IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 1, Ver. IV(Jan – Feb. 2016), PP 19-22
www.iosrjournals.org

An Efficient And Secure Cryptography Techniques Usingunimodular Matrix

ApurvaK.Vangujar[1], Kajal Agrawal[2]
[1]*Student of BE CSE: Dept of Computer Science & Engineering, Jawaharlal Nehru Engineering College Aurangabad, Maharashtra 431003, and India*
[2]*Student of ME CSE: Dept of Computer Science & Engineering, Jawaharlal Nehru Engineering College, Aurangabad, Maharashtra 431003, and India*

Abstract*: In day to day life, transmission of data from sender to receiver with security is very difficult. "Cryptography" is one of the famous techniques which provide security for confidential data. Cryptography is one of the best techniques for the secure data transmission. Confidentiality of data, access control and non-repudiation are the main goals of cryptography. The existing system is having limitations related to decrypts of Armstrong numbers. But the algorithm used in the proposed method uses unimodular matrix for encryption. Therefore, access control, non-repudiation and confidentiality of data is maintained.*
Keywords*: cryptography, decryption, encryption, unimodular matrix, Armstrong numbers*

I. Introduction

Security is more important to ensure the confidentiality of data. Sending a data from one node to another node with security is most difficult. There are several techniques are followed for secure data transmission.

Cryptography is one of the best techniques for the secure data transmission. Confidentiality of data, access control and non-repudiation are the main goals of cryptography.Cryptography consists of two processes that is encryption and decryption. Encryption and decryptionconsists of the key, i.e. some secret information. Encryption is the process in which plain text, convertsinto cipher text. And cipher text converts into plain text is knows as decryption process. The same key and different key are used for encryption and decryption .The same key might be used for both encryption and decryption depending on the encryption mechanism. While for other mechanisms, the keys used for encryption and decryption might be different.[1], [2], [3]

There are many encryption algorithm processes like AES, DES, RSA in which encryption is done with help of substitutions and transformation on plain text. It uses Armstrong numbers.

1. Cryptography using secret key (SKC):secrete key is a value independent of a plain text and of the algorithm. Single key is used for encryption and decryption by an algorithm. It includes of advance encryption standard (AES) and data encryption standard (DES)[4].
2. Cryptography using public key (PKC): two different keys are used in this cryptography. One key is used for encryption and another is used for decryption[4].
3. Hash function:It uses mathematical transformation for encryption which is not recoverable from the cipher text[4].

II. Literature Survey

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/ data, and telecommunications) [3]

This definition introduces three key objectives that are at the heart of computer security:

- Confidentiality: This term covers two related concepts:
- Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
- Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
- Integrity: This term covers two related concepts:
- Data integrity: Assures that information and programs are changed only in a specified and authorized manner.
- System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

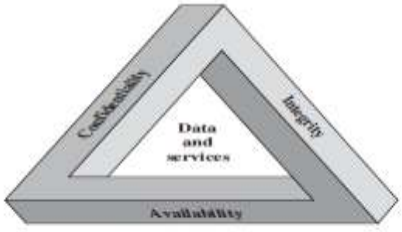

Figure 1.1 The Security Requirements Triad

Availability: Assures that systems work promprolyandservice is not denied to authorize users.

Proposed System

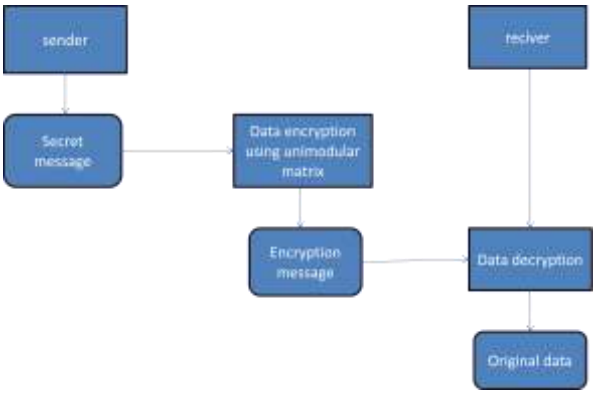

Fig. 1 proposed system architecture

There many techniques used for the secure communication. In our system, Armstrong numbers are used for the secure communication. Proposed method uses unimodular matrix for the encryption.As shown in the above diagram our proposed system will work. Here we are using cryptographic algorithm for encryption and decryption using Armstrong numbers[1]. These are carried out by performing substitutions and transformation of matrix. This technique uses Armstrong no. as same key for both encryption and decryption purposes. Therefore, it is symmetric key cryptography[5], [6].

Encryption algorithm

It is the cryptographic technique to convert plain text into cipher text by performing substitution and transformation on message character. This is performed by sender site by using some secret key.

