RESEARCH ARTICLE OPEN ACCESS

A Review Paper on Cryptography-Science of Secure Communication

T.Saravanan [1], Dr.S.Venkatesh Kumar [2]
Department of Computer Application (PG)
Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore
Tamil Nadu -India

ABSTRACT
Cryptography is the technique of using mathematical algorithms to encryption and decryption the information. Store data or transfer it across unconfident networks [like the Internet] so that it cannot be view by anyone except the intended recipient. While cryptography is the science of protecting data, crypt analysis is the science of analyzing and breaking secure conversation. A cryptographic method, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in composite with a key — a word, number, or phrase to encrypt the plaintext.
Keywords:- cryptographic, encryption and decryption, information security, Symmetric Key, Asymmetric Key

I. INTRODUCTION

Society across the world generate a huge amount of data daily. Information security is the most difficult task in the internet and network. Computer and network security is a new and quickly moving technology and Security of data can be done by a art called cryptography. Nowadays information security system includes confidentiality, authenticity, integrity, non repudiation. It translate data of a given format is plaintext to another format is cipher text, using an encryption key. The operation of reversing cipher text to its original plain text is called decryption algorithm. Purpose of cryptography include ATM cards, computer passwords, and army, medical field[7].

The cryptography is still in its developing stages and a reasonable research effort is still needed for secured communication. This paper talks about the state of the art for a deep area of cryptographic method that are used in networking applications.

II. ARCHITECTURE DIAGRAM

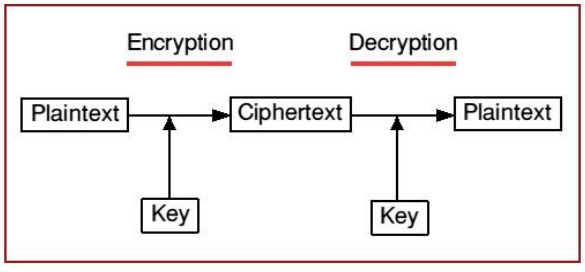

Fig.1 Architecture diagram

CHARACTERISTICS

FOLLOWING CHARACTERISTICS ARE,

- Reliability
- Data security
- Data Productivity
- Data Confidentiality
- Data Integrity
- Data breaches
- Authentication and Authorization
- Non-repudiation

III. METHODOLOGY

A. BASIC TERMINOLOGY OF CRYPTOGRAPHY

Cryptography is the conversion of simple and readable data into a form that cannot be in order to secure data. The word cryptography comes from the Greek word "Kryptos", that means unknown and invisible, and "graphikos" which means writing.

Cryptography is a method for putting away and transmitting data in a exact frame so that it is expected can read and process it. The term is usually connected with clamber plaintext information (customary content, in some cases intimate to as cleartext) into ciphertext (a method called encryption), then back once more (known as decoding).

The data that need to hide, is called original text, It could be in a form of characters, numerical data, executable programs, pictures, or any other kind of data, The data that will be translated is called cipher text , it's a term refers to the string of "worthless" data, or meaningless text that nobody must find out, except the

recipients. It is the data that will be transmitted specifically through network, Many algorithms are used to convert plaintext into cipher text.

B. DATA ENCRYPTION

A data encryption is a random string of bits created specially for clamber and clarify data. Data encryption is designed with algorithms intended to ensure that every key is different and unstable.

Cryptography uses two types of keys symmetric and asymmetric. Symmetric keys have been around the highest they handle a single key for both the encryption and decryption of the cipher text. This type of key is called a secret key. Secret-key ciphers mostly fall into one of two categories: stream ciphers or block ciphers. A block cipher applies a private key and algorithm to a block of data synchronously, where as a stream cipher applies the key and algorithm single bit at a time. Almost cryptographic processes use symmetric key encryption to encrypt data transmissions but use asymmetric key encryption to encrypt and interchange the secret key. Symmetric encryption, also known as private key encryption, uses the same private key for both encryption and decryption.

