A Study on Network Security Using Cryptography and Comparison of AES, DES Cryptographic Algorithms

[1]N.V.Poornima,[2]Dr.B.Srinivasan
[1]phd scholar , Department of computer science, Gobi Arts &Science College, Gobichettipalayam.
[2]Associate Professor, Department of computer science, Gobi Arts & Science College, Gobichettipalayam.

Abstract:

Network security has become more important to personal computer users, organizations, and the military. Data Security is the main aspect of secure data transmission over unreliable network. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. The task of network security not only requires ensuring the security of end systems but of the entire network. Data security is the utmost critical issue in ensuring safe transmission of information through the internet. Networks are very much needed but they are very prone to attacks because of security breaches and vulnerabilities in traditional establishments. There are many types of attacks which can be penetrated in our networks or edge devices. In internet, security is main aspect and the process of cryptography plays an important role to provide the security to the networks. Network Security & Cryptography is a concept to protect network and data transmission over wireless network. Network security and data security can be provided with the help encryption and decryption using cryptographic techniques and algorithms. In this paper, an attempt has been made to review the various Network Securityand Cryptographic concepts. This paper discusses the state of the art for a broad range of cryptographic algorithms that are used in networking applicationsand provide an overview on Network Security and various techniques through which Network Security can be enhanced i.e. Cryptography also studied cryptography along with itsprinciples. Cryptographic systems with ciphers are described. The cryptographic models and algorithms are outlined.

Keywords— **NetworkSecurity, Cryptography, Encryption, Decryption, Ciphers.**

I .INTRODUCTION

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password. Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication, nonrepudiation, and integrity control.

Network Security & Cryptography is a concept to protect network and data transmission over wireless network. Security of data can be done by a technique called cryptography. So one can say that cryptography is an emerging technology, which is important for network security.

Security goals

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

The three concepts describe the fundamental security objectives for both data and information and computing services.

Confidentiality

Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

Integrity

Assures that information and programs are changed only in a specified and authorized manner.

Availability and authenticity

Verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

Types of security attacks

1.Passive attacks

This type of attacks will not disturb the system resources; intruder will collect the information from the transaction. The goal of the opposite party is to obtain information that is being transmitted.

Types of passive attacks.

1.1 Traffic analysis

During a traffic analysis attack, the observer analyses the traffic and tries to determine the location of the communicating hosts and observes the patternof the message and alsothe length of exchanged messages. Later he will use all this information to predict the nature of communication. All incoming and outgoing traffic of the network is analysed, but not altered.

1.2 Release of message contents

Forreleasing a data Read contents ofmessage from sender to receiver. A passive attack monitors the contents of the transmitted data.

2. Active attacks

An active attack tries to alter system resources oraffect their operation. It involves some modification of thedata stream or the creation of a false stream. Types ofactive attacks:

2.1. Modification of messages

A part of valid message is altered, or that messages aredelayed or reordered.

2.2 Denial of service

An intruder may tries to putdownnetwork by sending numerous messages directed to a particular destination.

2.3. Replay

It involves the passive capture of a data unitand its subsequent retransmission to produce an unauthorized effect.

2.4. Masquerade

It takes place when one entity pretendsto be a different entity.

Security services

It is a service that is provided by a protocol layer ofCommunicating open systems and that ensures adequatesecurity of the systems or of data transfers. It enhances thesecurity of data processing and transferring.

Data integrity

It can apply to a stream of messages, a single message, or selected fields within a message. A loss of integrity isthe unauthorized modification or destruction of information.

Data confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personalprivacy and proprietary information. A loss ofconfidentiality is the unauthorized disclosure ofinformation.

Authenticity

Provide authentication to all the node and base stationfor utilizing the available limited resources. It also ensuresthat only the authorized node can participant for thecommunication.

Nonrepudiation

Nonrepudiation prevents either sender or receiver fromdenying a transmitted message. Thus, when a message issent, the receiver can prove that the alleged sender in factsent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in factreceived the message.

Access control

Access control is the ability to limit and control the access to host systems and applications viacommunications links. To achieve this, each entity tryingto gain access must first be identified, or authenticated, sothat access rights can be tailored to the individual.

Securitymechanism

Encipherment

It is a security mechanism that involves the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it not intended Encipherment of data, can provide confidentiality.

Data integrity

A variety of mechanisms used to assure the integrity of data unit or stream of data units. Forexample, it depends short check value that has been related by specific process from data itself.The receiver receives the data and the check value. He creates a new check value from received data and compares the newly created check value with the one received. If the two check values are the same the integrity of the data has been preserved.

