International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Message Security Using Armstrong Numbers and Authentication Using Colors

Vaibhav Sonavane*, Jyoti Soni, Aadil Ansari, Ikram Hussain
Computer Engineering Department, Mumbai University, India

ABSTRACT

Today's world is all based on information technology. Hence data security plays an important role. Hackers are becoming more active nowadays. Unsecured networks can be hacked into easily, and hackers can do lots of things in short amounts of time. Hence it is mandatory to increase security to protect our important data. There are some techniques used to make data transmission with protection. Cryptography is one of them. This project provides a technique in which Armstrong number is used for encryption of message. Colour is important in authentication process as it acts as password. Using this technique, message is hidden from unauthorized people and accessible to an authorized individual when required.

Keywords : Cryptography, Authentication, Secure data transmission, Armstrong numbers, validation, Colors

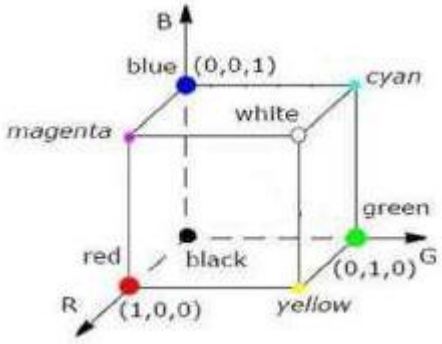
I. INTRODUCTION

1.1 Introduction Concepts for project

In today's world scenario it is difficult to transmit data from one place to another with security .Secure data transmission is really difficult because of the hackers. Cryptography is the universal technique for providing security to confidential data. The main goals is to ensure privacy by keeping the data hidden from anyone for whom it is not intended. It consists of encryption and decryption processes. Encryption and decryption have need of some secret information, usually referred to as a key. The same key might be used for both encryption and decryption depending on the encryption mechanism. While for other mechanisms, the keys used for encryption and decryption might be different.

1. RGB representation

Any color is the mixture of three colors RGB (Red, Green and Blue) in present quantities. This is nothing but a RGB representation. Here values for Red, Green and Blue represent each pixel. So any color can be individually represented with the help of three dimensional RGB cube. RGB model uses 24 bits, 8 bits for each color. Hence colors are used as a password for authentication purpose. Then encryption or decryption process takes place.



2. Armstrong number

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 3^3+7^3+1^3 =1 + 343 + 27 = 371.

1.2 Problem Definition

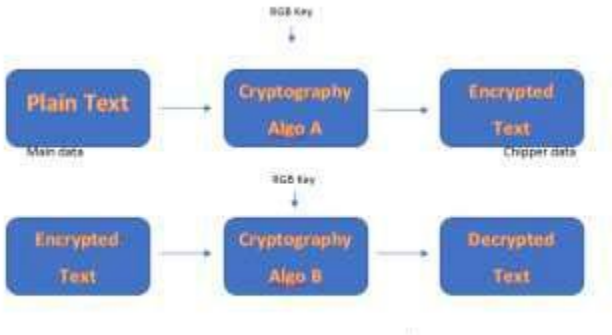
There are many algorithms for encryption decryption process like AES, DES, RSA in which

encryption is done with the help of substitutions and transformations on the plaintext. It uses prime numbers for encryption process.

A. Cryptography using secret key (SKC): Secret key is a value independent of a plaintext and of the algorithm. Single key is used for both encryption and decryption by an algorithm. It includes Data Encryption Standard (DES) and Advanced Encryption Standard (AES).

B. Cryptography using Public Key (PKC): Two different keys are used in this. One key is used for encryption and another for decryption. It includes Rivest, Shamir, Adleman (RSA) algorithm.

C. Hash Functions: It uses mathematical transformation for encryption which is not recoverable from the cipher text.



Basic Concept

1.3 Scope of Project

The project have lots of scope in future and in present also, the technique which we are using involves keys with a minimum length of 8 bits for Armstrong numbers. This minimum key length reduces the efforts taken to encrypt the data. We can also increased key length if needed, with increase in character length. This increases the complexity thereby providing highly increased security.

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, 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.

II. REVIEW OF LITERATURE

The use of public-key cryptography is persistent in the information protection and privacy areas. Public key cryptography algorithms utilize prime numbers broadly because prime numbers are a crucial part of the public key systems. This technique ensures that using two main steps data transfer can be performed with protection. First step is to convert the data into ASCII form, then by adding with the digits of the Armstrong numbers. Second step is to encode using a matrix to generate the required encrypted data. Tracing process becomes difficult with this technique. This is because in each step the Armstrong number is used in different way. Three different keys are used namely the colors, key values added with the colors and Armstrong numbers. Data can be retrieved only if all the three key values along with this technique is known. Simple encryption and decryption techniques may just involve encoding and decoding the actual data. But in this proposed technique the password itself is encoded to provide more security to the access of original data. Armstrong numbers and colors are used in this technique. The sender is attentive of the required receiver to whom the message has to be sent.

