International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

An Effective Way for Data Encryption and Decryption Using Hierarchical Techniques

Kavyashree S[1], Manjula V[2], Gnanashree S[3]

[1]UG Student, School of Engineering and Technology, Jain University,
Jain Global Campus, Kanakpura Taluk, Ramanagara District, Karnataka, India

[3]Assistant Professor, Jain University, Department of Information Science and Engineering,
Jain Global Campus, Kanakpura Taluk, Ramanagara District, Karnataka, India

[3]UG Student, School of Engineering and Technology, Jain University,
Jain Global Campus, Kanakpura Taluk, Ramanagara District, Karnataka, India

Abstract: ***In the current world scenario, securing the data is really an important criteria for high confidentiality, integrity and authenticity. The technique which is used to attain the high confidentiality is called cryptography. As the time changes people have started to access the technology regardless of the geographical conditions and time. Internet is the major source of usage for all the financial transactions. Internet is well known for providing conveniences and equally prone for causing inconveniences with respect to security issues. Therefore, internet security became important to be achieved. This paper provides the methodology to encrypt the information by the usage of three set of key values including Armstrong numbers and colors as the password. Here the input is taken in the form text message and converted to ASCII equivalents.***

Keywords: Cryptography, Encryption, Decryption, RGB Color, Armstrong numbers

1. Introduction

The current generation is mainly concerned about using the technology benefits without exposing some confidential data. This can be achieved by many algorithmic techniques which inscribes the required data. One of the common methodologies used to secure data is cryptography. The cryptography technique ensures that the data transmitted is secured.

More generally, Cryptography is the analysis and development ofprotocols that prevent any other illegal access of private data. Encryption is the process of securing the data in such a way that only the privileged users can access it. The main purpose of encrption is deny the required content rather thn preventing interference. Decryption is the converse of encryption; it is the conversion of secured data back into some required format. Both encryption and decryption involves the usage of key(private to the methodology) to perform the operations. The data which is to be secured is called as plain text. The resulting data after encryption is called as cipher text.The type of key depends on encryption mechanism used and the keys used both encrytion and decryption can be differential.Security impedence can be administered in the form of passive attack and active attack.

1) A passive attack is one in which the attacker checks on the message contents which is exchanges but will not modify the message. After the encryption process also the messages can be viewed by analyzing the traffic on the stream of data which is exchanged.

2) In active attack the attacker will be able to modify the message contents, he can delete some contents and resend new contents into the message stream and exchange messages.

3) Security impedances can be alleviated by providing security services as follows:

Integrity, Authentication, Confidentiality, Non-Repudiation, Access Control, Availability

A single layer will not enough for providing solution for the security issues therefore we require a layered approach for eradicating the service attacks. The primary level of defense at the initiation to a system is Firewall and VPN. An Anti-Virus is commonly used to protect data on desktop pc's. The secondary level of defense is Intrusion Detection System (IDS). Intrusion means the set of activities which is performed to provide security. Intrusion detection is mainly concerned on identifying intrusions. Basically IDS are an intrusion detection tool. It is a dynamic device which identifies each and every message exchanges happening on the network, perform analysis and notifies the administrator regarding intrusions. The administrator will take steps on correcting the stopping some more damages. to stop any more damage. But it does not prevent any attacks from occurring. There are Intrusion Prevention systems (IPS) which will detect intrusions and also prevents them. The further level of defense is Cryptography. 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. The three types of algorithms are depicted as follows:

1) 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).

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)

2. Proposed Approach

The user needs to select an Armstrong number when he logs in to the system for the first time and also set a password. Whenever the user wants to access the system he needs to enter the password.

2.1 Encryption

Step 1: (Encryption of the actual data)
Let the message to be transmitted be "CRYPTOGRAPHY". First find the ASCII equivalent of the above characters.

C R Y P T O G R A P H Y
67 82 89 80 84 79 71 82 65 80 72 89

Step 2: Suppose the Armstrong number is 153. Now add these numbers with the digits of the Armstrong number as follows:

67 82 89 80 84 79 71 82 65 80 72 89
(+) 1 5 3 1 25 9 1 125 27 1 5 3
---
68 87 92 81 109 88 72 207 92 81 77 92

Step 3: Convert the above data into a matrix as follows:

$$A=\begin{bmatrix} 68 & 81 & 72 & 81 \\ 87 & 109 & 207 & 77 \\ 92 & 88 & 92 & 92 \end{bmatrix}$$

