IJITKM 0973-4414 Volume-10, Number-2 Jan-June 2017 pp. 34-36 **Impact Factor 2.8** available online at www.csjournalss.com

Encryption Algorithms with Hypothetical Encryption/Decryption in Network Security

Ms Manoj Kumari[1], Mr.Ramesh loar[2], Mr. Anil Vadhwa[3]
[1] M.Tech (CSE) Student, [2]Assistant Professor, [3]Assistant Professor,
RPS College of Engineering and Technology, Balana Mohindergarh

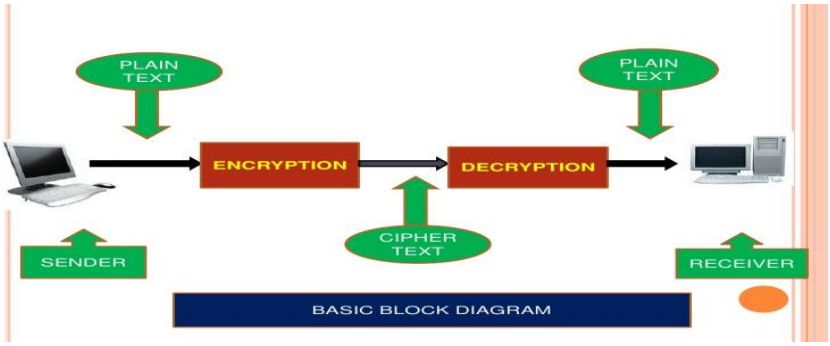
Abstract: Encryption is the process of converting a plain text message in to cipher text which can be decode back in to the original message. An encryption algorithm a key is used in the encryption and decryption of data. There are various types of data encryption which form the basis of network security. Encryption schemes are based on block or stream cipher.
The type of the keys length used depends upon the encryption algorithm and the amount of security needed. In Conventional symmetric encryption a single key is used. With this key the sender can encode a message and a receiver can decode the message but the security of the key becomes problematic. In asymmetric encryption, the encryption key and decryption key are different. One is a public key by which the sender can encrypt the message and the other is a private key by which the receiver can decrypt the message and vice-versa. With probabilistic encryption algorithms a crypto analyst can no longer encrypt random plain texts looking for correct cipher text. Since multiple cipher texts will be developed for one plain text, even if he decode the message to plain text, he does not know how far he had decided the message correctly. To illustrate, a crypto analyst has a certain cipher text ct_i. Even if he guesses message correctly, when he encrypts message the result will be completely different ct_j.
Keywords: - Encryption, Decryption, private key, Wireless Sensor Network, Broadcasting Applications.

Introduction

The necessity of information security within an organization have undergone major changes in the past and present times. In the earlier times physical means is used to provide security to data. With the advent of computers in every field, the need for software tools for protecting data. The important tool designed to protect data and thwart illegal users is computer security.
Security mechanisms usually involve more than an algorithm for encryption & decryption purpose and as well as for generation of sub keys to be mapped to plain text to create cipher text. It means that participants be in possession of some secret information, which can be used for protecting data from unauthorized use.
Thus an algorithm has to be developed within which security services and mechanisms can be viewed. To identify and support the security services of an organization at its effective level, the manager needs a systematic way. One approach is to consider three aspects of information security that is Security attack, Security mechanism and Security services. Security attack identifies different modes by which intruder tries to get unauthorized information and the services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.
As the importance of information systems is ever growing in all most all fields, electronic information takes on many of the roles, earlier they being done on papers. Few information integrity functions that the security mechanism has to support are security and confidentiality of the data to be transmitted and authentication of users.

Proposed Methodology & Algorithm

The type of operations used for transforming plain text to cipher text. All encode algorithms are depended on two general principles. Substitution in which each element in the plain text is mapped to another element and transposition in which the elements in the plain text are re arranged. Mainly all systems involve multiple steps of substitution and transpositions.
The number of keys used. If the sender and receiver use the same key, the system is called as symmetric, single key, secret key or conventional encode.



