ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Review on Security Using Colours and Armstrong Numbers

Prof: Riya Qureshi, Shikha singh, Diksha Itankar

Head of Department, Dept. of computer science, Gondwana University, Maharashtra, India

B.E Student, Dept. of Computer Science, Gondwana University, Maharashtra, India

B.E Student, Dept. of Computer Science, Gondwana University, Maharashtra, India

ABSTRACT: Data Security is the science and study of methods of protecting data from unauthorized disclosure and modification. As per the technology upgraded, there is need to secure data which is transmitted over the network. We are living in the information age. Information is an important asset, like other assets, it has value to various organization and need to be suitably protected. Hence data security plays an important role. Hackers are becoming more active nowadays. Hence it is increasingly becoming more important to protect our confidential data. There are some techniques for secure data communication with presence of third parties. Cryptography is one of them. This paper provides a technique in which Armstrong number is used for encryption of message. Three set of keys provide more security when data is transmitted. Colour acts for the process of authentication.

KEYWORDS: Data security, Armstrong numbers, Authentication, Cryptography, Colours

I. Introduction

Now 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. 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 is 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.

II. Related work

Public key cryptography algorithms utilize prime numbers broadly because prime numbers are a crucial part of the public key systems. This technique ensures that using two main steps data transfer can be performed with protection. First step is to convert the data into ASCII form, then by adding with the digits of the Armstrong numbers. Second step is to encode using a matrix to generate the required encrypted data. Tracing process becomes difficult with this technique. This is because in each step the Armstrong number is used in different way. Three different keys are used namely the colors, key values added with the colors and Armstrong numbers. Data can be retrieved only if all the three key values along with this technique is known. Simple encryption and decryption techniques may just involve encoding and decoding the actual data. But in this proposed technique the password itself is encoded to provide more security to the access of original data. Armstrong numbers and colors are used in this technique. The sender is attentive of the required receiver to whom the message has to be sent.

III. BACKGROUND STUDY

The original message called plaintext is converted into random text called cipher text. The science and art of manipulating messages to make secure is called cryptography. Public key cryptography algorithms utilize prime numbers broadly because prime numbers are a crucial part of the public key systems. This paper considers a technique in which Armstrong numbers and colours are used. The sender is attentive of the required receiver to whom the data has to be sent. So the receiver's unique colour is used as the password. The set of three key values are added to the original colour values. They are encrypted at the sender's side.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, governments are targeted by the system where data security is given more importance. Colours, 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.

IV. PROPOSED SYSTEM

Armstrong numbers are used for encryption purpose while existing system uses prime number. Colour is used for authentication purpose. Basic concept is that unique colour is assigned to each receiver. This unique colour acts as password. The sender knows required receiver to whom the data has to be sent. There can be N numbers of receivers who can access the encrypted data if they are authorized (N⩽224). Firstly, encryption of colour is done by adding key values to the original colour values at sender ’ s side. This encrypted colour acts as a password. Then data is encrypted using Armstrong numbers. At the receiver’s side when the receiver enters secret key, decryption of colour takes place. The decrypted colour is then matched with colour assigned by sender i.e. original colour stored at the sender’s database. Without the secret key, there is no way for user to access the data. Further a combination, substitution and permutation methods are used with Armstrong number to ensure data security. S For encryption it converts each letter to its ASCII equivalent by substitution method and permutation is done with the help of Armstrong number. Later it converts that data into matrix form. It performs permutation process by using matrices. Receiver will perform in reverse manner

A. RGB representation

Any colour is the mixture of three colours RGB (Red, Green and Blue) in pre-set quantities. This is nothing but a RGB representation. Here values for Red, Green and Blue represent each pixel. So any colour can be individually represented with the help of three dimensional RGB cube. RGB model uses 24 bits, 8 bits for each colour. Hence colours are used as a password for authentication purpose. Then encryption or decryption process takes place.

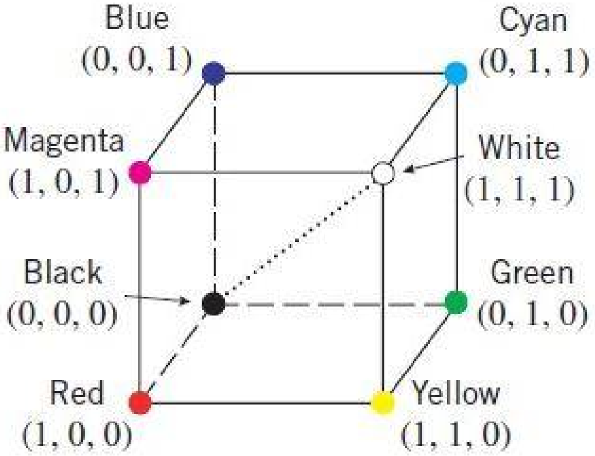

Fig1 rgb model

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 371 is an Armstrong number because 33+73+13 =1 + 343 + 27 = 371.