Step 4: Consider an encoding matrix

$$B=\begin{bmatrix} 1 & 5 & 3 \\ 1 & 25 & 9 \\ 1 & 125 & 27 \end{bmatrix}$$

Step 5: After multiplying the two matrices (B X A) we get

$$C=\begin{bmatrix} 779 & 890 & 1383 & 742 \\ 3071 & 3598 & 6075 & 2834 \\ 13472 & 16082 & 28431 & 12190 \end{bmatrix}$$

The encrypted data is...
779, 3071, 13427, 890, 3598, 16082, 1383, 6075, 28431,742, 2834, 12190

The above values represent the encrypted form of the given message. This is stored in the database

2.2 Decryption

Now , when the user wants to access his e-mails offline, he can view only the sender of the mail and for viewing the contents of the mail he needs to enter the Armstrong number in the reverse order so as to proceed with the decryption of the contents. And only if the reverse Armstrong number is correct the data gets decrypted.

Step 1: (Decryption of the original data)
The inverse of the encoding matrix is

$$D = (-1/240)*\begin{bmatrix} 450 & 240 & -30 \\ 18 & 24 & -6 \\ 100 & -120 & 20 \end{bmatrix}$$

Step 2: Multiply the decoding matrix with the encrypted data (D X C) we get

$$\begin{bmatrix} 68 & 81 & 72 & 81 \\ 87 & 109 & 207 & 77 \\ 92 & 88 & 92 & 92 \end{bmatrix}$$

Step 3: Now transform the above result as given below

68 87 92 81 109 88 72 207 92 81 77 92

Step 4: Subtract with the digits of the Armstrong numbers as follows:

68 87 92 81 109 88 72 207 92 81 77 92
(-) 1 5 3 1 25 9 1 125 27 1 5 3
---
67 82 89 80 84 79 71 82 65 80 72 89

Step 5: Obtain the characters from the above ASCII equivalent
67 82 89 80 84 79 71 82 65 80 72 89
C R Y P T O G R A P H Y
In this way we get the required contents back in the original form.

3. Related Work

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 and assigns a set of three key values to each receiver. 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. As a step further ahead let us considers a technique in which we use Armstrong numbers and colors. 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.

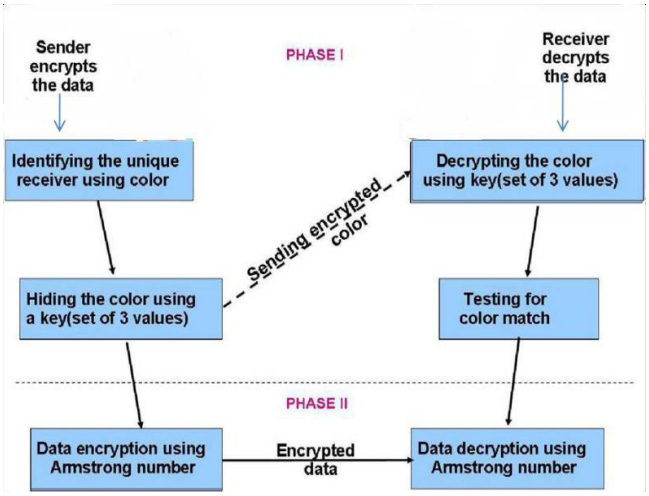

Figure 1: Architecture of proposed system

3.1 RGB Model

The proposed scheme includes two phases: Registration, Authentication. *1) User registration*: user module selects on RGB color value for the user and then find the position of this RGB in the cube and send request with its ID and POS to the base station for registration in WSNs. Base station generate a random number Which is termed as seed Also the base station module scales the seed value with the Armstrong number and multiply it with the POS it received from the user. It performs MD5 on this product and generate 128 bit key which is used for data security in AES algorithm. Base station send the key and seed to user and store the values in its database.

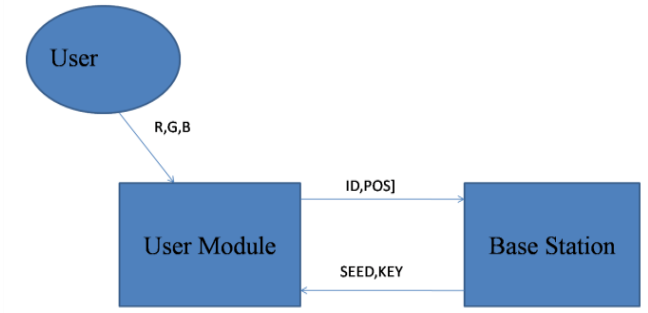

Figure 3.1: User registration

3.1.1 User Authentication on Login

In this phase user find out the new position of RGB using RGB color cube and PRNG in which the user module generate next random number using PRNG in which it uses the seed received from the base station in the registration phase and then offsets its previous RGB POS to NEW_POS with this new SEED_NEW and login with its ID and H[POS_NEW] to the base station. Upon Login request base station also generate the SEED_NEW using PRNG and find out the POS_NEW1 in the RGB cube. If the POS_NEW matches POS_NEW1 the user is authentic.