Step 1:convert characters of secrete message into their ASCII equivalent. Consider message to be send is ENCRYPT

E	N	C	R	Y	P	T	-	-
69	78	67	82	89	80	84	-25	-25

Step 2: convert data into matrix form

$$P = \begin{bmatrix} 69 & 78 & 67 \\ 82 & 89 & 80 \\ 84 & -25 & -25 \end{bmatrix}$$

Step 3: Select any Armstrong number and calculate encoding matrix by using a unimodular matrix technique as follow:

$$\begin{bmatrix} 8n^2+8n & 2n+1 & 4n \\ 4n^2+4n & n+1 & 2n+1 \\ 4n^2+4n+1 & n & 2n-1 \end{bmatrix}$$

Where n = sum of Armstrong number

Consider if Armstrong number = 370

n = 3 + 7 + 0 = 10

Encoding matrix will be

$$E = \begin{bmatrix} 880 & 21 & 40 \\ 440 & 11 & 21 \\ 441 & 10 & 19 \end{bmatrix}$$

Step 4: Multiply encoding matrix E with data matrix P and resultant matrix will be P that is encrypted matrix

$$C = \begin{bmatrix} 880 & 21 & 40 \\ 440 & 1121 & * \\ 441 & 10 & 19 \end{bmatrix} \begin{bmatrix} 69 & 78 & 67 \\ 82 & 89 & 80 \\ 84 & -25 & -25 \end{bmatrix}$$

$$C = \begin{bmatrix} 65802 & 69509 & 59640 \\ 33026 & 34774 & 29835 \\ 32845 & 34813 & 29872 \end{bmatrix}$$

Step 5: convert the resultant values in the form of string

65802, 69509, 59640, 33026, 34774, 29835, 32845, 34813, 29872

This is the cipher text generated which will be send to receiver and he/she will be able to read original message only after decryption.

1. Decryption Algorithm :

Decryption is the cryptographic bezique used to convert cipher text into plain text. It is performed by using secrete key which may be same as used in the encryption process or it may be different. In our system we are using same key for encryption and decryption purpose[7].

Step 1: convert the received cipher text into matrix form

$$C = \begin{bmatrix} 65802 & 69509 & 59640 \\ 33026 & 34774 & 29835 \\ 32845 & 34813 & 29872 \end{bmatrix}$$

Step 2: calculate the inverse of encoding matrix E for decryption matrix D using mathematical formula.

$$D = -451 \begin{bmatrix} -1 & 1 & 1 \\ 901 & -920 & -88 \\ 461 & 440 & \end{bmatrix}$$

$$D*C = 32845 \begin{bmatrix} 65802 & 69509 & 59640 & -1 \\ 33026 & 34774 & 29835 & * \\ 34813 & 29872 & -451 & 461 \end{bmatrix} \begin{bmatrix} 1 & 1 & \\ 901 & -920 & -880 \\ 440 & & \end{bmatrix}$$

$$D*C = \begin{bmatrix} 69 & 78 & 67 \\ 82 & 89 & 80 \\ 84 & -25 & -25 \end{bmatrix}$$

Step 3: Now resultant matrix containing the ASCII values for the alphabets in message. So, convert matrix into string.

69, 78, 67, 82, 89, 80, 84, -25, -25

Step 5: convert ASCII values into equivalent.

69 78 67 82 89 80 84 -25 -25
E N C R Y P T - -
This is original message send by sender and now decryption is done successfully.Reciever is able to read message[2], [8].

Previously we were using concepts Armstrong numbers with some algorithm .But this technique was having limitations. Because values are private keys of user it should not be known to other users. Another limitation was about Armstrong no. The technique which was used was not useful for decryption. This is because if Armstrong no contains 0 then inverse of encoding matrix is not possible which is required for decryption.Now we have overcome this limitation by using concept of unimodular matrix. Message length restrictions have also overcome using unimodular matrix[6].

III. Anyalsis And Result

The above technique involves keys with a minimum key length which reduces the efforts taken to encrypt the data. The key length can be increased if needed, with increase in character length. This increases the complexity thereby providing increased security[2].

A unimodular matrix is matrix with real square with its determinant det (A) = {-1, 0, 1}[6]

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 that means in ASCII values, Second step by adding with the digits of the Encoding matrix to form the required encrypted data using unimodular matrix. Tracing process becomes difficult with this technique[8].

This is because data is encrypted by key usingArmstrong number and again this Armstrong number is encrypted by using as key. So it is more secure.In this proposed technique encryption algorithm is too difficult to trace or hack externally[9].

IV. 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[3]. 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[10], [2].

References

[1]. Ajmal, K., et al. Security using Colors, Figures and Images. in International Conference on Emerging Technology Trends on Advanced Engineering Research (ICETT'12) Proceedings published by International Journal of Computer Applications (IJCA). 2012.
[2]. Belose, S., M. Malekar, and G. Dharmawat, Data Security Using Armstrong Numbers. International Journal of Emerging Technology and Advanced Engineering. ISSN, 2012: p. 2250-2459.
[3]. Stallings, W., Cryptography and Network Security, 4/E. 2006: Pearson Education India.
[4]. Anoop, M., Public key Cryptography-applications Algorithms and Mathematical Explanations. Tata Elxsi Ltd, India, 2007.
[5]. Rescorla, E., Diffie-Hellman key agreement method. 1999.
[6]. Weisstein, E.W., Unimodular matrix. 2003.
[7]. Cormen, T.H., et al., Introduction to algorithms. Vol. 6. 2001: MIT press Cambridge.
[8]. Deepa, S.P., S. Kannimuthu, and V. Keerthika. Security using colors and Armstrong numbers. in Innovations in Emerging Technology (NCOIET), 2011 National Conference on. 2011. IEEE.
[9]. Bansode, A., et al., Data Security in Message Passing using Armstrong Number.
[10]. Saoji, S., et al., Securing e-mails in XML format using colors and Armstrong numbers. International Journal of Scientific & Engineering Research, ISSN, 2013: p. 2229-5518.