V. CRYPTOGRAPHY

Cryptography is used to keep the communication private. It protects from theft and alteration. There are two processes in cryptography encryption and decryption. The purpose of encryption is to ensure privacy that is to hide the data and converting it into unreadable form. Decryption is reverse of encryption. It is used for getting the data back into a readable form. The data to be encrypted is called plain text and the data after encryption is called 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.

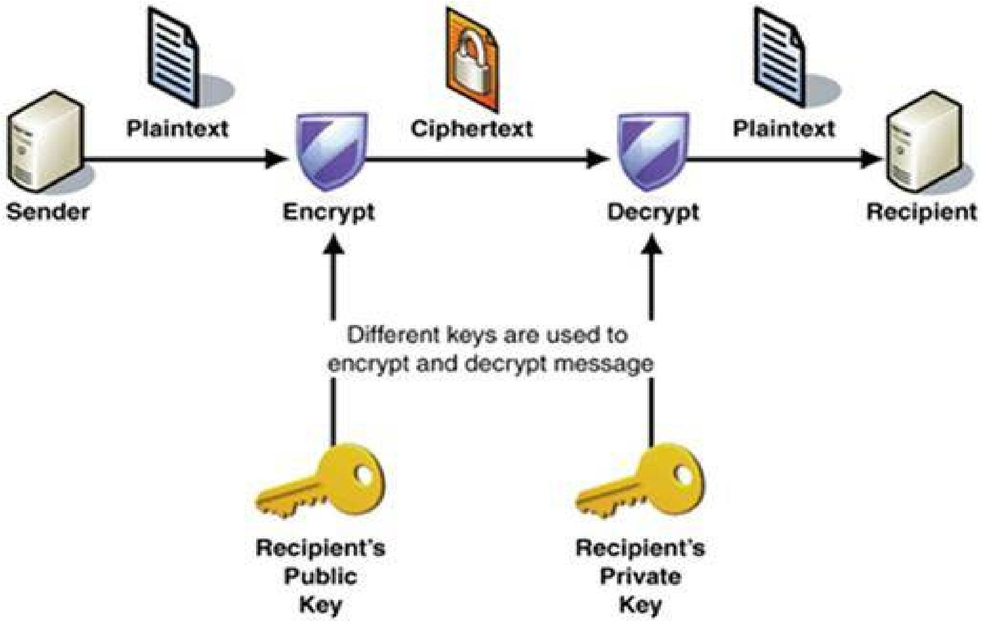

Fig2: Cryptographic model

VI. TYPES OF CRYPTOGRAPHIC ALGORITHMS

There are two types of cryptographic algorithm to accomplish these goals: symmetric cryptography, asymmetric cryptography. The initial unencrypted data is referred as normal text. It is encrypted into cipher text with a cryptographic algorithm, which will in turn be decrypted into usable plaintext. In symmetric cryptography single key is used for encryption and decryption e.g. Data Encryption Standard (DES) and Advanced Encryption Standards (AES).In asymmetric algorithm different keys are used to encrypt and decrypt the data.RSA is widely used in electronic ecommerce protocols. With sufficiently long keys and the use of up-to-date implementations; RSA is believed to be totally secure.

There are two ways in which we can achieve security 1.encrypted file transfer 2.Strong secure protocol for transmission of files. RSA (Rivest, Shamir & Adleman) is asymmetric cryptographic algorithm developed in 1977. It generates two keys: public key for encryption and private key to decrypt message [2].RSA algorithm consist of three phases, phase one is key generation which is to be used as key to encrypt and decrypt data, second phase is encryption, where actual process of conversion of plaintext to cipher text is being carried out and third phase is decryption, where encrypted text is converted in to plain text at other side.

As a public key is used for encryption and is well known to everyone and with the help of public key, hacker can use brute force method to find private key which is used to decrypt message. Secure RSA prevents files from hackers and help safe transmission of files from one end to other

Cryptography is a process which is associated with scrambling plaintext (ordinary text, or clear text) into cipher text (a process called encryption), then back again to plain text (known as decryption). The key feature of asymmetric cryptography system is encryption and decryption procedure are done with two different keys - public key and private key. Private Key cannot be derived with help of public key that provides much strength to security of cryptography. This is one main difference between symmetric and asymmetric cryptography, but that difference makes whole process different. This difference is small but it is enough that it has implications throughout the security. Mainly, symmetric cryptography is seen as faster, more lightweight, and better suited for applications that have a lot of data to transfer, while at the same time, it is known to be less secure and more open to wider areas of attacks because of maintenance of a private key required.

