SECURITY USING COLORS AND ARMSTRONG NUMBERS

[1]Mrs.S.Kavitha, [2]Mr.K.D.SatishKumar, [3]Mr.M.SaravanaPandi, [3]Mr.R.Srinivasan@Balu
[1]Assistant professor, [2]UG Student, [3]UG Student, [4]UG Student
[1]Computer Science and Engineering,
[1]Velammal college of Engineering and Technology, Madurai, India

Abstract : In real world, data security working 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.

Index Terms - Security, Armstrong numbers ,Cryptography.

I. INTRODUCTION

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. Indeed, the protection of sensitive communications has been the emphasis of cryptography all through much of its history. 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, even those who can see the encrypted data. Decryption is the reverse of encryption; it is the transformation of encrypted data back into some intelligible form. Today governments use sophisticated methods of coding and decoding messages. One type of code, which is extremely difficult to break, makes use of a large matrix to encode a message. The receiver of the message decodes it using the inverse of the matrix. This first matrix is called the encoding matrix and its inverse is called the decoding matrix An Armstrong number is an n-digit base b number such that the sum of its (base b) digits raised to the power n is the number itself. Hence 153 because 13 + 53 + 33 = 1 + 125 + 27 = 153.

Much more information can be found at the site of Lionel Deimel. The most principal information is that the number of Armstrong numbers for a particular base is finite. So, theoretically, you could list all Armstrong numbers up to a particular base, and that is what I have done, using a program of course. My first program was pretty fast compared to what I have found later in the literature. For instance I found references of weeks of computing all base 10 Armstrong numbers while my program did it at that time in about 34 minutes. Compare that to my current desktop computer (fairly old) which does it in 11 minutes, and my next desktop computer which will perform the same feat in 1.5 minutes! But searching times will be exponential on the base. The last base I did on the old computer (a CDC Cyber) was 12, and it took 36 hours 6 minutes and 30.061 seconds back in 1985. Later (1997) we had faster local computers so I could complete the search until base 16, but it still took quite some time. As far as I know it took slightly less than a year to complete base 16. So I will not continue on this path. The results can be found in the table.

II. 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:

- *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).
- *Public Key Cryptography (PKC):* Uses one key for encryption and another for decryption. RSA (Rivest, Shamir, Adleman) algorithm is an example.

- *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).

III. Proposed system

- In this technique the first step is to assign a unique color for each receiver. So the receiver's unique color is used as the password.
- The set of four color values are added to the original color values and encrypted at the sender's side. This encrypted color actually acts as a password.
- 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 and Armstrong number.
- The reverse is performed by the receiver. And the receiver is validated by the use of his unique color.

3.1 Purpose

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.

3.2 Projects Scope

Encryption and decryption require the use of some secret information, used for new technology as color and Armstrong number usually referred to as a key. 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.

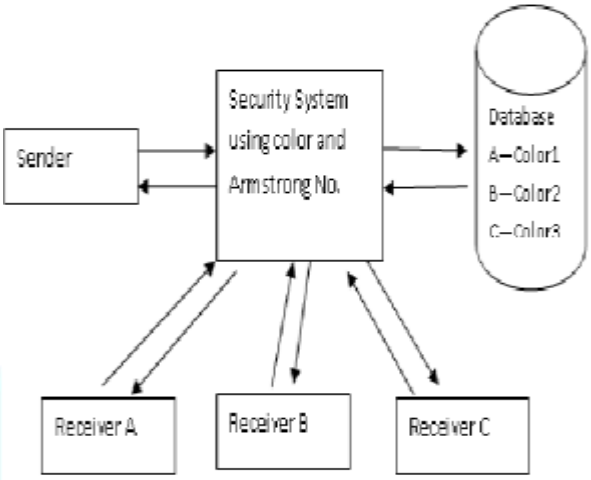
IV. Literature Survey

The use of public-key cryptography is pervasive in the information protection and privacy arenas. Public key crypto algorithms utilize prime numbers extensively; indeed, prime numbers are an essential part of the major public key systems. This paper provides an introduction to prime numbers and how they are chosen, identified and used in public key systems. The content of this paper is specifically targeted at an audience that has only basic mathematical knowledge. A reader who has taken a high school or college algebra class should be able to follow the math herein. The objective of this paper is to inform the mainstream information security professional – who does not necessarily possess an extensive knowledge of mathematics – about the nature of prime numbers and how they are used in contemporary public key systems, thereby increasing his/her overall understanding of contemporary asymmetric encryption algorithms. As part of this investigation the basic elements of Diffie- Hellman exchange and the RSA algorithm are explored.

