A Survey on Cryptographic Techniques for Network Security

Ankit Garg[1], Kamal Kumar Sharma[2], Sharad Chauhan[3]

[1]Student, M. Tech, ESEAR, Ambala
[2]Professor, Dept. of ECE, E-Max group of Institutions, Ambala
[3]Assistant Professor, Dept. of CSE, E-Max group of Institutions, Ambala

Abstract— **Cryptography plays a vital role in information security system against various types of attacks. This security mechanism uses some algorithms to scramble data into unreadable text which can be only being decrypted by party those possesses the associated key. The two important characteristics that identify and differentiate encryption algorithms from another are their capability to secure the protected data against attacks and their speed and effectiveness in securing the data. Cryptography is method that provides the security mechanism in timely driven fashion. Main objective of this paper is to compare the most commonly used algorithms for data encryption. Main concern in this paper is the performance analysis of different algorithms under different settings.**

Keywords— **cryptography, plain text, security, cipher text, encryption, decryption**

I. INTRODUCTION

The security of network is a big issue for security administrators because network is growing day by day. Security on the Internet and on Local Area Networks is now at the forefront of computer network related issues. Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, modification, denial of a computer network, misuse and network-accessible resources. Network security involves authorization of access to data in network, which is controlled by the network administrator. Each and every client who is working on the internet wants security of information but sometimes he or she do not know that someone else may be a intruder is collecting the information. The information is an asset that must be protected. Network security is the process by which digital information assets are protected, the goal of security is to protect confidentiality, to maintain integrity and to assure availability. To secure the entire network system and the information, one specific methodology is required which can be capable of providing the complete security solutions.

II. CRYPTOGRAPHY

Cryptography is the study of Secret (crypto) Writing (graphy). It is the art or science of encompassing the principle and method of transforming an intelligible message into coded form or unreadable form at the senders end and that coded form then transforming the message back to its original form at the receivers end. As we know the field of cryptography has advanced, cryptography is the study of techniques of securing the integrity and authenticity of transfer of information under difficult circumstances. Cryptography encodes information in such a way that nobody can read it, except the person who holds the key i.e. receiver. More advanced crypto techniques ensure that the information being transmitted has not been modified during the transmission of information from sender to receiver. The term cryptography and steganography are different, in cryptography the hidden message is always visible to all, and because information is in plain text form but in steganography hidden message is invisible.

A. Various goals of cryptography

1) Confidentiality:

The information in computer is transmitted and has to be accessed only by the authorized party and not by any other unauthorized party.

2) Authentication:

The information received by any system has to check the identity of the sender that whether the information is arriving from an authorized party or a false identity.

3) Integrity:

Only the authorized party is allowed to modify the information transmitted by the sender. No one in between the sender and receiver are allowed to modify or change the given message.

4) Non Repudiation:

Non repudiation is the assurance that both parties the sender and the receiver of message should be able to deny the transmission.

5) Access control:

Only the authorized persons are able to access the given information, any unauthorized person cannot access the given information.

B. Basic terms related to cryptography

1) Plain Text:

Plain text is the original message that the sender wishes to transmit to others. For example, Alice is a person wants to send “Hello how are you” message to the person Bob. Here “Hello how are you” is a plain text message.

2) Cipher Text:

The message that cannot be understood by any unauthorized person or a meaningless message is what we call as Cipher text. For Example, “Ajd67@91ukl8*^5%” is a Cipher Text produced for “Hello how are you”.

3) Encryption:

Encryption is the process of converting plain text into cipher text in such a way that only authorized parties can read our message. The encryption process requires two things- an encryption algorithm and a key. An encryption algorithm is the technique that has been used for encryption of plain text. The encryption takes place at the sender side.

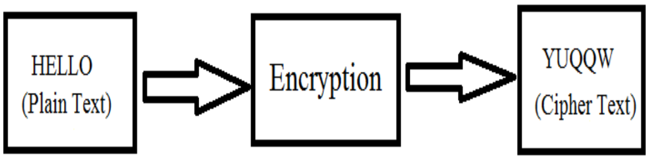


Fig 1: Encryption process

4) Decryption:

A reverse process of encryption is called as Decryption. The process of converting Cipher text into Plain text is called decryption. The decryption process requires two things- a decryption algorithm and a key. A decryption algorithm is the technique that has been used for the decryption of cipher text. Generally the encryption and decryption algorithm are same and the decryption takes place at the receivers end.

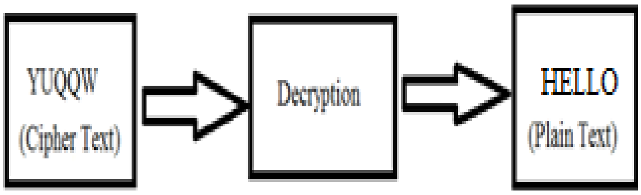


Fig 2: Decryption process

5) Key:

A key is the numeric or alpha numeric text or may be a special symbol. The key is used for the encryption process takes place on the plain text and at the time of decryption process takes place on the cipher text. For example, if the Alice uses a key of 4 to encrypt the plain text "Hello" then cipher text produced will be "Lipps".