III. PLANNING & FORMULATION FEASIBILITY REPORT

The very first phase in any system developing life cycle is preliminary investigation. The feasibility study is a major part of this phase. A measure of how beneficial or practical the development of any information system would be to the organization is the feasibility study.

The feasibility of the development software can be studied in terms of the following aspects:

1.Operational Feasibility.
2.Technical Feasibility.
3.Economical feasibility.
4.Motivational Feasibility.
5.Legal Feasibility

IV. METHODOLOGY

4.1 Proposed System

In proposed system Armstrong numbers are used for encryption purpose while existing system uses prime number. Colour is used for authentication purpose. Basic concept is that unique colour is assigned to each receiver. This unique colour acts as password. The sender knows required receiver to whom the data has to be sent. There can be N numbers of receivers who can access the encrypted data if they are authorized (N≤224). Firstly, encryption of colour is done by adding key values to the original colour values at sender's side. This encrypted colour acts as a password. Then data is encrypted using Armstrong numbers. At the receiver's side when the receiver enters secret key, decryption of colour takes place. The decrypted colour is then matched with colour assigned by sender i.e. original colour stored at the sender's database. Without the secret key, there is no way for user to access the data.

Data at sender and receiver end

Further a combination, substitution and permutation methods are used with Armstrong number to ensure data security. S For encryption it converts each letter to its ASCII equivalent by substitution method and permutation is done with the help of Armstrong number. Later it converts that data into matrix form. It performs permutation process by using matrices. Receiver will perform in reverse manner.

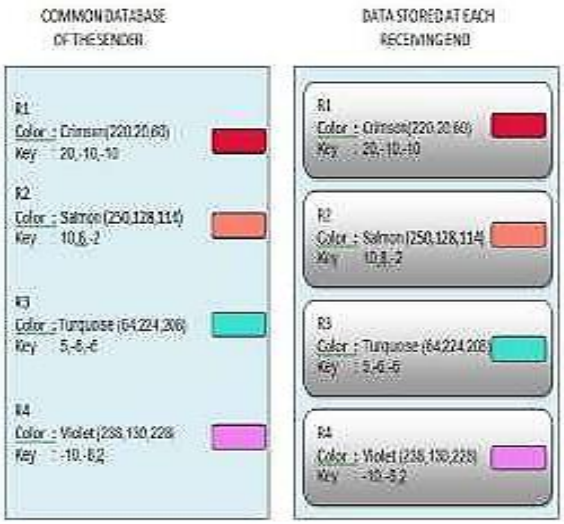
4.2 Proposed Methodology

Admin Module:-
1. Admin login into the application using username and password .
2. Admin manages employees of the organization.
3. In the upload file module

- ✓ admin select the file which he have to share with the employee.
- ✓ Select the employee username with whom he have to share a file.
- ✓ Allocate the color to each employee during file share
- ✓ Select the Armstrong no which is use for file encryption which is use as a key for file encryption.
- ✓ When admin click on upload button, colors RGB value get send on users email id and file get encrypted using Armstrong number and that encrypted file get loaded on server.(that RGB value is use as a authentication key for the employee).

Employee Module:-

- ✓ Employee login into the application using username and password.
- ✓ Employee can view the name of the file which is share by the admin.
- ✓ Employee click on download hyperlink
- ✓ Then employee have to enter the RGB value into the textbox. If the value of the RGB value get matches then file get decrypted by using Armstrong no and get download into the system. Else it will show invalid user key error message.
- ✓ Employee can change the password if required.



V. CONCLUSION & FUTURE SCOPE

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, governments are targeted by the system where data security is given more importance. Colors, key values 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.

VI. REFERENCES

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

[2]. http://mathworld.wolfram.com/UnimodularMatrix.html

[3]. S. Pavithra Deepa,S. Kannimuthu, V. Keerthika., "Security Using Colors and Armstrong Numbers", Proceedings of the National Conference on Innovations in Emerging Technology-2011. India.17 & 18 February, 2011.pp.157-160.

[4]. http://www.scribd.com/doc/29422982/Data-Compression-andEncoding-Using-Col

[5]. 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).

[6]. Chavan Satish, Lokhande Yogesh, Shinde Pravin,

[7]. Yewale Sandeep, Sardeshpande S. A, "Secure Email using Colors and Armstrong Numbers over web services", International Journal Of Research

[8]. In Computer Engineering And Information Technology VOLUME 1 No.

[9]. Atul Kahate, "Cryptography and Network Security", Tata McGraw Hill Publications.