# A Study on Network Security and Cryptography

Ms.S.Anitha
Assistant Professor
Department of Computer Applications
Tamil Nadu, India

Ms.R.Padmalatha
Assistant Professor
Department of Computer Applications
Tamil Nadu, India

## ABSTRACT

Network Security is a concept of securing data through wireless transmission with the help is used to ensure the contents of a message which are confidentiality means of cryptography. Data Security is the main aspects 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 is used in various computer network sectors such as private and public. Networks used in the organizations, enterprises, institutions, etc..are in the form of private and public. The task of network security is not only ensuring the security of end systems but also to the entire network. Network Security is used in various applications like Government agencies, Organization, Enterprises, Bank, Business etc. Cryptography nobody can understand the received message expect the one who has the decipher key, this is done when the sender includes a cryptographic operation called hash function on the original message. A hash function is a mathematical representation of the information, when any information arrives to receiver, the receiver calculates the value of this hash function. Security of data is done by a technique called cryptography. So one can say that Cryptography is an emerging technology, which is important for network security. In olden day's cryptography was used to keep the military information, diplomatic correspondence secure and in protecting the national security but the usage was limited. Now-a-days, the range of cryptography applications have been expanded a lot in this modern area after the development of communication. Cryptography is essentially required to ensure that data's are protected against penetrations and to prevent and it is also a powerful meansin securing e-commerce.

# INTRODUCTION

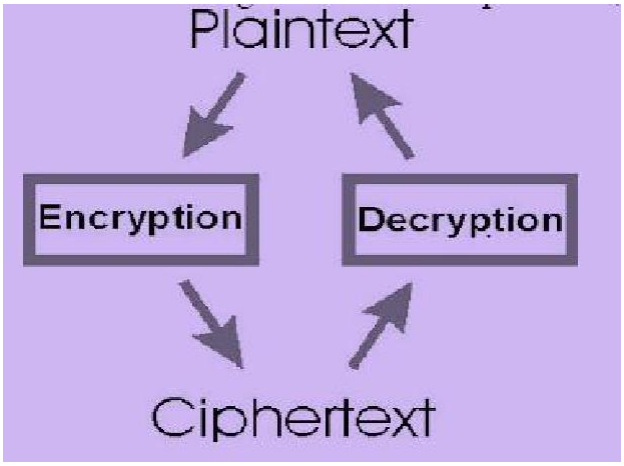
Network Security protects our network and data from breaches, intrusions and other threats. This is a vast and overarching term that describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility and overall threat protection. Network Security involves access control, virus and antivirus software, application security, network analytics, types of network-related security [endpoint, web, wireless], firewalls, VPN encryption and many more. Network Security is the most vital component in information security because it is responsible for securing all the information passed through networked computer. Network Security refers to hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, administrative and management policy required to provide an acceptable level of protection for hardware and software in a network. Internet has become more widespread, if an unauthorized person is able to get access to this network, he can not only spy on us but he can easily mess upour lives. Network Security and Cryptography is a concept of protecting the network and data transmission over a wireless network. A Network Security system typically relies on layers of production and consists of multiple components including networking, monitoring and security software in addition to hardware's and appliances. All components work together to increase the overall security of the computer network. Security of data can be done by a technique called Cryptography.

Cryptography is the science of writing in secret code. Modern Cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Anapplication of cryptography includes ATM cards, computer password, and electronic commerce. The development of the World Wide Web resulted in broad use of cryptography for e-commerce and business applications. Cryptography is closely related to disciplines of cryptology and cryptanalysis. Techniques used for decrypting a message without any knowledge of the encryption details fail into the area of cryptanalysis. Cryptanalysis is what the layperson calls "breaking the code". The areas of cryptography and cryptanalysis together are called cryptology. Cryptography means "Hidden Secrets" is concerned with encryption.

**Encryption** is the process of converting ordinary information (called plaintext) into unintelligible text (called cipher text).

**Decryption** is the reverse process of encryption, moving from the unintelligible cipher text back to plaintext.

**Cryptosystem** is the ordered list of elements of finite possible plaintext, cipher text, keys and the encryption and decryption algorithms which correspond to each key.




The various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography.

The testing issue is the way to successfully share scrambled information. Encode message with unequivocally secure key which is known just by sending and beneficiary end is a note worthy perspective to get strong security in sensor organize. The safe trade of key amongst sender and recipient is a lot of trouble some errand in as set imperative sensor arrange. information ought to be scrambled first by clients before it is outsourced to a remote distributed storage benefit and both information security and information get to security ought to be ensured to such an extent that distributed storage specialist organizations have no capacities to unscramble the information, and when the client needs to pursuit a few sections of the entire information, the distributed storage framework will give the availability without recognizing what the segment of the encoded information came back to the client is about.