III. Symmetric and Asymmetric encryptions

There are two types of techniques that are commonly used for the encryption/decryption of the secured data i.e. Asymmetric and Symmetric encryption technique.

A. Symmetric Encryption/Decryption Technique:

In case of Symmetric Encryption/decryption, same cryptography key are used for encryption of plaintext and decryption of cipher text. Symmetric key encryption is simpler and faster but their main drawback is that both the users need to transfer their keys in a secure way for the encryption and decryption.

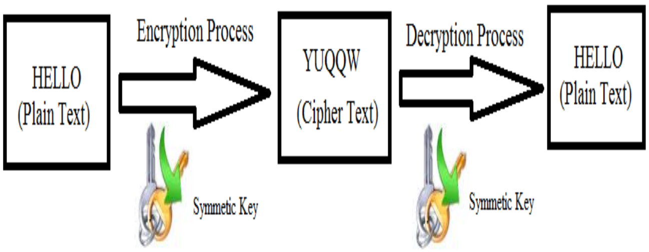
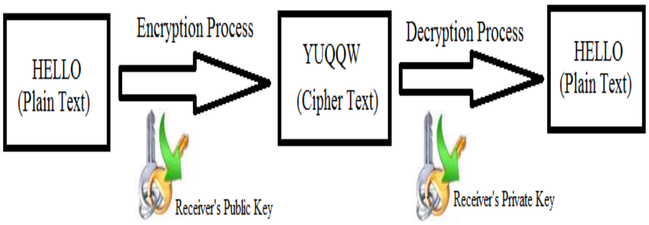


Fig 3: Symmetric key cryptography

In the figure 3, there is only one key used for both encryption and decryption of secured data. So the main problem over this system is users have to transfer their keys also in a very safe manner. If the key is disclosed to any other person, then system will be collapsed.

B. Asymmetric Encryption/Decryption Technique:

In case of Asymmetric encryption process, two keys are used i.e. public and private key. It is also known as Public Key Cryptography (PKC), because users tend to use two keys: the public key and the private key. If sender wishes to encrypt the message then it uses the receiver's public key for encryption and at the receivers end the receiver use its own private key to decrypt the message.



In figure 2, there are two different keys are used for encryption and decryption of data i.e. Public key and Private Key.

IV. Algorithm Comparison

A. DES (Data Encryption Standard):

Data Encryption Standard is a block encryption algorithm. It is a symmetric algorithm, so in this algorithm same key is used for encryption and decryption both. This algorithm uses a 64-bit key. From these 64 bits, 56 bits make independent key, which determines the exact cryptography transformation process, and 8 bits are used for error detection in DES.

Six different permutation operations are used both in key expansion part and cipher part. The decryption of DES algorithm is similar to encryption, only the round keys are applied in reverse order during the decryption. Many attacks and methods recorded the weaknesses of DES, which made it an insecure. The DES is now considered to be insecure, due to the 56-bit key size being too small.

B. 3-DES:

It uses a 64 bit block size with 192 bits of key size. The encryption method is similar to the original DES but applied three times to increase the encryption level and the average safe time. 3DES is slower than the other block cipher methods.

C. AES:

The Advanced Encryption Standard algorithm (AES) also known as the Rijndael algorithm is a symmetric block cipher. It was recognized that Data Encryption Standard (DES) was not secure because of advancement in computer processing power. It can encrypt data blocks of 128 bits using symmetric keys of size 128 bit, 192 bit, or 256 bit. It has variable key length of 128, 192, or 256 bits; the default is 256 bits. It encrypts the data blocks of size 128 bits in 10, 12 and 14 rounds depending on the key size. The AES encryption is fast and flexible. AES algorithm can be implemented on various platforms especially in small devices. This algorithm has been tested for many security applications.

D. **Blowfish**:

The Blowfish is a symmetric block cipher that can be effectively used for encryption of secure data. It takes a key of variable-length of size from 32 bits to 448 bits, for encryption process. The Blowfish was designed by Bruce Schneier in 1993 as a fast and free alternative to existing encryption algorithms. Blowfish is license-free, so it is available free for all uses. Blowfish algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size used in Blowfish is 64 bits, and the key can be of any length up to 448 bits.

The comparison of symmetric encryption algorithms is based on key size, block size and rounds as shown in table 1:

Algorithm	Key size	Block size	Rounds
DES	56 bits	64 bits	16
3DES	112 bits or 168 bits	64 bits	48
AES	128 bits, 192 bits, 256 bits	128 bits	10,12 or 14
Blowfish	32-448 bits	64 bits	16

Table (1): Comparison of DES, 3DES, AES and Blowfish algorithms

V. LITERATURE SURVEY

E. Rohiem et. al. presents a novel method of using customized (AES) variable parameters is introduced. This method depends on a continuous parameters reconfiguration and a customization of each internal block. The customization depends on varying the four transformations (polynomial and affine transformations for S-Box (SB), ShiftRows (SR) transformation, and MixColumn (MC) transformation). Internal AES blocks (SB, SR, and MC) are varied each round. Further more, these blocks are randomly interconnected during each session. The ciphered output was tested using avalanche, strict avalanche, and other NIST tests. This method overcomes (ECB) mode problems which appear when there is high redundancy in the plain data and also increasing strength against brute force attacks. The proposed AES is implemented on Field programmable Gate Arrays (FPGAs)[1].