Digital signature

Data appended to, or a cryptographic transformation of, a data unit that allows recipient of the data unit to proves the source and integrity of the data unit and protect against forgery.

Authentication exchange

Authentication is aprocess in which the credentials provided are compared to those on file in a database of authorized user's information on a local operating system. If the credentials match, the process is completed and the user is granted authorization for access.

Traffic padding

The traffic padding is insertion of bogus data or bits into gaps in a data stream to frustrate traffic analysis attempts.

Bit padding

A single set ('1') bit is added to the message and then as many reset ('0') bits as required (possibly none) are added. The number of reset ('0') bits added will depend on the black boundary to which the message needs be extended. In bit terms "10000……000".

Routing control

Route control is a specialized type of network management that aims to improve internet connectivity, and reduce bandwidth cost and overall internetwork operations.

Notarization

Notarization is defined to be synonymous with "data certification". That is, the notary certifies the data is valid are correct, where the meaning of "correct" is necessarily dependent on the type of the data being certified.

Access control

In the field of physical security and information security access control is the restriction of access to view or use resources in computing environment.

II.CRYPTOGRAPHY MECHANISM

Cryptography is transmitting information in a specific frame so that those for whom it is expected can read and process it. The term is regularly connected with plaintext message into cipher text (a procedure called encryption), then back once more (known as decryption). There are, three sorts of cryptographic plans commonly used to achieve data security: symmetric cryptography, asymmetric cryptography, and hash functions.

Purpose of cryptography

Authentication Authentication mechanism helps to prove the identity of the user. And also this procedure ensures that the origin of the message is correctly identified.

Confidentiality

The principle of confidentiality specifies that only the sender and the intended recipient should be able to process the contents of a message.

Availability

The principle of availability states that resources should be available to authorized parties all the times.

Integrity: The integrity mechanism ensures that the contents of the message remain the same when it reaches the intended recipient as sent by the sender.

Access Control

Access Control specifies and controls who can access the process.

Cryptography terms

KeyA key is a numeric or alpha numeric text or may be a unique figure to hide the original data.

Plain Text The original message that the individual wishes to send with the other is denoted as Plain Text. For example, a man named Alice wishes to send "Hi Friend how are you" message to the individual Bob. Here "Hi Friend, how are you" is a plain text

.

Cipher Text This is a scrambled message that can'tbecomprehended by any one is called Ciphertext.forinstanceAssume,"Ajd672#@91uk l8*^5%" is a Cipher Text created for "Hi Friend how are you".

EncryptionA procedure of changing over plain text into figure content is called as Encryption. This procedure requires two things-an encryption algorithm and a key. Encryption of information happens at the sender side.

DecryptionA reverse procedure of encryption is called as Decryption. In this procedure Cipher text is changed intoPlain text. Decoding process requires two things-an unscrambling algorithm and a key.

Cryptographic principles

Redundancy

All encrypted messages must contain some redundancy, the information that is not required for understanding the message reducing the chances for a passive intruder to make attacks. Messages must contain some redundancy.

Freshness

Some method is needed to stop replay attacks. One such measure is including in every message a timestamp valid only for, say, 10 seconds. The receiver can then just keep

messages around for 10 seconds, to compare newly arrived messages to previous ones to filter out duplicates. Messages older than 10 seconds can be thrown out, since any replays sent more than 10 seconds later will be rejected as too old.

Types of cryptography

Secret Key Cryptography in this type of cryptography same key is used for both encryption and decryption. It is also known as symmetric key cryptography. Example for this type may include DES, Triple DES, AES, RC5 and etc.

Public Key Cryptography When two different keys are used, for encryption and decryption that type of cryptography is known as public key cryptography. It is also known as asymmetric key cryptography example of this type includes RSA, Elliptic Curve and etc.

Hash function Unlike secret key and public key algorithms, hash functions, also called message digests or one-way encryption, have no key. Hashed Message Authentication Code (HMAC): Combines authentication via a shared secret with hashing.

III. ENCRYPTION ALGORITHMS

Symmetric key cryptography

Data Encryption Standard (DES) DES (Data Encryption Standard) algorithm purpose is to provide a standard method for protecting sensitive commercial and unclassified data. In this same key used for encryption and decryption process.

