

## Security Using Colors and Armstrong Numbers

### Synopsis:-

In real world, data security plays an important role where confidentiality, authentication, integrity, non repudiation are given importance. The universal technique for providing confidentiality of transmitted data is cryptography. 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.

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.

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.

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. Thus any color can be uniquely represented in the three dimensional RGB cube as values of Red, Green and Blue.

Therefore, in our approach we make use of colors whose values serve as a password for initial authentication and encryption decryption process.

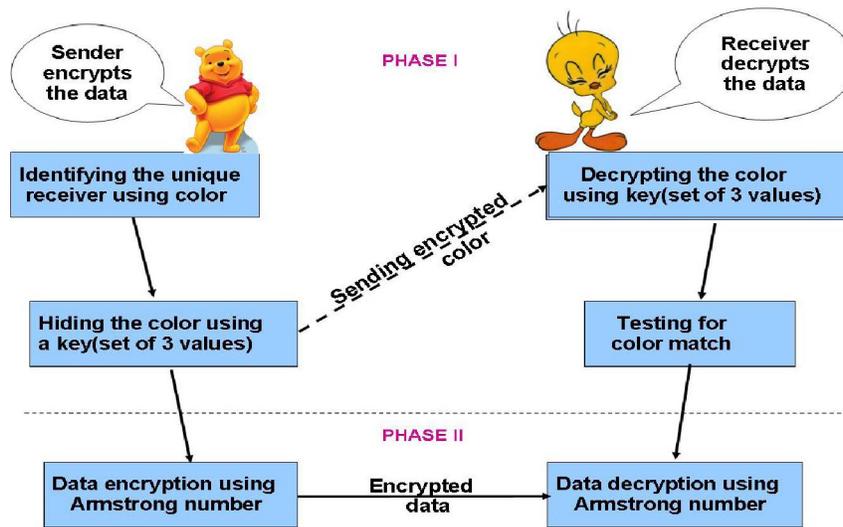
### Existing System:-

- 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. 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).

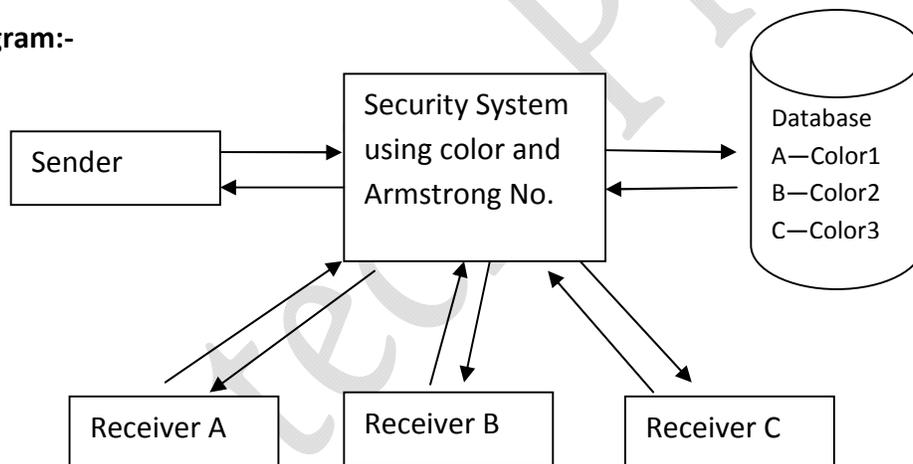
### Proposed System:-

- 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 and assigns a set of three key values to each receiver. 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.
- As a step further ahead let us consider a technique in which we use Armstrong numbers and colors. 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. Permutation process is performed by using matrices as in an Armstrong number.
- The reverse is performed by the receiver. And the receiver is validated by the use of his unique color.

## Architecture:-



## Block Diagram:-



## System Requirements:-

LAN Connection.

Software used:-Java , J2EE.

Database:- Mysql 5

## Application-

- Applicable area where security issues are considered on high priority.