A Review Paper: Network Security and Privacy Using Encryption Techniques

Vishwambhree C. Konde[1], Harshada Warade[2], Sumeet P. Karande[3], Vaibhav V. Hanegavakar[4]
[1, 2, 3, 4] Department of Computer Science
[1, 2, 3, 4] G.S.Moze College of engineering, Pune (India)

Abstract-*In last few years, the use of Internet is increasing day-by-day. Data Security is the main issue of secure data transmission over the network. User is more concern about their Data Security. To transmit and keep data safe over the internet Security Techniques are important. In this Paper, we will discuss various Security Techniques that will provide secure data transmission over a network. Security techniques like Cryptographic Techniques- AES, SHA, RSA etc.. We will be comparing all these techniques, Advantages and their drawbacks in this paper.*

Keywords-Cryptography, Encryption Algorithm, Encryption Techniques.

I. INTRODUCTION

Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Network security includes in, enterprises, organizations, business oriented works and other any types of institutions. Network Security contain 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. Any User can choose or are assigned an Identity Number and password or other authenticating information that allows them to access an information and programs within their authority provided to them.

Cryptography can be termed as Data Hiding. Cryptography encrypted the data like text, image, audio and video unreadable during transmission and reception. The main goal is to keep our data safe from any illegal action like hacking, unauthorized access etc. It is deal with mathematics which is used to encrypt and decrypt data. It enables to exchange data between two parties more securely. It store sensitive information or transmit the information across insecure networks so that it cannot be readable by any person except authorized person. The personal data, images, text, videos, Computer passwords this kind of data can be transmit or send from one place to another are done with cryptography.

II.LITERATURE SURVEY

Cryptography is a process which is associated with scrambling plaintext into cipher text it is also called as Encryption then back again into Plaintext (known as decryption).

There are various techniques to classify the algorithms.

The most common types are :

i) Secret Key Cryptography which is also called as Symmetric Key Cryptography
ii) Public Key Cryptography which is also called as Asymmetric Key Cryptography.

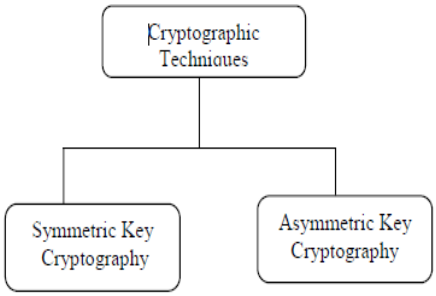

Fig 2.1 Cryptographic Techniques

2.1 Secret key cryptography:

A single key is used for both encryption and decryption, in Symmetric key cryptography. The Figure 1 shows, the sender uses the key (or some set of rules) to convert the plaintext into encrypted form and sends the converted encrypted form which is known as ciphertext to the receiver. The receiver applies the same key which is used for encrypt the plaintext to decrypt the message and again convert to the plaintext. A single key is used for both functions therefore; it is also called secret key cryptography. In the symmetric or secret key cryptography, the one must make sure that the key must be known to both the sender and the receiver; that, in fact, is the secret. The main issue with this technique, of course, is the distribution of the key.

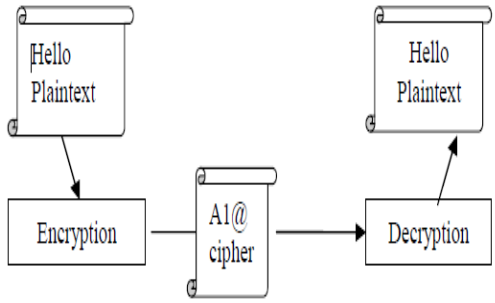

Fig 2.2 Secret key cryptography

2.2 Public key cryptography or asymmetric key cryptography:

The Asymmetric Key Cryptography uses key pairs: one private key and one public key. Both keys are required to encrypt and decrypt a message or transmission. The private key, not to be confused with the key utilized in private key cryptography, is just that, private. It is not to be shared with anyone. The owner of the key must be make sure that the key should not be known to anyone. Key must be secure in such a manner that it will not be lost or compromised, and cannot be accessed by anyone except sender . On the other hand, the public key is just that, public. Public key can be distributed. The asymmetric cryptography intends for public keys to be accessible to all users. In fact, this makes the system more strong. When a person has access to public key easily, usually via some form of directory service, then the two parties have less effort to communicate with each other communicate securely. That is without a prior key distribution arrangement.

