ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (89-92), Month: April - June 2016, Available at: www.researchpublish.com

Authentication Using Color Codes and Data Security Using Armstrong Numbers

Nivedita Debnath[1], Supriya Guduru[2], Prof. Devendra Singh[3]

[1,2] U.G Student, [3]Assistant Professor, Department of Computer Science and Engineering, IT, GGV, Bilaspur, Chhattisgarh

Abstract: **In order to provide authentication, confidentiality and security to the transmitted data the universal technique used is cryptography. Cryptography is the science of manipulating the data such that it is made unreadable for the unintended readers. It is the practice and study of hiding information. Here in this paper data is encrypted using Armstrong numbers on which RGB colours are used for authentication and key generation is done using random prime number generator thereby making use of both Armstrong numbers and prime numbers which also provides better security. Further, this encryption-decryption algorithm has already been implemented taking a 3-digit Armstrong number i.e. on a 3X3 matrix , but in this paper we would implement it taking a 4-digit Armstrong number , thereby providing security of data on a higher level.**

Keywords: **Data Security, Armstrong numbers, RGB colours, random prime number generator.**

I. INTRODUCTION

In real world, data security is very important where importance is given to the confidentiality, authentication and integrity. The data may get hacked by the intruder, hacker or the people having access to such credential data. The basic technique used for the security purpose is cryptography. The main goals of cryptography are access control and non- repudiation. It consists of encryption and decryption processes. Encryption and decryption have need of some secret information, usually referred to as a key. Overview of some basic concepts:

A. RGB representation:

Any color is the mixture of three colours RGB (Red, Green and Blue) in preset 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 colours are used as a password for authentication purpose. Then encryption or decryption process takes place.

B. 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 1634 is an Armstrong number because $1^4+6^4+3^4+4^4=1634$

II. OVERVIEW OF CRYPTOGRAPHY

Cryptography is the science of writing in secret code and is an ancient art. It is concerned with keeping communications private. Encryption in this context means transforming the data into a form which is unreadable. Similarly decryption is converting that unreadable data into that original data called the plain text and the encrypted text is known as the cipher text. To convert plain text into cipher text a medium is required which may be algorithms or simply a key. These algorithms can be categorized into 2 types based on number of keys used for encryption and decryption process. They are:

1) Private Key Cryptography (PKC): 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 and Adleman) algorithm is an example.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (89-92), Month: April - June 2016, Available at: www.researchpublish.com

Within the context of any application-to-application communication, there are some specific security requirements, including:

- ***Authentication:*** The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- ***Privacy/confidentiality:*** Ensuring that no one can read the message except the intended receiver.
- ***Integrity:*** Assuring the receiver that the received message has not been altered in any way from the original.
- ***Non-repudiation:*** A mechanism to prove that the sender really sent this message.

III. PROPOSED SYSTEM

In the existing techniques related to security using Armstrong numbers a set of three key values are added to the colour code for encryption. As a step further the set of key values can be generated using random prime number generator there by making use of both prime numbers and Armstrong numbers to provide better security. Here, also we use 4 digits Armstrong number and this approach can also be extended to any digit Armstrong number which increases the security of the data or message. The colour codes are used for authentication of each data packet in which each data packet is assigned with a colour code. And then in the receiver side the decryption of the colour code is done.

Algorithm Description:

Step 1: (Creating password) Initially the sender knows the required receiver to be A. So the key values are added with the color values assigned for receiver A.

135 38 87
  1 3 5
---
136 41 92

Now a newly encrypted color is designed for security check

Step 2: (Encryption of the actual data begins here) Let the message to be transmitted be "NETWORKS".

First find the ASCII equivalent of the above characters.

N E T W O R K S

78 69 84 87 79 82 75 83

Step 3: Now add these numbers with the digits of the Armstrong number as follows

	78	69	84	87	79	82	75	83
(+)	1	6	3	4	1	36	9	16
	79	75	87	91	80	118	84	99

Step 4: Convert the above data into a matrix as follows

A=

$$\begin{bmatrix} 79 & 80 \\ 75 & 118 \\ 87 & 84 \\ 91 & 99 \end{bmatrix}$$

Step 5: Consider an encoding matrix

B=

$$\begin{bmatrix} 1 & 6 & 3 & 4 \\ 1 & 36 & 9 & 16 \\ 1 & 216 & 27 & 64 \\ 1 & 1296 & 81 & 256 \end{bmatrix}$$

Step 6: After multiplying the two matrices (B X A) we get

C=

$$\begin{bmatrix} 1154 & 1436 \\ 5018 & 6668 \\ 24452 & 34172 \\ 127622 & 185156 \end{bmatrix}$$

Therefore the encrypted data is

1154,5018,24452,127622,1436,6668,34172,185156

The above values represent the encrypted form of the given message.

2) Decryption: 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

Step 1: (Authenticating the receiver) For the receiver A (as assumed) the actual color being assigned is Raspberry. (135, 38, 87), the key values (set of three values) are subtracted from the color being received to get back the original color. The decryption is as follows.

136 41 92 (Received data)

(-) 1 3 5 (Key values) ← (Generated through random prime number generator)

---

135 38 87

The above set of values (135, 38, 87) is compared with the data stored at the sender's side. Only when they both match the following steps could be performed to decrypt the original data.

Step 2: (Decryption of the original data starts here)

The inverse of the encoding matrix B is denoted by D

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (89-92), Month: April - June 2016, Available at: www.researchpublish.com

D=

$$\begin{bmatrix} 2.39 & -1.79 & 0.43 & -0.03 \\ -0.06 & 0.10 & -0.04 & 0.005 \\ -1.33 & 1.88 & -0.61 & 0.05 \\ 0.75 & -1.12 & 0.41 & -0.04 \end{bmatrix}$$

Step 3: Multiply the decoding matrix D with the encrypted data to get the original data matrix

DXC=

$$\begin{bmatrix} 79 & 80 \\ 75 & 118 \\ 87 & 84 \\ 91 & 99 \end{bmatrix}$$

Step 4: Getting the equivalent ASCII codes for the above obtained data matrix we get

79 75 87 91 80 118 84 99

N E T W O R K S

IV. CONCLUSION

The use of 4 digit Armstrong number increases the level of security and this method can be applied to any digit Armstrong numbers. By using this method the attacker must have to try 2^{24} values of passwords which are practically most difficult. And also combination of substitution & permutation increases the security of algorithm using these many colours. This method can be applied to those Armstrong numbers whose digits are distinct which happens to be the disadvantage of this algorithm. And the digits of the Armstrong number should not be zero as inverse can't be found.

REFERENCES

[1] Atul Kahate, "*Cryptography and Network Security*", Tata McGraw Hill Publications

[2] A Survey on Security Mechanism using Colors and Armstrong Numbers International Journal of Science and Research (IJSR) Nutan Gurav, Savitribai Phule Pune University, Institute of Knowledge 2Professor, Savitribai Phule Pune University, Institute of Knowledge COE, Pimple Jagtap, Pune, Maharashtra, India.

[3] "Message Security Using Armstrong Numbers and Authentication Using Colors"Gayatri Kulkarni, Pranjali Gujar, Madhuri Joshi, Shilpa Jadhav Computer Department Pune University, India.

[4] S.Pavithra Deepa, S.Kannimuthu, V.Keerthika, "Security using colors and Armstrong numbers", Innovations in Emerging Technology (NCOIET), Feb2011