ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

Network Security and Encryption Schemes

Anjali[1], Ashish Vashisht[2]
M.Tech Student[1], Assistant Professor[2]
Department of Computer Science
Kurukshetra Institute of Technology and Management, Bhor Saidan, Kurukshetra, India

Abstract:
Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. The businesses create an “intranet” to remain connected to the internet but secured from possible threats.

Keywords: Cipher, Encryption, Security, Algorithm

I. INTRODUCTION

The necessicity 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 files and other information stored on the computer became important. The important tool designed to protect data and thwart illegal users is computer security. With the introduction and revolution in communications, one more change that affected security is the introduction of distributed systems which requires carrying of data between terminal user and a set of computers. Network security measures are needed to protect data during their transmission. The mechanisms used to meet the requirements like authentication and confidentiality are observed to be quite complex. Security mechanisms usually involve more than a particular algorithm or protocol for encryption & decryption purpose and as well as for generation of sub keys to be mapped to plain text to generate cipher text. It means that participants be in possession of some secret information (Key), which can be used for protecting data from unauthorized users. Thus a model 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.

II. PROJECT WORK

In this work an attempt has been made to generate two algorithms which provide security to data transmitted. The first algorithm considers a random matrix key which on execution by a series of steps generates a sequence. This sequence is used a sub key to build three different encryption models. Each model can be used for encryption of data. The second algorithm considers not only the key but also initialization vector and a time stamp to generate sub keys which are used for encryption process. And also a mechanism has been discussed which identifies any garbled key while transmitted from the Key Distribution Centre. In this work both the algorithms are discussed in terms of computational security, computational complexity and computational overhead. Both the algorithms are studied for their strengths and limitations. A crypto analytical study of the algorithms with emphasis on probabilistic encryption is also considered in this study. The encryption algorithms are compared with standard algorithms like RC4 and DES. The algorithms are also discussed in terms of its applications and also about their advantages and limitations in network security environment.

III. LITERATURE SURVEY

A crypto system [1,2,3,4] is an algorithm which include all possible plain texts, cipher texts and keys. There are two general types of key based algorithms: symmetric and public key.

a) Symmetric Encryption Schemes:

With *symmetric-key encryption*, the encryption key can be calculated from the decryption key and vice versa. With most symmetric algorithms, the same key is used for both encryption and decryption, encryption can be highly efficient, so that users do not experience any significant time delay as a result of the encryption and decryption. Symmetric-key encryption also provides a degree of authentication, since information encrypted with one symmetric key cannot be decrypted with any other symmetric key. Thus, as long as the symmetric key is kept secret by the two parties using it to encrypt communications, each party can be sure that it is communicating with the other as long as the decrypted messages continue to make sense. Encryption functions normally take a fixed-size input to a fixed-size output, so encryption of longer units of data must be done in one of two ways: either a block is encrypted at a time and the blocks are somehow joined together to make the cipher text, or a longer key is generated from a shorter one and XOR'd against the plaintext to make the cipher text. Schemes of the former type are called block ciphers, and schemes of the latter type are called stream ciphers.

b) Public-Key Encryption

The most commonly used implementations of public-key [4,5] encryption are based on algorithms patented by RSA Data Security. Therefore, this section describes the RSA approach to public-key encryption. Public-key encryption (also called asymmetric encryption) involves a pair of keys a public key and a private key, used for security & authentication of data. Each public key is published, and the corresponding private key is kept secret. Data encrypted with one key can be decrypted only with other key. The scheme says public key is distributed and encryption being done using this key. In general, to send encrypted data, one encrypt's the data with the receiver's public key, and the person receiving the encrypted data decrypts it with his private key. Compared with symmetric-key encryption, public-key encryption requires more computation and is therefore not always appropriate for large amounts of data. However, a combination of symmetric & Asymmetric schemes can be used in real time environment. This is the approach used by the SSL protocol. As it happens, the reverse of the scheme also works: data encrypted with one's private key can be decrypted only with his public key. This may not be an interesting way to encrypt important data, however, because it means that anyone with receiver's public key, which is by definition published, could decipher the data. And also the important requirement with data transfer is authentication of data which is supported with Asymmetric encryption schemes, which is an important requirement for electronic commerce and other commercial applications of cryptography.