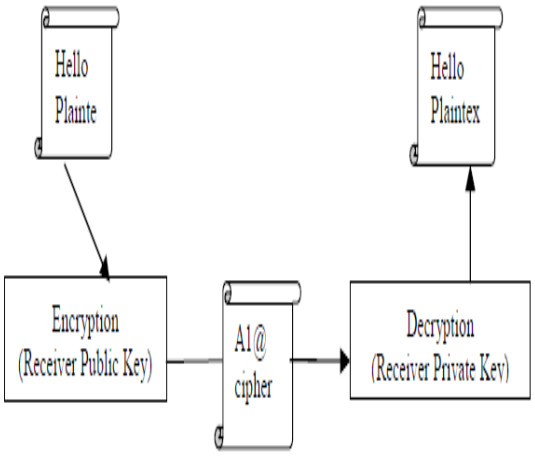

Fig 2.3 Public key cryptography

III. GOALS OF CRYPTOGRAPHY

A] Authentication

The process of identity proving is authentication. Authentication verifies the message's source. Authentication has two types:

(i) Peer entity authentication, and

(ii) Data origin authentication.

B] Confidentiality

It provides the security of transmitted data from passive attacks. It provide protection against unauthorized discovery of information. It may be applied to whole messages, parts of messages, and even existence of messages.

C] Data integrity:

To ensure data is protected from accidental or deliberate (malicious) modification. Integrity is usually provided by message authentication code or hashes. A hash value is a fixed length numeric value derived from a sequence of data. Hash values are used to verify the integrity of data sent through insecure channels. The hash value of received data is compared to the hash value of the data as it was sent to determine if the data was altered.

D] Non-repudiation

Non-repudiation is a term that source and destination of information cannot disavow that they have sent or received information. This is useful at that time when we try to search about the malicious nodes which are always tries to interrupt the network operations between various authorized nodes.

IV. CRYPTOGRAPHY ALGORITHM

A] Data Encryption Standard (DES):

- DES is a cipher that operates on 64-bit blocks of data, using a 56-bit key.
- It is a 'private key' system.
- DES algorithm applied on block of data rather than one bit at a time.
- It uses 16 round Feistel structure.

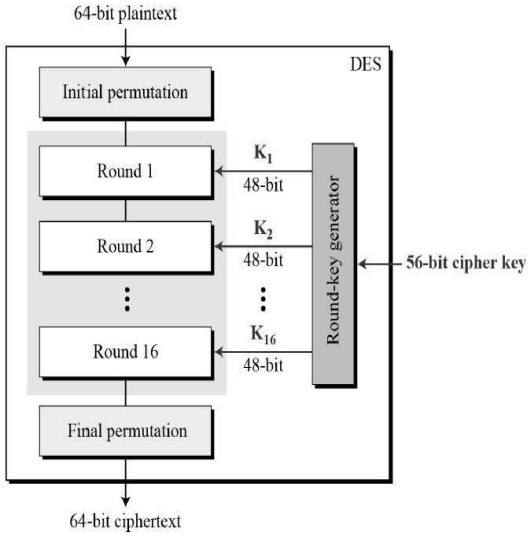

Fig 4.1: DES Structure

B] Rivest, Shamir, and Adleman(RSA):

- RSA is a public-key system.
- RSA is widely used in encrypted connection, digital certificates core algorithms.
- RSA is based on arithmetic modulo large numbers, it can be slow in constraining environments[9]
- RSA decrypts the cipher text and generates the signatures,
- Therefore, more computation capacity and time will be required
- Reducing modules technique speed up the RSA decryption.
- Following steps are followed in RSA to generate the public and private keys [7]:

Step 1: Choose large prime numbers p and q such that p not equal to q.
Step 2: Compute n=p*q
Step 3: Compute φ (pq) = (p-1)*(q-1)
Step 4: Choose the public key e such that gcd (φ (n), e) =1; 1<e< φ (n)
Step 5: Select the private key d such that d*e mod φ (n) =1

- In RSA algorithm encryption and decryption are performed as follows:

1] Encryption:
Calculate cipher text C from plaintext message M such that,

C=M ^e mod n
2] Decryption:
M=C^d mod n=M^ed mod n

C]Advanced Encryption Standard:

- AES is a block oriented symmetric key encryption algorithm.
- It is more secure than Data Encryption Standard (DES) algorithm.
- It operates on a 128 bit data block at a time and uses 128, 192 or 256 bits key length and uses 10, 12 0r 14 rounds.
- A data block is partitioned into an array of bytes.
- The input is divided into 16 bytes and then arranged into a 4x4 matrix column wise [8]. This matrix is known as the state matrix.
- The original 128-bit key is also divided in to 16 bytes as like 128 bit data and arranged in the form of 4x4 matrixes. This matrix is called keyMatrix.

