 108).
Step 5: Finally sender sends this encoded colour values to the receiver.

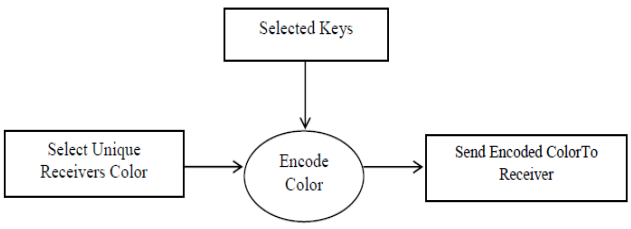

Fig1: color encryption

b) Data Encryption Module:
Step 1: Select Armstrong number randomly which is not contain the zero digit.
Step 2: Convert plaintext into ASCII equivalent.
Step 3: Add ASCII number with the digits of Armstrong number
Step 4: Convert result produce by this operation is converted into the matrix.
Step 5: Convert Armstrong number into the matrix
Step 6: Multiply the above two matrices and finally get the encrypted value.Encrypted values converted into the form of message like (779, 3071, 135, 742…)
Step 7: Send this message to the receiver.

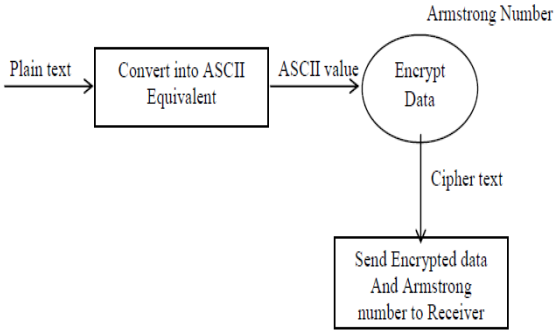

Fig2: Data Encryption

RECEIVER MODULE:
This module is used for authentication of the receiver and actual data decryption. At the receiver side, both modules depend on sender side modules. The authentication module depends on the colour encryption module and data decryption module depends on the data encryption module. So that until sender side module will not develop we cannot develop receiver's modules.

a) Authentication Module:
Step 1: Receiver receives the encoded colour and key value which is assigned by the sender.
Step 2: decode the encoded colour by subtracting the key value from the encoded colour value and get back the original colour of receiver.
Step 3: Check the original colour with a database.
Step 4: If the colour is matched then the receiver can access the encrypted data.

b) Data Decryption Module:
Step 1: convert the cipher text into the matrix.
Step 2: take the inverse of cipher text matrix.
Step 3: multiply inverse matrix with the cipher text matrix
Step 4: The result produce by this operation is converted into equivalent values like (779, 3071, 135, 742…)

Step 5: subtract Armstrong number from this resulted values.
Step 6: Convert this values into character i.e receiver get the original plain text.

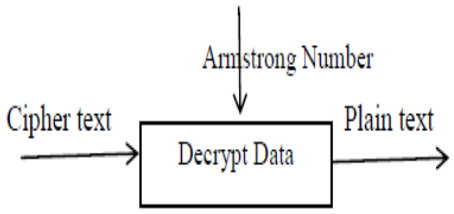

Fig3: Data Decryption

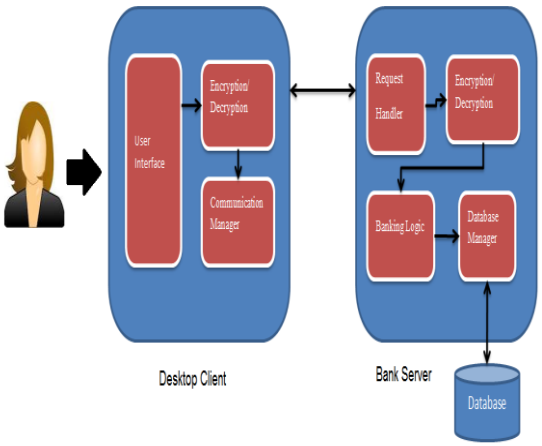

Fig4: Architectural Design

III.ADVANTAGES:

Colors are used for the authentication purpose. The range of color is 2^0 to 2^24. RGB model uses 24 bits, 8 bits for each color. To encrypt the data set of three key values are added to the original color values. This encrypted color acts as a password. To break this password attacker has to check 256^3 possible values which are practically most difficult. The combination of substitution and permutation process increases the data security. To increase the strength of algorithm 9 digits, Armstrong number is used for encryption and decryption, a length of an Armstrong number can be increased if necessary for security purpose.

IV.CONCLUSION:

Thus, we addressed the problem of security of secret message. Hence, a technique is proposed in which Armstrong numbers are used instead of prime numbers to provide more security. The confidential areas like military, banking sector, governments are

targeted by the system where data security is given more importance. 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

V.REFERENCES

[1] Security Using Colors and Armstrong Numbers-NATIONAL CONFERENCE ON INNOVATIONS IN EMERGING TECHNOLOGY YEAR 2011

[2] Message Security Using Armstrong Numbers and Authentication Using Colors-International Journal of Advanced Research in Computer Science and Software Engineering January 2014

[3] Data Security Using Armstrong Numbers-International Journal of Emerging Technology and Advanced Engineering April 2012

[4] Data Security in Message Passing using Armstrong Number-International Journal of Computer Science Trends and Technology (IJCST)-Mar-Apr 2014