This technique ensures that the data transfer can be performed with protection since it involves two main steps. First step is to convert the characters into another form, by adding with the digits of the Armstrong numbers. Second step is to encode using a matrix to form the required encrypted data. Tracing process becomes difficult with this technique. This is because the Armstrong number is used differently in each step. The key can be hacked only if the entire steps involved in the encoding process is known earlier. This technique could be considered as a kind of triple DES algorithm since we use three different keys namely the colors, key values added with the colors and Armstrong numbers. Unless all the three key values along with the entire

encryption and decryption technique is known the data cannot be obtained. So hacking becomes difficult mainly because of the usage of colors. Simple encryption and decryption techniques may just involve encoding and decoding the actual data. But in this proposed technique the password itself is encoded for providing more security to the access of original data.

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 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..

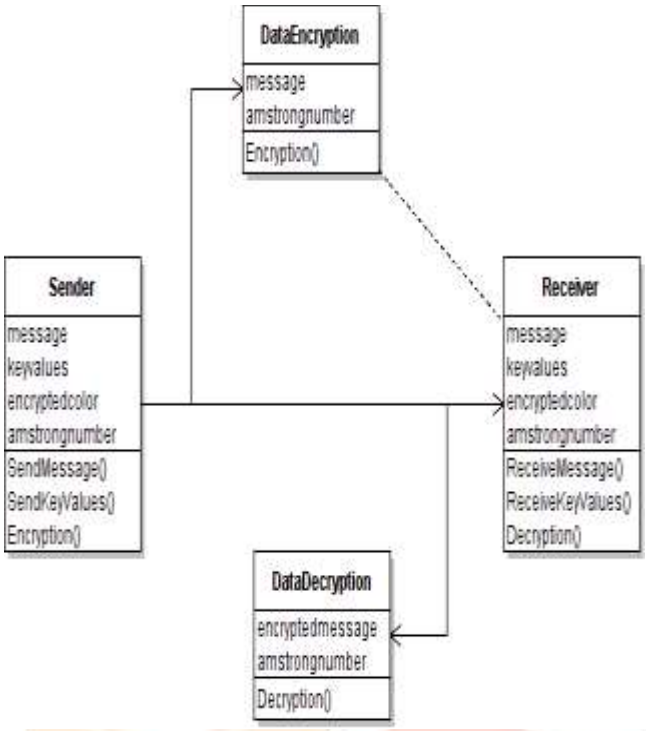


We perform the substitution process by assigning the ASCII equivalent to the characters. Permutation process is performed by using matrices as in [2] and Armstrong number. In this technique the first step is to assign a unique color for each receiver. Each color is represented with a set of three values. 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. This encrypted color actually acts as a password. The actual data is encrypted using Armstrong numbers. At the receiver's side, the receiver is aware of his own color and other key values. The encrypted color from the sender decrypt by subtracting the key values from the received set of color values. It is then tested for a match with the color stored at the sender's database. Only when the colors are matched the actual data can be decrypt using Armstrong numbers. Usage of colors as a password in this way ensures more security to the data providing authentication. This is because only when the colors at the sender and receiver's side match with each other the actual data could be accessed

