International Journal of Academic Research
ISSN: 2348-7666; Vol.5, Issue-10, October, 2018
Impact Factor: 6.023; Email: drtvramana@yahoo.co.in

Data Security using Colours and Armstrong Numbers

Nalimela Srividya,
Department of Electronic Communication and Engineering, Kakatiya University, Warangal

Abstract

Now a day's data security is the main issue. Confidentiality, integrity, non-repudiation, authentication, mainly comprises by the data security. The universal technique for contribute confidence of transmitted data is cryptography. In certifiable, information security assumes an imperative part where classification, verification, trustworthiness, non renouncement are given significance. The all inclusive system for giving classification of transmitted information is cryptography. In real world, data security plays a vital role where security, privacy, validation, integrity, non-repudiation is given importance. There are some common techniques used for secure data transmission over network. This paper provides a technique for data security which encrypt the data using a key involving Armstrong numbers and colours as the password. Three set of keys is used to provide secure data transmission with the colours acting as vital security element thereby providing authentication.

Keywords: secure data transmission, Armstrong numbers, validation, Cryptography, Colors.

Introduction

In today's world, electronic media become a necessity. Cryptography is a way to make secure that electronic media. Data security plays an important role. Day by day hackers is becoming more powerful. So it is increasingly becoming more important to protect our valuable data Basically cryptography is used to protect valuable information resources on intranets, extranets and internet. 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.

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. 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 is decrypted 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 decrypted 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. Encryption and Decryption process applies to both data as well as its key. So that two way security is provided to the application. After successful authentication, data is encrypted by random Armstrong number and at the same time that Armstrong number is get encrypted. Now for both these encrypted data and key current system timestamp is attached. So whenever receiver gets both the data he can easily recognize which key is for which data. Then encrypted key is decrypted by sender's public key and that resulted Armstrong number is used to decrypt actual data.

Cryptography

Most people are concerned with keeping communications private. 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. Its purpose is to ensure privacy by keeping the data hidden from anyone for whom it is not intended. 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 the 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. Security is one of the major concerns of all the users irrespective of the domain in which they work. There are various ways by which one can ensure the security of the data which is present in different files on the computer.

Cryptography is the art and study of hiding information i.e. technique to convert plain text into cipher text i.e. encryption. Decryption in which cipher text is converted back into plain text with the help of the key. To maintain privacy and to prevent an unauthorized person from extracting information from the communication channel.

Types of Cryptographic Algorithms There are several ways of classifying cryptographic algorithms. In general, they are categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use as in the three types of algorithms are depicted as follows

1) Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption.

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) algorithm is an example.

Advantages: Colors are used for the authentication purpose. The range of color is 2 ^ 0 to 2 ^ 24. RGB model uses 24 bits, 8 bits for each color. To encrypt the data set of three key values are added to the original color values. This encrypted color acts as a password. To break this password attacker has to check 256 ^ 3 possible values which are practically most difficult. The combination of substitution and permutation process increases the data security. To increase the strength of

algorithm 9 digits, Armstrong number is used for encryption and decryption, a length of an Armstrong number can be increased if necessary for security purpose.

RGB Color Format

The red Green and Blue are the primary colors. And any color is formed by the combination of these three primary colors. Which are in fixed quantities? In a computer color is stored in the form of Red, Green and Blue by representing their quantities which is known as RGB representation. In the computer for storing the image in PDF, JPEG or BMP formats, the RGB representation is use. Values for Red, Green and Blue is represented by each pixel. Thus in the three dimensional RGB cube, any color can be uniquely represented as values of Red, Green and Blue.

To produce other colors, the values of Red, Green and Blue are merge together in different ways in the RGB color model. Many colors can be represented by using convenient merging of Red, Green and Blue intensities. Typically, to store a color pixel 24 bits are used in which 8 bits each for red, green and blue. For each hue, all these colors are presents in the range of 256 possible values. 16 777 216 (256 ^ 3 or 2 ^ 24) various combinations of intensity and hue can be specified with this system acceptable.

Proposed Approach

The current procedures include the utilization of keys including prime numbers and so forth. As above and beyond ahead let us considers a system in which we utilize Armstrong numbers and hues. Further we likewise utilize a mix of substitution and change techniques to guarantee information security. We perform the substitution process by allotting the ASCII equal to the characters. Stage procedure is performed by utilizing frameworks as a part of Armstrong number.

The sender knows about the obliged recipient to whom the information must be sent. So the collector's extraordinary shading is utilized as the secret key. The arrangement of three key qualities are added to the first shading values and encoded at the sender's side. This scrambled shading really goes about as a secret key. The genuine information is encoded utilizing Armstrong numbers.

At the recipient's side, the beneficiary knows about his own particular shading and other key qualities. The encoded shading from the sender is unscrambled by subtracting the key qualities from the got set of shading qualities. It is then tried for a match with the shading put away at the sender's database. Just when the hues are coordinated the genuine information can be unscrambled utilizing Armstrong numbers. Use of hues as a secret key along these lines guarantees more security to the information giving confirmation.

System Architecture

We assign the ASCII equivalent to the characters, this is the substitution process. Using matrices and Armstrong number the permutation process is complete. The first step of this technique is to appoint a different color for each and every receiver. Set of three values are represented with each color. For example in RGB format as (238, 58,140) is represented by violet red

color. In the next step a set of three key values assign to each receiver. Common Database Of The Sender Data Stored At Each Receiving End.

Data Encryption: Once the user is authenticated, now the sender sends the requested data to the receiver. Initially ASCII value for each character is found. Then Armstrong number is added to this ASCII value in an iterative manner until each character is assigned with the number. The resultant sum value is now converted into a matrix. Consider an encrypted matrix (Armstrong number), multiply it with the resultant sum matrix. The resultant matrix value consists of the encrypted data.

Conclusion

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, banking sector, 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. In military, the above combination of public key and secrete key cryptography can be applied because, more importance is for security of data. When the length of the key of the Armstrong numbers increase, then this technique pro-vides more security. Thus by the use Armstrong numbers, additional set of key values and colors in this technique there is surety that the data is deliver securely and that only authorized peoples can access it contribution.

REFERENCES:

1. M.F.Armstrong "A brief introduction to Armstrong Numbers"
2. Chavan Satish, Lokhande Yogesh, Shinde Pravin, Yewale Sandeep, Sardeshpande S. A, "Secure Email using Colors and Armstrong Numbers over web services", International Journal of Research in Computer Engineering and Information Technology Volume 1 No. 2.
3. G.Ananthlakshmi, S.Ramamoorthy "A Multilevel Encryption Scheme for Secure Network Data Transfer". International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012.
4. Security Using Colors and Armstrong Numbers-National Conference on Innovations in Emerging Technology Year 2011.
5. Message Security Using Armstrong Numbers and Authentication Using Colors-International Journal of Advanced Research in Computer Science and Software Engineering January 2014.
6. "Security Using Colors and Armstrong Numbers" by S. Pavithra Deepa, S. Kannimuthu, V. Keerthika 1,3UG Student, Department of IT, Sri Krishna College of Engineering and Technology.
7. 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).