Sumedha Kaushik et. al. Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software , and information in a network. Only one particular element underlies many of the security mechanisms in use: Cryptographic techniques; hence our focus is on this area Cryptography. Cryptography is an emerging technology, which is important for network security. Research on cryptography is still in its developing stages and a considerable research effort is still required for secured communication [2].

Sweta K. Parmar et. al. Security is the most challenging aspects in the internet and network application. Internet and networks applications are growing very fast, so the importance and the value of the exchanged data over the internet or other media types are increasing. Information security has been very important issue in data communication. Any loss or threat to information can prove to be great loss to the organization. Encryption technique plays a main role in information security system. This paper gives a comparison of various encryption algorithms and then finds best available one algorithm for the network security [3].

Ritu Pahal et. al. With the fast progression of digital data exchange in electronic way, information security is becoming much more important in data storage and transmission. Cryptography has come up as a solution which plays a vital role in information security system against various attacks. This security mechanism uses some algorithms to scramble data into unreadable text which can be only being decoded or decrypted by party those possesses the associated key. Two types of cryptographic techniques are being used: symmetric and asymmetric. In this paper we have used symmetric cryptographic technique AES (Advance encryption standard) having 200 bit block as well as key size. And the same conventional 128 bit conventional AES algorithm is implemented for 200 bit using 5*5 Matrix. After the implementation, the proposed work is compared with 128 bit, 192 bits & 256 bits AES techniques on two points. These points are encryption and decryption time and throughput at both encryption and decryption sides [4].

Siddharth Ghansela Network security is main issue of this generation of computing because many types of attacks are increasing day by day. Establishing a network is not a big issue for network administrators but protecting the entire network is a big issue. There are various methods and tools are available today for destroying the existing network. In this paper we mainly emphasize on the network security also we present some major issues that can affect our network [5].

Amritpal Singh et. al. In today world importance of exchange of data over internet and other media type is eminent; the search for best data protection against security attacks and a method to timely deliver the data without much delay is the matter of discussion among security related communities. Cryptography is one such method that provides the security mechanism in timely driven fashion. Cryptography is usually referred to as "the study of secret", which is most attached to the definition of encryption. The two main characteristics that identify and differentiate encryption algorithm from another are their capability to secure the protected data against attacks and their speed and effectiveness in securing the data. This paper provides a comparative study between four such widely used encryption algorithms DES, of DES, 3DES, AES and RSA on the basis of their ability to secure and protect data against attacks and speed of encryption and decryption[6].

N.Lalitha et. al. In this paper we propose a data hiding technique using AES algorithm.Steganography and Cryptography are two popular ways of sending vital information in a secret way.Cryptography was introduced for making data secure. But alone cryptography cannot provide a better security approach because the scrambled message is still available to the eavesdropper. There arises a need of data hiding. So here we are using a combination of steganography and cryptography for improving the security. There are many cryptography techniques available; among them AES is one of the most useful techniques .In Cryptography, I have using

AES algorithm to encrypt a message using 128 bit key the message is hidden . In this proposed technique, we use advance hill cipher and AES to enhance the security level which can be measured by some measuring factors. The result of this work shows that this advance hybrid scheme gives better results than previous techniques [7].

VI. CONCLUSION

This paper mainly emphasize on the network security and some major issues that can affect network. This paper provides a comparative study of four widely used encryption algorithms DES, 3DES, Blowfish and AES. DES is the most vulnerable and can be easily broken by brute force attack. AES is the better algorithm in terms of performance and security.

REFERENCES

[1] A. E. Rohiem, F. M. Ahmed and A. M. Mustafa ’’FPGA Implementation of Reconfigurable Parameters AES Algorithm”, 13th International Conference on *Aerospace Sciences & Aviation Technology, ASAT- 13, May 26 – 28, 2009*

[2] Sumedha Kaushik Ankur Singhal, ”Network Security Using Cryptographic Techniques*”, International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 12, December 2012*

[3] Sweta K. Parmar and Prof K.C. Dave, ”A Review on Various Most Common Symmetric Encryptions Algorithms”, *IJSRD - International Journal for Scientific Research & Development| Vol. 1, Issue 4, 2013*

[4] Ritu Pahal and Vikas Kumar, ”Efficient Implementation of AES” *International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 7, July 2013*

[5] Siddharth Ghansela, “Network Security: Attacks, Tools and Techniques” *International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, June 2013*

[6] Amritpal Singh, Mohit Marwaha, Baljinder Singh, Sandeep Singh, “Comparative Study of DES, 3DES, AES and RSA”

[7] N.Lalitha, P.Manimegalai, V.P.Muthukumar, M.Santha,” Efficient data diding by using AES & advanced hill cipher algorithm” *International Journal of Research in Computer Applications and Robotics Vol.2 Issue.1*