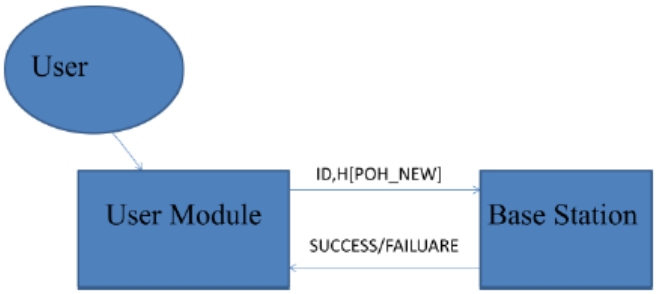

Figure 3.1.1: User authentication

The three primary colors of the additive color model are red, green, and blue. This RGB color cube displays smooth transitions between these colors. It has 8 bits per components. 256 * 256 * 256 number of possible colors Each color represented by a number in the cube(POS): POS = r + (g*256) + (b*256*256)

3.1.2 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 3^3+7^3+1^3 =1 + 343 + 27 = 371. For example 153 is an Armstrong number because cube of 1 is 1(1x1x1=1) + cube of 5 is 125(5*5*5=125) + cube of 3 is 27(3*3*3=27). Now add all the cubes 1+125+27=153 which is equals to number itself.

4. Conclusion and Future Work

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.

Some open issues remain to be explored in our future work. First, the proposed mechanisms are limited to static wireless ad hoc networks. Frequent changes on topology and link characteristics have not been considered. Extension to highly mobile environment will be studied in our future work. Misbehaving source and destination will be pursued in our future research. Moreover, in this paper, as a proof of concept, we mainly focused on showing the feasibility of the proposed crypto-primitives and how second-order statistics of packet loss can be utilized to improve detection accuracy.

As a first step in this direction, our analysis mainly emphasize the fundamental features of the problem, such as the untruthfulness nature of the attackers, the public verifiability of proofs, the privacy preserving requirement for the auditing process, and the randomness of wireless channels and packet losses, but ignore the particular behavior of various protocols that may be used at different layers of the protocol stack. The implementation and optimization of the proposed mechanism under various particular protocols will be considered in our future studies.

References

[1] S. Pavithra Deepa, S. Kannimuthu, V. Keerthika, "Security Using Colors and Armstrong Numbers," National Conference On Innovations In Emerging Technology Year 2011
[2] Ajay Bansode, Amit Joshi, Awanish Singh, Kiran Gosavi, Prasad S.Halgaonkar, Vijay M.Wadhai, "Data security in message passing using armastrong number," International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 2, Mar-Apr 2014
[3] S.Belose, M.Malekar, S.Dhamal , G.Dharmawat & N.J.Kulkarni, "Data Security Using Armstrong Numbers", Undergraduate Academic Research Journal (UARJ), ISSN : 2278 – 1129, Volume-1, Issue-1, 2012
[4] Shambhu Kumar Singh, N. P. Jagtap, S. J. Patil, "Use Of Rgb Colors And Cryptography For Could Security" Pratibha: International Journal Of Science, Spirituality, Business And Technology (Ijssbt), Vol. 3, No. 1, Dec 2014
[5] Manish Shrivastavaa, Shubham Jainb, Pushkar Singh, "Content Based Symmetric Key Algorithm", International Conference on Computational Modeling and Security (CMS 2016)
[6] Jyothika Chandra, Dr. Prema K.V, "Implementation of sub key generation algorithms", International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 4, April 2014
[7] Rutika S. Ingole and V. B. Bhagat, " Data Security in Email system in XML using Graceful code and Graphical Password", International Journal of Current Engineering and Technology, 2015
[8] Mrunali Vaidya, Vaibhav Bansod, Mangesh Manwar, "A Review on Cryptography using Armstrong numbers and Colors", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.10, October- 2014
[9] Puja Maruti Lad, Yallawa Shivaji Vhankade,Ashwini Jagannath Khandagale3 and Prajakta Ram Bhalerao, "Security of data based on coor and Armstrong numbers", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 10, October 2015.
[10] Kush Jain, Vaishali Ingale, Ashwini Sapkal, "Kunal Secure Astro-Encryption- Data Encryption and Compression Using Planar Geometry", International Association of Scientific Innovation and Research (IASIR)