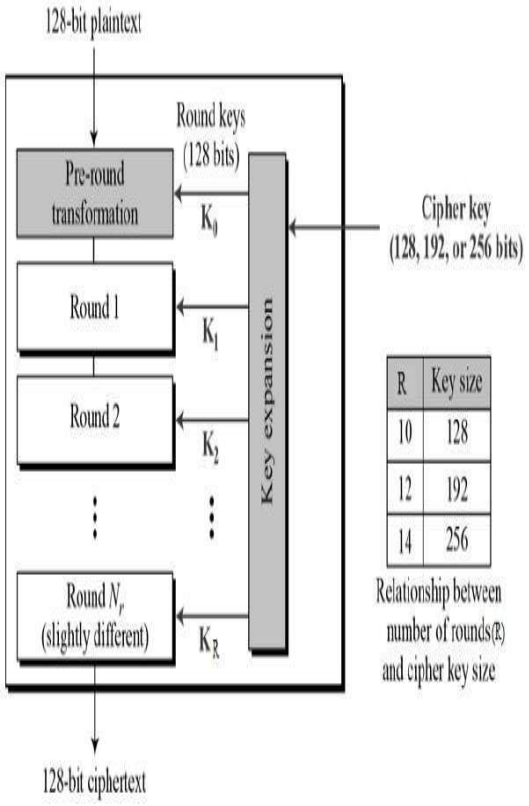

Fig4.2: AES Structure

D] Secure Hashing Algorithm(SHA):

- SHA-1 is a hashing algorithm similar in structure to MD5, but producing a digest of 160 bits.
- Because of the large digest size, it is less likely that two different messages will have the same SHA-1 message digest.
- For this reason SHA-1 is recommended in preference to MD5.

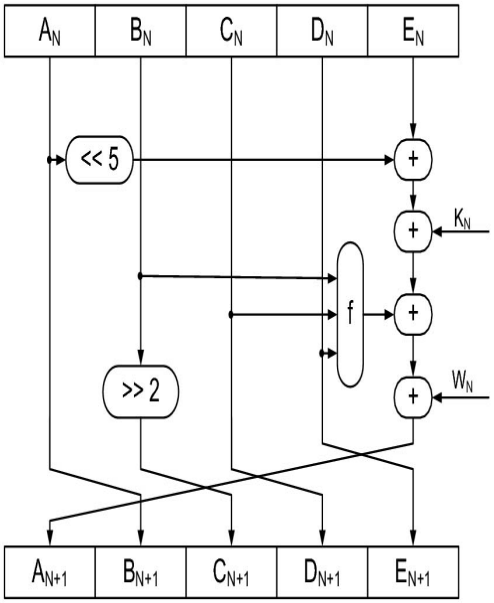

Fig4.3: SHA-1 Structure

V. COMPARISON BETWEEN ALGORITHMS

1] DES Verses AES :-

Parameters	DES	AES
Developed	1976	1999
Block Size	64	128
Key Length	56	128,192,256
Number of Rounds	16	9,11,13
Encryption Primitives	Substitution, permutation	Substitution, shift, bit mixing
Design	Open	Open
Selection Process	Secret	Secret, but accept open public comment
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion
source	IBM, enhanced by NSA	Independent Cryptographers

2] AES Verses RSA

Parameters	AES	RSA
Key Length	128,192 or 256 bits	1024 bits
Block Size	128,192 or 256 bits	128 bits
Cipher Text	Symmetric Block Cipher	Asymmetric Block Cipher
Developed	2000	1978
Better	In terms of cost And security.	In terms of speed and security
Possible Keys	2^{128},2^{192} and 2^{256}	2^{128}

VI. CONCLUSION

We successfully study the topic on A Review Paper: Network Security and Privacy Using Encryption Techniques. This assignment would not have been completed without the efforts and cooperation from our group members. We also sincerely thank our HOD for the proper guidance, encouragement and support.

REFERENCES

[1] Coron, J. S. , " What is cryptography?", IEEE Security & Privacy Journal, 12(8), 2006, p. 70-73.

[2] DIFFIE, W., and HELLMAN, M.: 'New directions in cryptography', IEEE Trans., 1976, IT-22, pp. 644-654

[3] SIMMONS, G.J.: 'Symmetric and asymmetric encryption', ACM Comput. Surveys, 1979, 11, pp. 305-330

[4] RIVEST, R.L., SHAMIR, A., and ADLEMAN, L: 'A method for obtaining digital signatures and public-key cryptosystems', CACM, 1978, 21, pp. 120-126

[5] S. William, Cryptography and Network Security: Principles and

[6] Ritu Tripathi, Sanjay Agrawal Comparative Study of Symmetric and Asymmetric Cryptography Techniques International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348 – 4853.

[7] Aman Kumar, Dr. Sudesh Jakhar, Mr. Sunil Makkar Comparative Analysis between DES and RSA Algorithm's International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 ISSN: 2277 128X.

[8] T. Saravanan, V. Srinivasan, R, Udayakumar "MATLAB-Simulink Implementation of AES Algorithm for Image Transfer" Middle-East Journal of Scientific Research 18(12) 1709-1712, 2013

[9] AnnapoornaShetty, Shravya Shetty K, Krithika K A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 5, October 2014ISSN(Online): 2320-9801 ISSN (Print): 2320-9798

[10] Algorithms: http://www.cryptographyworld.com/algo.htm