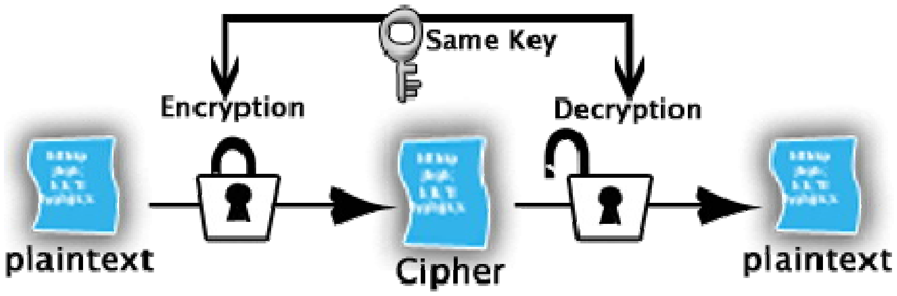

Fig3: symmetric cryptography

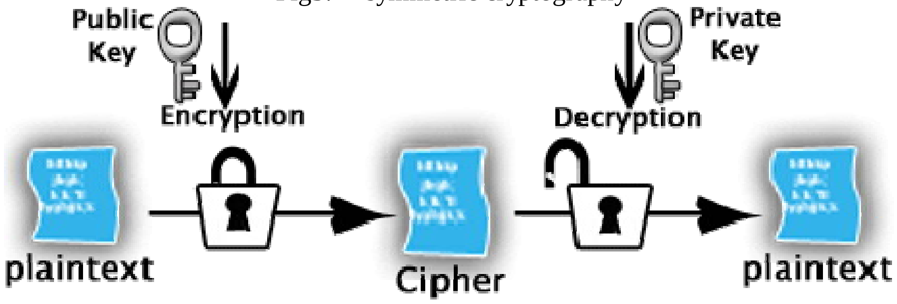

Fig4: asymmetric cryptography

VII. PROPOSED ALGORITHM

A.RSA FILE TRANSMISSION:

RSA is widely used in encrypted connection, digital signatures and digital certificates core algorithms. Public key algorithm invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman (RSA). It is the main operation of RSA to compute modular exponentiation. Since RSA is based on arithmetic modulo large numbers, it can be slow in constraining environments [18]. Especially, when RSA decrypts the cipher text and generates the signatures, more computation capacity and time will be required. Reducing modulus in modular exponentiation is a technique to speed up the RSA decryption. The security of RSA comes from integer factorization problem. RSA algorithm is relatively easy to understand and implement RSA algorithm is based on the theory of a special kind of reversible arithmetic for modular and exponent RSA is used in security protocols such as IPSEC/IKE, TLS/SSL, PGP, and many more applications. The public and private keys are functions of a pair of large prime numbers and the necessary activities required to decrypt a message from cipher text to plaintext using a public key is comparable to factoring the product of two prime numbers. RSA File Transmission Algorithm can be summarized as follows:
(1)Generate the asymmetric keys with required digits.
(2)Save and load the key, the key is saved as plain text.
(3)Use specified key to encrypt any file with RSA algorithm. 4. Encrypted files can be loaded and decrypted with the specified key to restore the original file.

B.STEPS INVOLVED IN IMPLEMENTATION OF RSA

The following step is taken to implement the RSA public key scheme:
1. Choose two large prime numbers, p and q. Let n =p * q,
Let (n) = (p- l)* (q- l) .
2. Randomly choose a value e (I < e < I (n)), which is relative prime to I (n) that gcd (e, n (n)).
3. Calculate de- l mod L(n) , send public key (e, n to transmitter and secret key (d, n) to receiver.

DOI: 10.15680/IJIRCCE.2016. 0403022

C. *PROPOSED CRYPTOSYSTEM:*

The previous RSA Algorithm was designed by using two random prime numbers to generate public key and private key. But in the proposed method we are using three prime numbers to generate public key and private key. In our proposed method we are increasing the security of data by increasing the robustness and complex city in finding the encrypted data.

VIII. 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, 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.

REFERENCES

[1] S. Pavithra Deepa,S. Kannimuthu, V. Keerthika., “Security Using Colours and Armstrong Numbers”, Proceedings of the National Conference on Innovations in Emerging Technology, 17 & 18 February, 2011.pp.157-160.

[2]Atul Kahate, “Cryptography and Network Security” Tata McGraw Hill Publications.

[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] M.F.Armstrong “A brief introduction to Armstrong Numbers”.

[5] R . L. Rivest, A. Shamir and L. Adleman, "On Digital Signatures and Public Key Cryptosystems", Technical Memo 82, Laboratory for Computer Science, Massachusetts Institute of Technology, April 1970

[6] R.L. Rivest, A. Shamir and L. Adleman, "A Method of obtaining Digital Signatures and Public Key Cryptosystems", Communication of the ACM, 21, 2(1978), pp 120-126 .

[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).

[8] Mrunali Vaidya, Vaibhav Bansod, Mangesh journal of computer science and mobile computing, (Vol.13,Issue.10,october2014,pg 926-931).

DOI: 10.15680/IJIRCCE.2016. 0403022