International Journal of Advanced Technology in Engineering and Science
Vol. No.4, Issue No. 08, August 2016
www.ijates.com
ijates
ISSN 2348 - 7550

PERFORMANCE EVALUATION OF NEW ENCRYPTION ALGORITHMS WITH EMPHASIS ON PROBABILISTIC ENCRYPTION

T.Deepak[1], A.Zakiudn Ahmed[2], P. Rizwan Ahmed[3]

[1]*Research Scholar, Computer Science*
[2]*Assistant Professor, Pg & Research Departmento of Computer Science*
[3]*Assistant Professor & Head, Department Of Computer Application & Pg,*
Mazharul Uloom College, Ambur, Tamil Nadu, (India)

ABSTRACT

The necessity of information security within an organization has 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.

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.

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.

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.

Keywords: Encryption, Decryption, Cipher Text

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.

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. This general model shows that there are four basic tasks in designing a particular security service.

1. Designing an algorithm for performing encryption & decryption process.
2. Generating the secret information with the help of algorithm of step 1.
3. Identifying methods for the distribution and sharing of secret information.
4. Identifying rules to be used by both the participating parties to make it secured.

A crypto system is an algorithm, plus all possible plain texts, cipher texts and keys. There are two general types of key based algorithms: symmetric and public key.

The process of symmetric-key encryption can be very fast as the users do not experience any significant time delay because of the encryption and decryption. Symmetric-key encryption provides security to data as the key is shared only by the participating parties. It 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 confident that it is communicating with the other as long as the decrypted messages specify a meaningful sense.

Symmetric-key encryption will be successful only if the symmetric key is kept secured by the two parties involved. If anyone else discovers the key, it affects both confidentiality and authentication. The success of a symmetric algorithm rests in the key, divulging the key means that anyone could encrypt and decrypt messages. As long as the communication needs to remain secure, the key must be protected between the participating parties.

Encryption and decryption with a symmetric algorithm are denoted by $E_K(M) = C$

$$D_K(M) = P$$

Symmetric algorithms can be divided into two categories. Some operate on the plain text a single bit or byte at a time, these are called stream algorithms or stream ciphers. Others operate on group of bits or characters. Such algorithms are called block algorithms.

Public Key algorithms use two keys, one key for encryption and the other for decryption. One key can be called as public key which can be declared public and the other one is private that is, the key is known only to the particular participating party. And also public key cryptography can be used for digital signing as it supports authentication of users. The information encrypted with one key will only be decrypted with the other key. Furthermore the decryption key cannot be calculated from the encryption key. Figure 1.3 shows a simplified view of the way public-key encryption works.

Compared with symmetric-key encryption, public-key encryption requires more computation and is therefore not always appropriate for large amounts of data. However, it's possible to use public-key encryption to send a symmetric key, which can then be used to encrypt additional data. This is the approach used by the SSL protocol. This provides Authentication, Integrity & Confidentiality of Information at low computing power. Since authentication of the users is very important in applications like e-commerce and other similar applications, public key cryptography is of much use.

Encryption and decryption can be represented in a public key scheme is $E_{Kpu}(M) = C$

$$D_{Kpr}(C) = M$$

Where Kpu is the public key and Kpr is the private key.

In public key encryption there is always a possibility of some information being leaked out. A crypto analyst tries to get some information based on ones public key. Complete information cannot be gained here but a part of information may be gained. In probabilistic Encryption, multiple cipher texts are generated for one plain text, a cryptanalyst cannot generate any information by chosen plain text and chosen cipher text attacks.

An attempted crypto analysis is called an attack. There are five types of attack. Each of them assumes that the crypto analyst has complete knowledge of the encryption algorithm used.

II. CIPHER TEXT ONLY ATTACK

Here the intruder is in hold of cipher text only. The crypto analyst has cipher text of several messages, all of which have been encrypted using the same encryption algorithm. The crypto analyst's job is to recover the plain text or the key used to encrypt the messages, in order to decrypt other part of messages encrypted with the same keys.

1. **Known Plaintext attack:** The crypto analyst is in possession of pairs of known plain text and cipher text. His job is to get the key used to encrypt the messages or an algorithm to decrypt any messages encrypted with the same key.

1. **Chosen Plaintext Attack (CPA):** Here the crypto analyst is in hold of not only cipher text but also parts of chosen plain text. Here the intruder is identified to be placed at encryption site to do the attack. Differential crypto analysis is an example of this mode.

2. **Chosen cipher text attack (CCA):** Under the CCA model, the crypto analyst is in possession of chosen cipher text and corresponding plain text being decrypted from the private key. After it has chosen the messages, however, it only has access to an encryption machine.

3. **Chosen text:** In this model, the analyst posses the encipher algorithm, Cipher text to be decrypted, chosen plain text messages and corresponding cipher texts, fabricated cipher text with the corresponding decrypted plain texts developed by the private key.

III. CONCLUSION

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 research paper.

In this paper 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.
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.

REFERENCES

1. Brics: Universally comparable notions of key exchange and secure channels, Lecture Notes in Computer Science, Springer, Berlin, March 2004.
2. 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.
3. Amjay Kumar, Ajay Kumar: Development of New Cryptographic Construct using Palmprint Based Fuzzyvoult, EURASIP Journal on Adv. In Signal Processing, Vol 21, pp234-238, 2009.
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. R.H.Rahnan, N,Nowsheen: A New Symmetric Key Distribution Protocol Using Centralized Approach, Asian Journal of Information Technology, 2007 6(8) pp 911-915.
7. Krishna A.V.N., A.Vinaya Babu: Web and Network Communication security Algorithms, Journal on Software Engineering, Vol 1,No.1, July 06, pp12-14.
8. Bluekrypt 2009: Cryptographic Key length Recommendations.