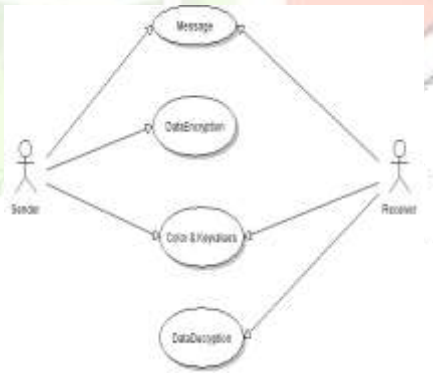
V. Overall Descriptions

5.1 User Classes and Characteristics

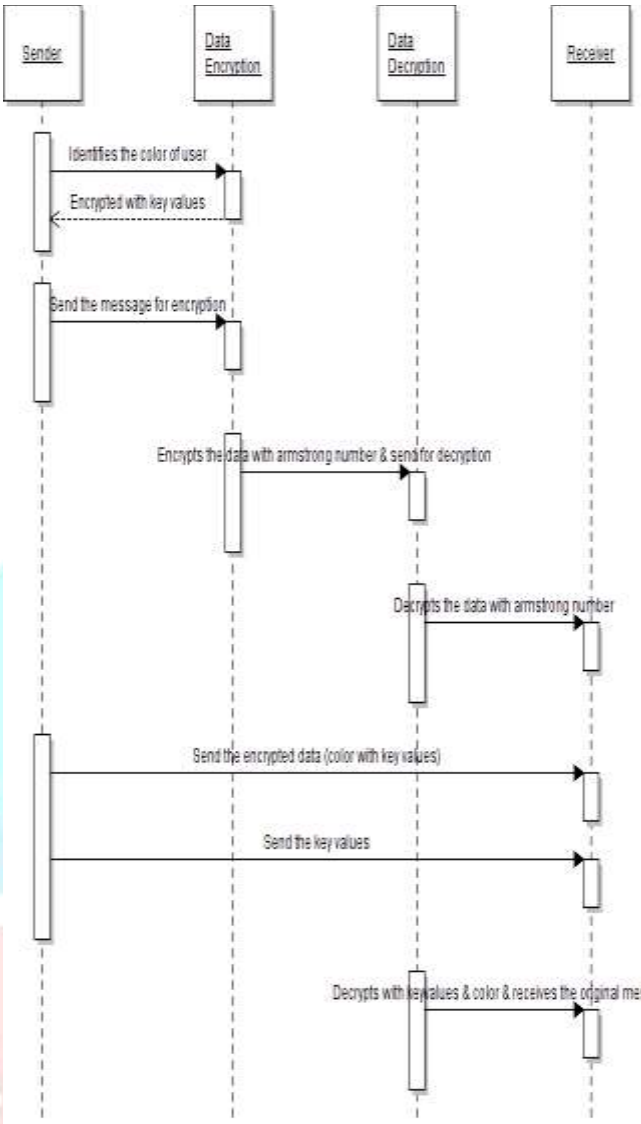
5.1.1 Class Diagram



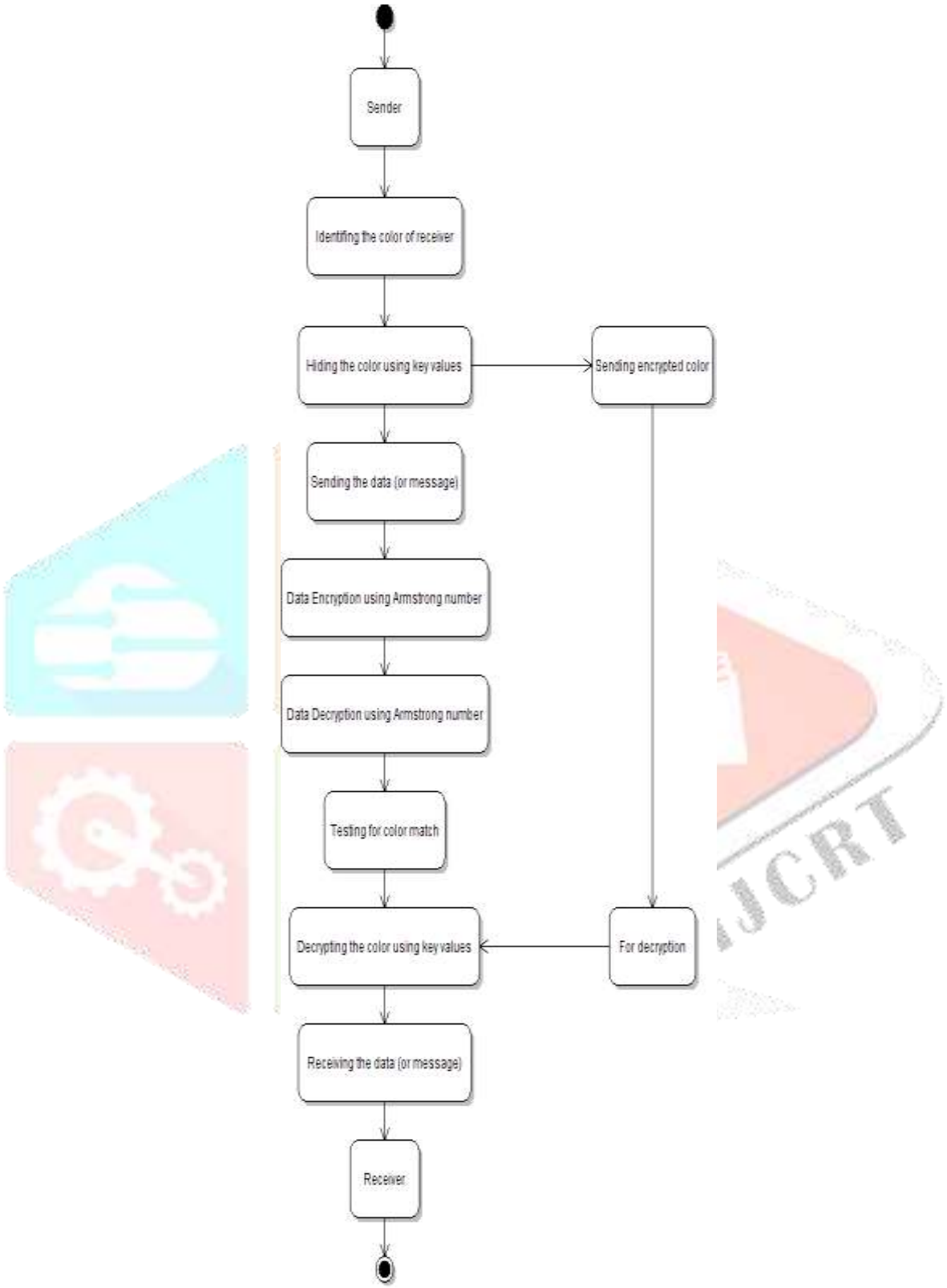
5.1.2 Use case Diagram



5.1.3 Sequence Diagram



5.1.4 Activity Diagram



VI. MODULES DESCRIPTION

- HIDING SENDER
- HIDING MESSAGE

- MESSAGES TRANSMISSION
- DECRYPT THE MESSAGE
- DECRYPT THE RECEIVER

The detailed description of the modules are ,

6.1. Hiding Sender

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.

When an sender's message send to the receiver this application will start to work and receiver send the sender's id(user id).Then user login their id and verifying id acknowledged. This process for comparing each other that contacting user was correct ,If not the sender rejects the user requests.

6.2. Hiding Message

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. At the receiver's side, the receiver is aware of his own color and other key values.

The encrypted color from the sender is decrypt by subtracting the key values from the received set of color values. It is then tested for a match with the color stored at the sender's database. Only when the colors are matched the actual data can be decrypt using Armstrong numbers. Usage of colors as a password in this way ensures more security to the data providing authentication. This is because only when the colors at the sender and receiver's side match with each other the actual data could be accessed.

6.3. Message Transmission

There are many types of encryption and not all of it is reliable. The same computer power that yeilds strong encryption can be used to break weak encryption schemes. Initially, 64-bit encryption was thought to be quite strong, but today 128-bit encryption is the standard, and this will undoubtedly change again in the future.

Today's technology-led business environment is influenced by multiple factors placing significant importance on software security. Software security implies identifying and understanding common threats, designing for security, and subjecting all software artifacts to thorough risk analysis assessment. It can set a messaging configuration parameter to determine if plain passwords are allowed or if passwords must be encrypted.

6.4. Decrypt The Message

Encrypt provides symmetric encryption functionality via the CryptoKey object. CryptoKey's core methods, EncryptFile, DecryptFile, EncryptText and DecryptText, allow you to implement file and text encryption in your application in just a few lines of code. An instance of the Crypto Key object is created using Crypto Context's methods GenerateKey and GenerateKeyFromPassword. The former generates a random key, while the latter generates a key based on a text password. A key generated by the GenerateKey method must be serialized to a file or other permanent storage in order to be used for decryption later. A password-derived key does not have to be serialized as it can always be re-created using the same password .