## METHODOLOGY:

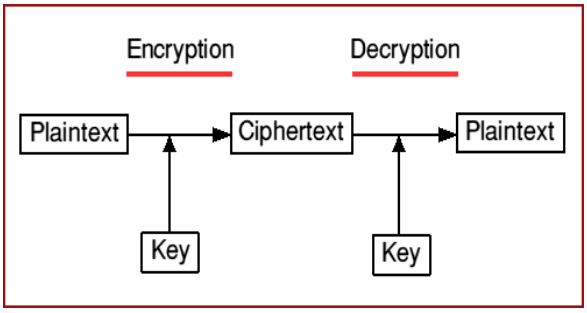
Internet security is a tree branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing. Different methods have been used to protect the transfer of data, including encryption.

Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.

## CRYPTOGRAPHIC PRINCIPLES

A. **Redundancy:** All the encrypted message contain some redundancy, there is no need of understanding the message by information.

B. **Freshness:** Time stamp is used in every message. For instance the time stamp is of 10sec for every message. The receiver keeps the message around 10sec to receive the message and filter the output within that10sec.The message exceeds the time stamp it is throw out.




## CRYPTOGRAPHY GOALS

By using cryptography many goals can be achieved, These goals can be either all achieved at the same time in one application, or only one of them, These goals are:

a) **Confidentiality:** It is the most important goal, that ensures that nobody can understand the received message except the one who has the decipher key.

b) **Authentication:** It is the process of proving the identity, that assures the communicating entity is the one that it claimed to be, This means that the user or the system can prove their own identities toot her parties who don't have personal knowledge of their identities

c) **Data Integrity:** Its ensures that the received message has not been altered in any way from its original form, This can be achieved by using hashing at both sides the sender and the recipient in order to create a unique message digest and compare it with the one that received.

d) **Non-Repudiation:** It is mechanism used to prove that the sender really sent this message, and the message was received by the specified party, so the recipient cannot claim that the message was not sent.

e) **Access Control:** It is the process of preventing an unauthorized use of resources. This goal controls who can have access to the resources, If one can access, under which restrictions and conditions the access can be occurred, and what is the permission level of a given access.

## CRYPTOSYSTEM TYPES

### 1. Asymmetric cryptosystems

It uses two different keys to send and receive the messages. It use public key for encryption and another key is used ford encryption. Two user A and B needs to communicate, A use public key of B's to encrypt the message. B use private key to decipher the text. It is also called as public key cryptosystems. Diffie-Hellman key exchange generate both public and private key.

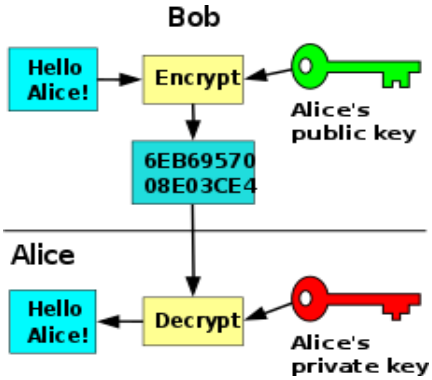



**Fig. Asymmetric cryptosystems**

### 2. Symmetric cryptosystems

In Symmetric cryptosystems both the enciphering and deciphering keys are identical or sometimes bother related to each other. Both the key should be kept more secure otherwise in future secure communication will not be possible. Keys should be more secure and it should be exchanged in a secure channel between two users. Data Encryption Standard(DES) is example of Symmetric cryptosystems.

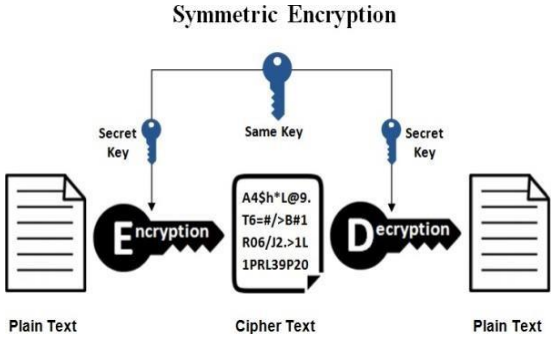
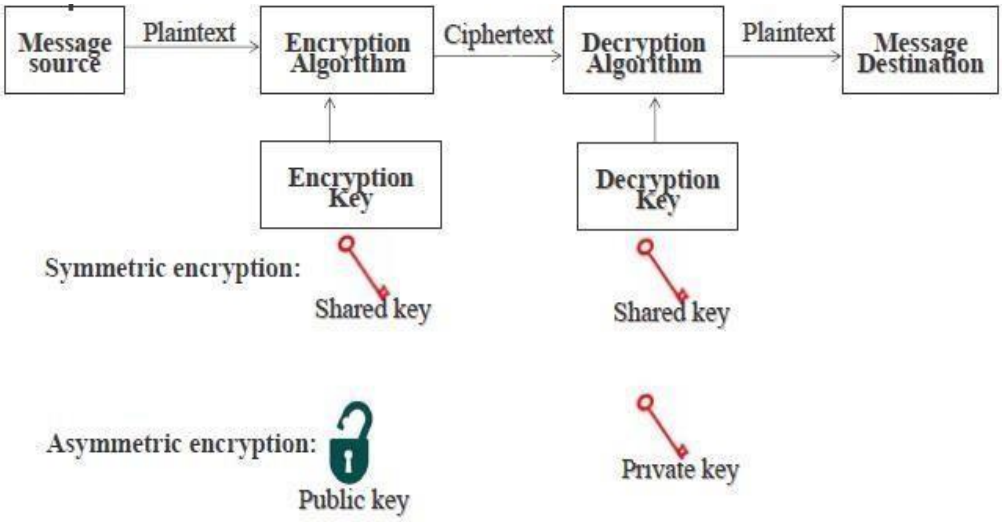