DES algorithm consists of the following steps

i. Encryption

1. DES accepts an input of 64-bit long plaintext and 56-bitkey (8 bits of parity) and produce output of 64 bit block.

2. The plaintext block has to shift the bits around.

3. The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.

4. The plaintext and key will processed by following

i. The key is split into two 28 halves

ii. Each half of the key is shifted (rotated) by one or two bits, depending on the round.

iii. The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed keys used to encrypt this round's plaintext block.

iv. The rotated key halves from step 2 are used in next round.

v. The data block is split into two 32-bit halves.

vi. One half is subject to an expansion permutation to increase its size to 48 bits.

vii. Output of step 6 is exclusive-OR'ed with the 48- itcompressed key from step 3.

viii. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.

ix. Output of step 8 is subject to a P-box to permute the bits. M © 2013 Global Journals Inc. (US) Global Journal of Computer Science and Technology Volume XIII Issue XV Version I 15 ( ) Year 013 2 E

x. The output from the P-box is exclusive-OR'ed with other half of the data block. k. The two data halves are swapped and become the next round's input

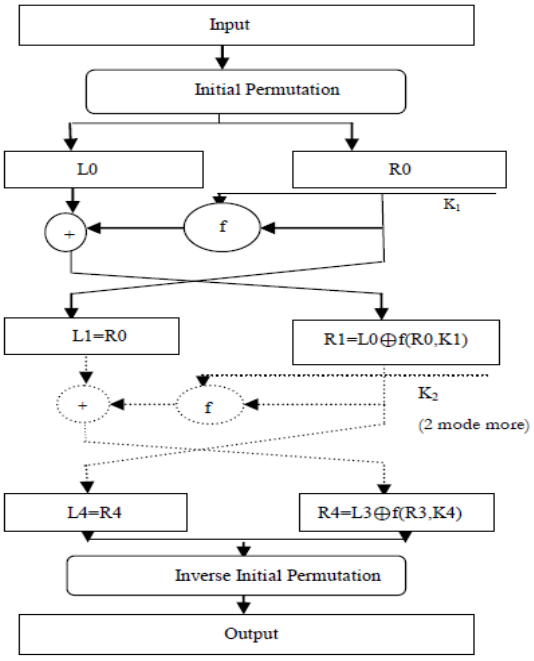

Fig.1

While sharing information in network attackers tries to trace out the traffic pattern and tries to find out the data without senders and receiver knowledge.to avoid these kind of activities the users can use DES(data encryption standard) can be used. DES is mainly used for encryption and decryption.DES accepts 64-bits plain text and 64 bit key.it uses the block cipher method, it consists of 16 rounds to encrypt the plain text, it uses feistel structure for round computing. Apply fesistelstructure to initial permutation (IP)

Fesistel structure:

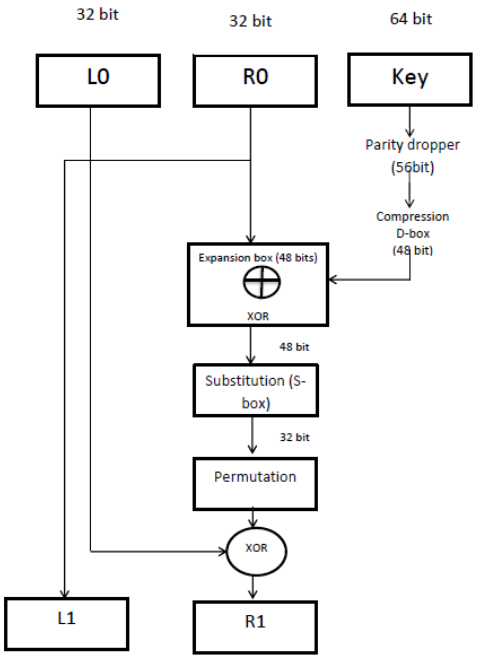

Fig.2

The plain text will be divided into 32 bits each denoted as L0and R_0. 64 bit key is applied after the parity dropper. The key will become 56 bits (eliminating the octet's bits).Again 56 bits key will be compressed using compression D-box technique then the key will become 48 bit. Beforecompressing left shift process will take place.

Now we got 48 bits of key but the data is 32 bit so we need to expand the data from 32 bit to 48 bit for that we are using expansion box.

The 32 bit is divided into 8 groups which consist of 4 bits each. Each 4 bits is expanded into 6 bits like 32 bit of the data become 1st bit of the 1st group and 1st bit of the 1st group become 2nd bit and 3rd becomes 4th, 4th becomes 5th, 2nd group 1st bit become 6th bit of the 1st expanded group, this process will continue until we get48 bits.

Now data as well as key became 48 bits, now we can do the XOR operation. In this data will be sent into the substitution box (S-box), in DES we have 8 S-boxes input will be 6 bits each output will be 4 bits. Now we got 32 bit data, this will be assigned to R1. Then R0 will be assigned to L1.