C. DATA DECRYPTION

The appliance for encryption-decryption system is hiding. As data crossing over the network, it becomes subject to access from unapproved or organizations. Decryption is the process encrypted data or other information convert into text that you or the computer can read and see the data.

Encryption is the operation of convert plain text into something that appears to be empty (ciphertext). Decryption is the process of transform cipher text back to plaintext.

D. SYMMETRIC KEY CRYPTOGRAPHY

In symmetric key cryptography is likewise private-key cryptography, a secret key may be held by one person or interchange between the sender and the receiver of a message. If private key cryptography is used to send secret key between the sender and receiver. If there should be an occurrence of Symmetric Encryption, same cryptography keys are utilized for encryption of plaintext and reduce of figure content. Symmetric key encryption is swift and less difficult yet their principle problem is that both the clients need to move their keys security.

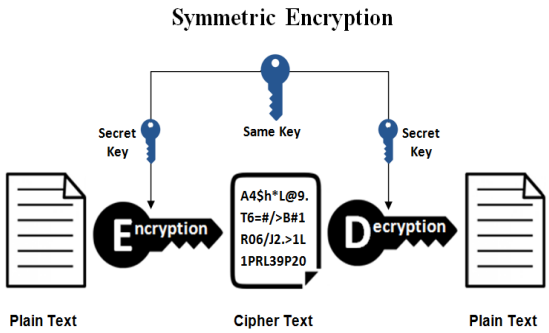

Fig.2 Symmetric Encryption

E. ASYMMETRIC KEY CRYPTOGRAPHY

In the two-key structure is also known as the public key system, one key encrypts the information and another, mathematically suitable key decrypts it. The computer sending an encrypted message uses a selected private key that is never shared and so is known only to the vendor. If a sending computer first encrypts the data with the proposed receiver's public key and again with the sender's private key, then the inheriting computer may decrypt the data, first using its secret key and then the sender's public key. Using this public-key cryptographic algorithm, the sender and receiver are intelligent to validate one another as well as secure the confidentiality of the data. Asymmetric encryption uses two keys and also known as Public Key Cryptography, because sender uses two keys: public key, which is known to public and a private key which is only known to sender.

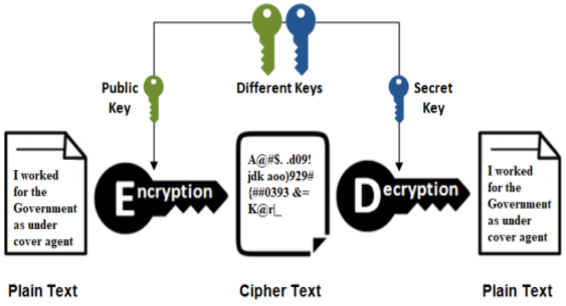

Fig.3 Asymmetric key cryptography

F. DATA ENCRYPTION STANDARD (DES)

DES is a block-cipher handle a 56-bit key that produce on 64-bit blocks. DES algorithm as characterize by Davis R. takes a fixed-limit string of plaintext bits and transfer it through a series of difficult operations into cipher text bit string of the same length. 3DES is an improvement of DES; it is 64 bit block size with 192 bits key size. In this general the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the moderate secure generation.

G. ADVANCED ENCRYPTION STANDARD (AES)

AES is a block cipher intended to replace DES for profitable function. It uses a 128-bit block size and a key size of 128, 192, or 256 bits. The number of constitutional rounds of the cipher is a function of the key length. The number of rounds for 128- bit key is 10[3].

H. PUBLIC-KEY CRYPTOGRAPHY

Public-key cryptography is a form of cryptosystem in which encryption and decryption are implement the different keys—one a public key and one a private key. These keys are mathematically associated although ability of one key does not allow someone to simply determine the other key. As shown in Figure ,the sender A uses the public key of receiver B (or some set of rules) to encrypt the plaintext message M and sends the cipher text C to the receiver. The receiver applies own private key to decrypt the cipher text C and recover the plaintext message M. Because pair of keys is needed, this access is also called asymmetric cryptography.