**Fig. Symmetric cryptosystems**

# CRYPTOGRAPHIC MODEL & ALGORITHM

## A. Encryption model

There are two encryption models namely they are as follows: Symmetric encryption and Asymmetric encryption. In Symmetric encryption, Encryption key=Decryption key. In Asymmetric encryption, Encryption key Decryption key.




## B. Algorithm

There are of course a wide range of cryptographic algorithms in use. The following are amongst the most well-known:

1) **DES:** This is the 'Data Encryption Standard'. This is a cipher at operates on 64-bit blocks of data, using a 56-bit key. It is a 'private key' system.
2) **RSA:** RSA is a public-key system designed by Rivest, Shamir, and Adleman.
3) **HASH:**A 'hash algorithm' is used for computing a condensed representation of a fixed length message/file. This is sometimes known as a 'message digest', or a 'fingerprint'.
4) **MD5:**MD5isa128 bit message digest function. It was developed by Ron Rivest.
5) **AES***:* This is the Advanced Encryption Standard(using the Rijndael block cipher) approved by NIST.
6) **SHA-1***:*SHA-1 is a hashing algorithm similar in structure to MD5, but producing a digest of 160bits(20bytes).Because of the large digest size, it is less likely that two different messages will have the same SHA-1 message digest. For this reasonSHA-1 is recommended in preference to MD5.
7) **HMAC***:* HMAC is a hashing method that uses a key in conjunction with an algorithm such asMD5 or SHA-1. Thus one can refer to HMAC-MD5 and HMAC-SHA1.

## CONCLUSION:

With the explosive growth in the Internet, network and data security have become an inevitable concern for any organization whose internal private network is connected to the Internet. The security for the data has become highly important. User's data privacy is a central question over cloud. With more mathematical tools, cryptographic schemes are getting more versatile and often involve multiple keys for a single application. The various schemes which are used in cryptography for Network security purpose. Encrypt message with strongly secure key which is known only by sending and recipient end, is a significant aspect to acquire robust security in cloud. The secure exchange of key between sender and receiver is an important task. The key management helps to maintain confidentiality of secret information from unauthorized users. It can also check the integrity of the exchanged message to verify the authenticity. Network security covers the use of cryptographic algorithms in network protocols and network applications. This paper briefly introduces the concept of computer security, focuses on the threats of computer network security. In the future, work can be done on key distribution and management as well as optimal cryptography algorithm for data security over clouds.

## REFERENCE:


1. DaveDittrich, Network monitoring/Intrusion Detection Systems (IDS),University of Washington.
2. Algorithms:http://www.cryptographyworld.com/algo.htm
3. Data_Communication_and_Networking_by_Behrouz.A.Foro uzan_4th.edition
4. Bellare,Mihir;Canetti,Ran;Krawczyk,Hugo,"HashFunctionsforMessage Authentication",1996.
5. William Stallings, "Cryptography and Network Security Principle and Practice", Fifth Edition,2011.
6. Diffie,W.,Hellman,M.E.:Newdirectionsincryptography.IEEETransactions on Information Theory 22,644–654(1976).
7. Gross, T.,M ¨odersheim, S.: Vertical protocol composition. In:24th IEEE Computer Security Foundations Workshop(CSF2011).
8. Publication197-Announcing the Advanced Encryption Standard (AES).Federal Information ProcessingStandards,26Nov.2001.
9. Ralston, Anthony, EdwinD. Reilly, and David Hemmendinger. Encyclopedia of Computer Science.Fourthed.London,England:Nature Publishing Group,2000
10. Maurer, U.: Secret key agreement by public discussion from common information. IEEE Transactions on Information Theory39(3),733–742(1993)
11. Shyam Nandan 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
12. Preneel, B. (2010, September). Cryptography for network security: failures, successes and challenges. In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security(pp.36-54).Springer, Berlin, Heidelberg.
13. Panda,M.(2014).Security in wireless sensor networks using cryptographic techniques. *American Journal of Engineering Research(AJER),3*(01),50-56.
14. Dhamdhere Shubhangi .T., & Gumaste, S. V. Security in Wireless Sensor Network Using Cryptographic Techniques.
15. Simmonds, A; Sandilands, P; van Ekert, L (2004). "*An Ontology for Network Security Attacks*". *Lecture Notes in Computer Science. Lecture Notes in Computer Science* 3285: 317-323.