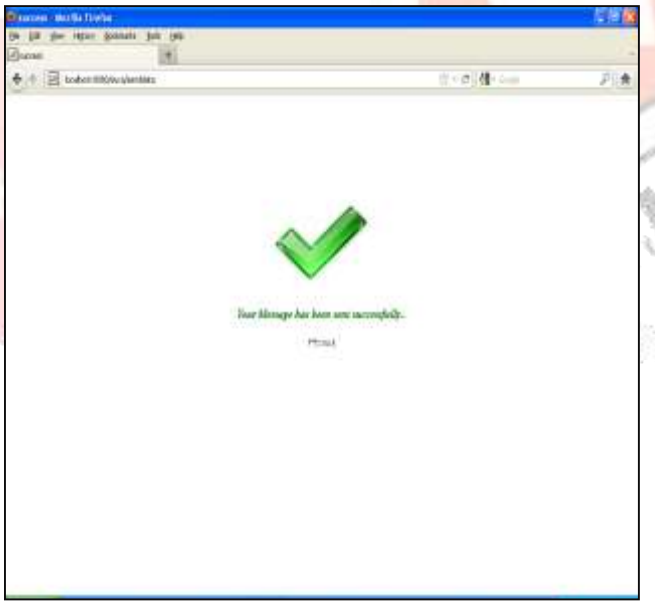
6.5. DECRYPT THE RECEIVER

Decryption involves the process of getting back the original data using decryption key. The data given by the receiver (the color) is matched with the data stored at the sender's end. For this process the receiver must be aware of his own color being assigned

and the key values. The received data now with substitute with the key value in the receiver side,then we get back a set of values.And then it compares to the data which is stored in the sender's side.if both get matched together following decryption

In an enterprise environment, using password-derived keys may not be feasible as everybody would have to share a password to encrypt and decrypt files. It makes more sense to encrypt files using randomly generated keys that are stored in a key repository and dispensed to eligible authenticated users upon request. Needless to say, these keys would have to be encrypted.

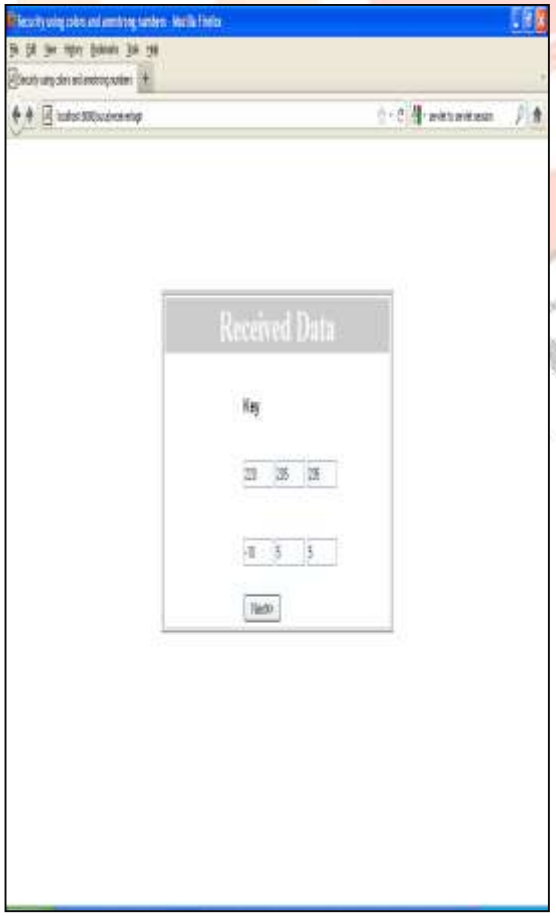
V. OUTPUT ANALYSIS




SECURITY USING COLORS AND ARMSTRONG NUMBERS


Received Data
Key


Receiver


Received Data
Key

VII. 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.

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] Singh, S., *The Code Book*, New York: Doubleday, 1999
[5] Miller, C., Lial, M. and Schneider, D., *Fundamentals of College Algebra*, 3rd Edition, Scott, Foresman and Company, 1990
[6] Diffie, W. and Hellman, M., "New Directions in Cryptography", *IEEE Transactions on Information Theory*, November, 1976
[7] Rivest, R., Shamir, A. and Adelman, L., "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", *Communications of the ACM*, February, 197
[8] Denning, D. and Denning, P., *Internet Besieged, Countering Cyberspace Scoflaws*, ACM Press (Addison-Wesley), New York, NY, 1998
[9] Denning, D., *Information Warfare and Security*, New York: Addison- Wesley/ACM Press, 1999