IV. CRYPTOGRAPHY – BENEFITS

Cryptography is an crucial data security mechanism. It provides the four most basic duty of information security −

- **Confidentiality** – confidentiality is a set of rules or a promise that limits access or places restrictions on certain types of information.
- **Authentication** – authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server.
- In asymmetric or public key, cryptography there is no need for exchanging keys, thus eliminating the key distribution problem.
- **Data Integrity** –data integrity is the assurance that digital information is uncorrupted and can only be accessed or modified by those authorized to do so integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle.
- A symmetric cryptosystem is faster.
- **Non-repudiation** – non-repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

V. CRYPTOGRAPHY – DRAWBACKS

- A strongly encrypted, authentic, and digitally signed information can be **challenging to access even for a proper users** at a crucial time of decision-making. The organization or the computer can be attacked and effected non-functional by an criminal.
- **High availability,** one of the major aspects of information security, cannot be ensured through the use of cryptography. Other approach are needed to guard against the risk such as denial of service or complete breakdown of information system.
- It depends on the secret key if you forget the keys you cannot recover data.
- It is always vulnerable to brute force attack.
- Symmetric cryptosystems have a problem of key transportation. The secret key is to be transmitted to the receiving system before the actual message is to be transmitted. Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only secure way of exchanging keys would be exchanging them personally.
- Cryptography comes at cost. The cost is in terms of time and money −
    - Addition of cryptographic techniques in the information processing leads to delay.
    - The use of public key cryptography requires setting up and maintenance of public key infrastructure requiring the handsome financial budget.
- The security of cryptographic technique is based on the computational difficulty of mathematical problems. Any breakthrough in solving such mathematical problems or increasing the computing power can render a cryptographic technique vulnerable.

VI. CONCLUSION

In this paper various cryptographic techniques are discussed to increase the security of network. Network security consist of the provisions and protect the network and the network-accessible resources from unauthorized access. Network Security is the most vital component in information security because it is

responsible for securing all information passed through networked computers.

The security of communication is a crucial issue on World Wide Web. Cryptography is used for Network security purpose. The secure exchange of key between sender and receiver is an important task. Network security covers the use of cryptographic algorithm in network protocols and network applications. The security for the data has become highly important.

REFERENCES

[1] Sarita Kumari, "A research Paper on Cryptography Encryption and Decryption" International Journal Of Engineering And Computer Science, 2017.

[2] https://en.wikipedia.org/wiki/Cryptography

[3] Jangala. Sasi Kiran M.Anusha, A.Vijaykumar, M.Kavya "Cryptography: The Science of Secure Communication" International Journal of Computer Science and Network Security(IJCSNS) 2016.

[4] Dr.Sandeep Tayal, Dr.Nipin Gupta, Dr.Pankaj Gupta, Deepak Goyal, Monika Goyal, "A Review paper on Network Security and Cryptography" Advances in Computational Sciences and Technology ISSN, 2017.

[5] IEEE Standard P1363.1, "IEEE standard specification for public key cryptographic techniques based on hard problems over lattices", 2009.

[6] M.-L. Akkar and C. Giraud. "An implementation of DES and AES, secure against some attacks" In Cryptographic Hardware and Embedded Systems (CHES 2001). Lecture Notes in Computer Science, Vol. 2162, pp. 309-318. Springer, 2001.

[7] Sandeep Kaur, Raghbir Kaur, C.K.Raina," Review on Network Security and Cryptography" International Journal of Scientific Research in Computer Science Engineering and Information Technology, 2017.

[8] Nikita Chaudhari, Priya Parate," Secure Online Payment System using Visual Cryptography," International Journal of Advanced Research in Computer and Communication Engineering, 2016.

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

[10] Cryptocoding.net, "Cryptographic Coding Standards" https://cryptocoding.net/index.php/Cryptography_Coding_Standard, 2013.