

# Data Security Using Armstrong Number

## Abstract:

In today's world data security during transmission is very important. Data Security refers to the protection of data from unauthorized users in a way such that confidentiality, authentication, integrity, non repudiation are given importance. This can be achieved by using cryptography. This project provides a technique to encrypt the data using a key involving Armstrong numbers and colors as the password. The key is passed between the sender and the receiver by using Diffie Hellman key exchange algorithm. A set of Keys are used to provide secure data transmission with the Colors acting as vital security element thereby providing authentication. To make the Authentication between two intended users along with the security, server is used. With the help of server, both sender and receiver will get validated. Then actual data could be transmitted by any of the means. Central server system is used to provide secure intended Authentication between users. 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.

## **EXISTING SYSTEM:**

Now a days, to make secure data transmission different methods are used. One of the techniques is Cryptography, in this 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. Security is one of the major concerns of all the users irrespective of the domain in which they work. The existing techniques involve the use of keys involving prime numbers and the like. There are various ways by which one can ensure the security for the data which is present in different files in the computer. Encryption-Decryption is one of those techniques which are quite popular. But, the complexity which is involved in this technique doesn't allow its users to apply it in a simpler way. Now, if we look into the detailed context of this technique then we may observe that there are number of ways which allows the user to encrypt the private files and information.

## **DISADVANTAGES OF EXISTING SYSTEM:**

- The existing techniques involve the use of keys involving prime numbers and the like.
- Simple encryption and decryption techniques may just involve encoding and decoding the actual data.
- The existing system not provides more security with increase in key length of the prime number

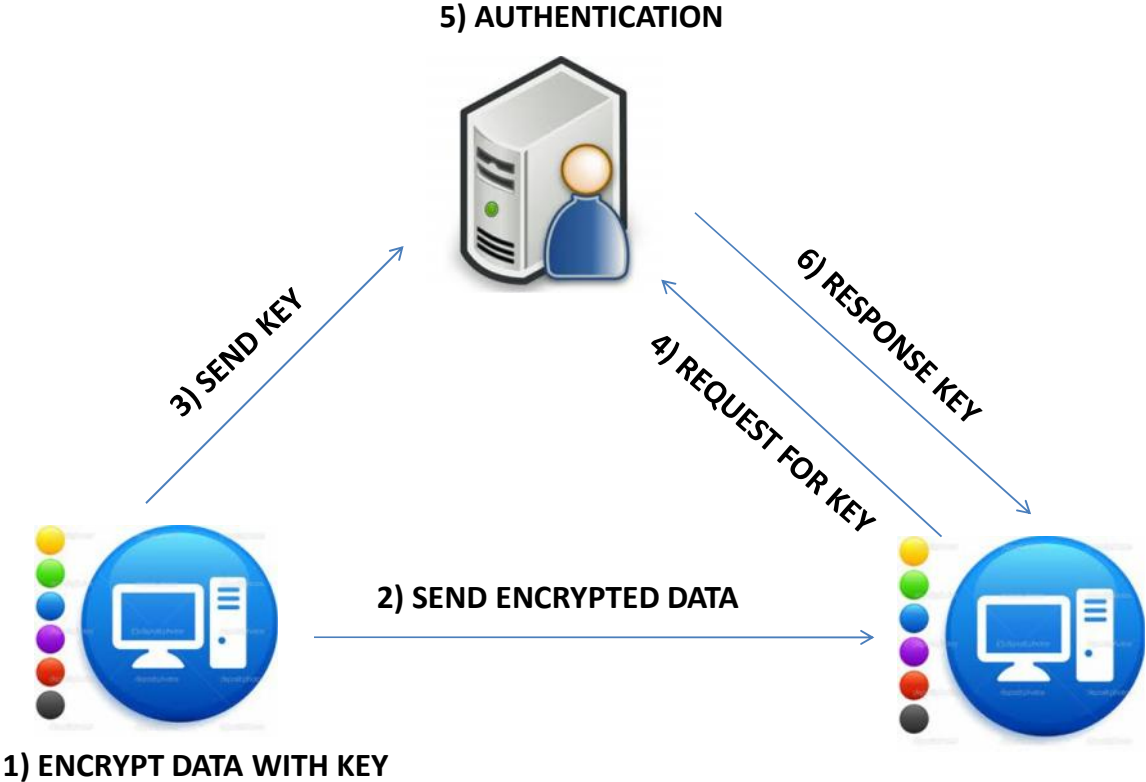
## **PROPOSED SYSTEM:**

In proposed approach we maintain 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.

## **ADVANTAGES OF PROPOSED SYSTEM:**

- This technique ensures that the data transfer can be performed with protection.
- Tracing process becomes difficult with this technique. So hacking becomes difficult mainly because of the usage of colors.
- This technique is applicable to any type of encryption algorithm.
- This hides the encrypted content. The hacker never realizes what the content is.

SYSTEM ARCHITECTURE



## **System configuration:**

### Software Requirements

- Front End : Java
- Back End : SQL Server 2005
- Operating System : Windows XP/07
- IDE : Net Beans, Eclipse

### Hardware Requirements:

- Processor : Pentium -III
- Speed : 1.1 GHz
- RAM : 256 MB(min)
- Hard Disk : 20 GB
- Key Board : Standard Windows Keyboard
- Mouse : Two or Three Button Mouse
- Monitor : SVGA