In this cryptographic algorithm for keys generating we used a very strong and lightweight block cipher algorithm that given as:

The steps that are involved in the proposed block cipher algorithm are as follows.

Step #1. The decimal values and letters of the plain text are given numerical values starting from 0.

Step #2. A random matrix is used as a key. Let it be X.

Step #3. A "Ternary Vector" for 3^3 values i.e. from 0 to 26 is generated.

Step #4. Let this be "Y".

Step #5. 1 is subtracted from all the values of ternary vector.

Step #6. The modified ternary vector is multiplied with the matrix key.

Step #7. A sign function is applied on the product of ternary vector & matrix key.

Step #8. 1 is added to all values of Step #7.

Step #9. A sequence is generated which is used as sub key

Step #10. The sub key is added to the individual numerical values of the message to generate cipher text.

Example

Encryption.

Plain Text	A	v	n	K	R	I
Alpha Numeric equivalent	10	31	23	20	27	18
Key	2	0	0	18	0	3
Add	12	31	23	38	27	21
Mod36	12	31	23	02	27	21
Cipher Text	C	v	n	02	R	L

Decryption

Cipher Text	C	v	n	02	R	L
Alpha Numeric equivalent	12	31	23	02	27	21
Add 36	12	31	23	38	27	21
Key	2	0	0	18	0	3
Subtract	10	31	23	20	27	18
Plain Text	A	v	n	K	R	I

As the model is probabilistic in nature, it is not only free from Differential and Linear cryptanalysis but also free from Chosen Cipher text attack. The model is also free from public key attacks. The second algorithm considers

not only the key but also time stamps and Initialization Vector to generate a sequence which is used as sub key to generate cipher text. The study outlines the components of these algorithms and their strength in a real time environment.

This process of improvement has been spurred on by the ever-growing user demand for security to the transmission (and storage) of information. The Postwar II period ushered in a new multifaceted era of advances in science and technology; emergence of multinational corporations; and globalization of economic activity. This change has and will continue to put heavy user demand on security to data in communication systems and networks. Increased competition globally in the ecommerce and other applications underlines the need for secured communication. For data storage and transmission, encryption becomes imperative for security and confidentiality.

Conclusion/Future Work

The present work deals with plain text being represented by numerical and characters of English alphabet. The work can be improved so that it can support the characters of not only English but also of other languages as well. The work can also be improved to support not only text but also other forms of message transmission like audio, video and image

References

1. Amjay Kumar, Ajay Kumar: Development of New Cryptographic Construct using Palmprint Based Fuzzyvoult, EURASIP Journal on Adv. In Signal Processing, Vol 21, pp 234-238, 2009
2. Baocang Wang, Qianhong Wu, Yupu Hu: A Knapsack Based Probabilistic Encryption Scheme, On Line March 2007, www.citeseer.ist.psu.edu.
3. Bluekrypt 2009: Cryptographic Key length Recommendations, http://www.keylength.com
4. Blum L., Blum M , Shub M. : A simple unpredictable pseudo random number generator , SIAM J. compute , 1986, 15, (2), pp 364-383.
5. Brics: Universally comparable notions of key exchange and secure channels, Lecture Notes in Computer Science, Springer, Berlin, March 2004.
6. Sage.math.Washington.edu/home/jetchev/Public.html/docs/jetchev-talk.ppt- Broadcast encryption schemes.
7. Brassard G.: Modern Cryptology , a tutorial lecture Notes on the computer science , (325) ,(spring-verlas) .
8. Bruce Scheneier: Applied cryptography (John Wiley & sons (ASIA) Pvt. Ltd.
9. Carlone Fontaine & Fabien Galand: A Survey of Homomorphic Encryption for non specialists, EURASIP Journal,Vol 07, Article 10.
10. Donavan G.Govan, Nathen Lewis: Using Trust for Key Distribution & Route Selection in Wireless Sensor Networks, International Conference on Network Operations & Management, IEEE Symposium 2008, PP 787-790.
11. Dorothy E. Denning et al.: Time Stamps in Key Distribution Protocol, Communication of ACM, Vol 24, Issue 8, Aug 1981, pp 533-536.