c) Probabilistic encryption schemes

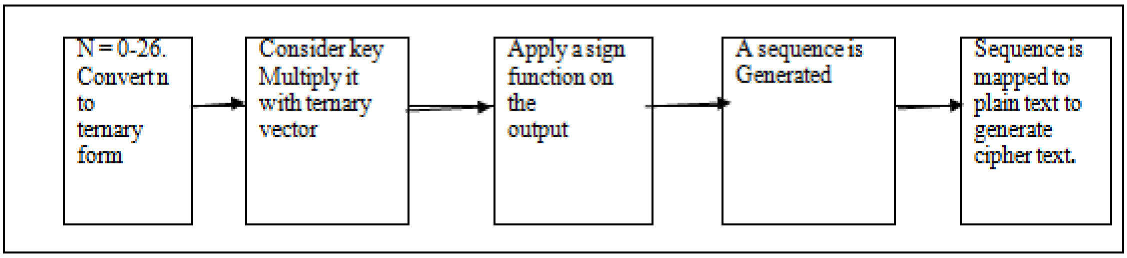
In public key encryption there is always a possibility of some information being leaked out. Because a crypto analyst can always encrypt random messages with a public key, he can get some information. Not a whole of information is to be gained here, but there are potential problems with allowing a crypto analyst to encrypt random messages with public key. Some information is leaked out every time to the crypto analyst, he encrypts a message.

An encryption scheme consists of three algorithms: The encryption algorithm transforms plaintexts into cipher texts while the decryption algorithm converts cipher texts back into plaintexts. A third algorithm, called the key generator, creates pairs of keys: an encryption key, input to the encryption algorithm, and a related decryption key needed to decrypt. The encryption key relates encryptions to the decryption key. The key generator is considered to be a probabilistic algorithm, which prevents an adversary from simply running the key generator to get the decryption key for an intercepted message. The following concept is crucial to probabilistic cryptography:

IV. PROPOSED SYSTEM

In the proposed system two algorithms are developed. The first algorithm uses a matrix key which on multiplication with a ternary vector and applying a sign function on the product generates a sequence. This sequence will be used to generate three different models of substitution technique. Thus the algorithm is considered to be a substitution algorithm which uses a single key to be shared by both the sender and receiver, and the cipher processes the input element continuously, producing output one element at a time. The new encryption algorithm is based on the concept of Poly alphabet cipher which is an improvement over mono alphabet. Three models are developed from the given algorithm [6, 7]. The first two models like Model 1 & Model 2 can be classified under block ciphers and Model 3 is a stream ciphers. Each model is having its own advantages and limitations. The second algorithm considers not only key but also initialization vector and a time stamp to generate sub keys which are used for encryption process. Model 1 A new Substitution cipher for data security.
The algorithm that is going to be discussed in this work will generate a Sequence. The algorithm considers a matrix key and executes a sequence of steps which generates the sequence. Each block of plain text is replaced by summation of alphanumerical value of the plain text and the sequence generated to form cipher text. Thus the cipher text obtained becomes computationally infeasible to break without knowing the key

Model 1: A new Substitution cipher for data security.


N=0-26. Convert n to ternary form
Consider key Multiply it with ternary vector
Apply a sign function on the output
A sequence is Generated
Sequence is mapped to plain text to generate cipher text.

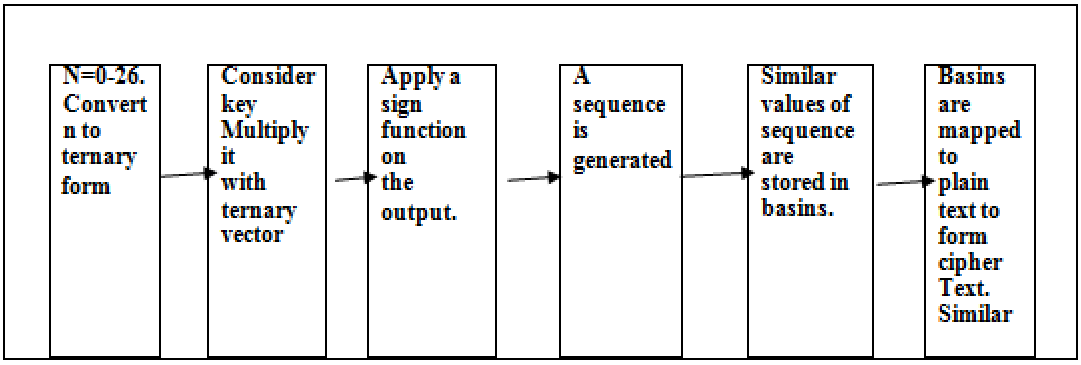
ADVANTAGES:

1.Even if the algorithm is known, it is computationally infeasible to generate matrix key.
2. Versatile to users: Different users of internet can use different modified versions of the new algorithm. Since in this algorithm, the sign function is used, it is supposed to be strong enough.

Model 2
A New Variable Length Key Block Cipher Technique for Network Security in Data Transmission

The algorithm that is going to be discussed in this work is going to consider a random matrix key which on execution of sequence of steps generates a sequence. Based on the equality of values this sequence is being divided into basins. Each basin represents one block of data. Depending on starting input plain text character, corresponding basin is considered as a key. Each block of plain text is converted to alphanumerical values which are mapped with the sub key to generate cipher text. The procedure is repeated for certain plain text depending on chosen value. Thus the cipher text obtained becomes very difficult to be broken without knowing the key. Key Words: Cryptography, Variable length key, Encryption Algorithm, Example, Add function.

Model 2: A new variable length key for data encryption.


N=0-26. Convert n to ternary form
Consider key Multiply it with ternary vector
Apply a sign function on the output.
A sequence is generated
Similar values of sequence are stored in basins.
Basins are mapped to plain text to form cipher Text. Similar

ADVANTAGES:

1. It is almost impossible to extract the original information.
2. Even if the algorithm is known, it is difficult to extract the matrix key.
3. Versatile to users. Different users of internet can use different modified versions of the new algorithm.

V. RESULTS

Encryption models provided in ranged over new block cipher techniques to stream cipher techniques. The first algorithm considers a matrix key executes a sequence of steps which generates a sequence. This sequence is used to generate four different encryption models. Model 1 is a new symmetric encryption technique. In the model it is observed that, for a given key the total computational overhead of the model 1 is 486 calculations. The complexity of the model by its construction is o(n), by its strength it is exponential in nature. It is also observed that by slight variations in the key alot of variations in cipher text is identified which provides more strength to the generated model. : this algorithm is completely free from cipher text only, type of attack. By the other attacks, the key may not be retrieved but a part of plain text may be retrieved.

VI. FUTURE WORK

The present work deals with plain text being represented by numerical and charaters of English alphabet. The work can nr 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, vedio and images.

VII. CONCLUSION

The study represents the importance of Encryption of data for storage and transmission. The significance of encrypted data can be identified in light of the mushrooming applications and globalization of communication. The advantages of encrypting data manifest themselves in the form of security & confidentiality in real time applications. Encryption of data is of particular significance in applications like email, ecommerce. E-cash where highly vulnerable lines is accessed or communication of high quality data.

VIII. REFERENCES

[1]. Amjay Kumar, Ajay Kumar: “Development of New Cryptographic Construct using Palmprint Based Fuzzyvoult” EURASIP Journal on Adv. In Signal Processing, Vol 21, 2009.

[2].Brassard G.: “Modern Cryptology“ a tutorial lecture Notes on computer science , (325) ,(spring-verlas) .

[3].Bruce Scheneier: “Applied cryptography” (John Wiley & sons (ASIA) Pvt. Ltd.

[4].Henry Baker and Fred Piper: “Cipher systems” (North wood books, London 1982).

[5].J.William stalling: “Cryptography and network security” (Pearson Education,ASIA1998).

[6].Krishna A. V. N., S. N. N. Pandit: “A new Algorithm in Network Security for data transmission” Acharya Nagarjuna International Journal of Mathematics and Information Technology, Vol: 1, No. 2, 2004.

[7]. Krishna A. V. N, S. N. N. Pandit, A. Vinaya Babu: “A generalized scheme for data encryption technique using a randomized matrix key” Journal of Discrete Mathematical Sciences & Cryptography, Vol 10, No. 1, Feb 2007.