AES (advanced encryption standard)

AES is a block cipher used to replace the DES for commercial applications. It uses 128-bit block size of data and key size of 128,192 or 256 bits. It is not following fesistel structure; instead of that each round consist of four separate stages namely

1. Byte substitution 2. Row shift 3. Column mixing 4. Round key addition

The number of rounds depends on the key length, so for 128 bit key 10 rounds 12 and 14 for 192 and 256 bits key respectively.

Characteristics of AES

1. It will resist against all known attacks
2. The speed and compactness of code is useful in wide range of platforms
3. Simplicity of design method

Description about the AES structure

1. AES is not following feistel structure
2. The key provided as a input is expanded into an array of 44, 32 bit words W (i).
3. Four different stages are used among that 1 is permutation and other is substation.
4. For both encryption and decryption, the cipher text begins with an add round key stage followed by nine rounds each consists of four rounds except tenth round it consists three stages.
5. Only add round key stage make use of key

The input is a single 128 bit block both forencryption and decryption and it is known as the ***in matrix*.**

This block is copied into a ***State Array***which is modified at each stage of the algorithm and then copied to an ***O/P Matrix***.
Plain text and key are illustrated as a 128 bit square matrix of bytes.
Key is expanded into an array of key schedule words (W matrix).
The ordering of bytes within the *in matrix*is by column this applies to the W matrix also.
Four stages in encryption side is 1.substitute bytes 2.shift rows 3.mix column 4.addround key.
For 128 bit key 10 rounds, in tenth round of encryption the mix columns stage will be leave out simply. The first nine rounds of decryption also follow the same nine rounds except the mix columns.
The decryption follows the inverse rounds of the encryption namely 1.inverse shift rows 2.inverse substitute bytes 3.inverse add round keys4.inverse mix columns.

Inner workings of rounds

Add round key

The 128 bits of state are bitwise XORed with the 128 bits of the round key.
This can be viewed as a column wise operation between the 4 bytes of a state column and one word of the round key. This is very easy but affects every bit of state.

Substitute bytes

This stage is simply a table look up using a 16*16 matrix of byte values called an s-box. This matrix consists of all the possible combination of an 8 bit sequence (2^8=16*16=256).This is not a just a random permutation, well defined method is to create s-box tables.

Shift Row Transformation

This is simple permutation and nothing else
1. The first row of state is not shifted.
2. The 2nd row is shifted 1 [bytes to the left in a circular manner.
3. The 3rd row is shifted 2 bytes to the left in a circular manner.
4. The fourth row is shifted 3 bytes to the left in a circular manner.

Mix Column Transformation

The mix columns theory is calculated using the formula

$$\begin{bmatrix} r0 \\ r1 \\ r2 \\ r3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \\ 1 & 1 & 2 \\ 3 & 1 & 1 \end{bmatrix} \begin{bmatrix} a0 \\ a1 \\ a2 \\ a3 \end{bmatrix}$$

Conclusion

Compared to DES, AES is more secured, because different lengths of keys are used and it is not using feistel structure.in DES the S-box are just a random permutation of these values but in case of AES there is a well-defined method for creating S-box tables .in DES the rounds are constants but in the AES depends on the key the rounds will be different.in AES the key length is high so the attackers are not able to try the possibilities of key i.e. brute force.

References

[1]Zhijie Liu XiaoyaoXie, Member,IEEE, School of Mathematics andComputer Science and Zhen Wang, Key Laboratory of Information Computing Science of GuizhouProvince, Guizhou Normal UniversityGuiyang, China, The Research of Network Security Technologies.

[2]The Research of Firewall Technology in Computer Network Security, 2009 Second Asia-Pacific Conference on Computational Intelligence and Industrial Applications by Xin Vue, Wei Chen, Yantao Wang, College of Computer and Information Engineering Heilongjiang Institute of Science and TechnologyHarbin, China.

[3]ShyamNandan Kumar, "Technique for Security of Multimedia using NeuralNetwork,"

Paper id-IJRETM-2014-02-05-020, IJRETM, Vol: 02, Issue: 05, pp.1-7. Sep-2014

[4] Daemen, J., and Rijmen, V. "Rijndael: AES-The Advanced EncryptionStandard, Springer, Heidelberg, and March 2001.

[5]RituPahal, VikasKumar,"Efficient implementation of AES", International Journal of advanced research in computer science and software engineering, volume3, issue 7, july2013.

[6]N.Lalitha,P.Manimegalai,V.P.Muthukumar, M. Santha,"Efficient data hiding by using AES and advance Hill cipher algorithm ", International journal of research in computer applications and Robotics, volume 2, issue 1 ,January2014.