Subject : Computer Network Security

Class : BCA/MCA

Semester : VI

Name of the Paper: Computer Network Security

Topic : Introduction of Network Security

Keywords : Computer Network, Network Security, Security Service, Cryptography, Type of Cryptography, Authentication.

Created by:-
Vineet Kumar Singh
Assistant Professor
Department of Computer Application (BCA)
Jagatpur Post Graduate College, Jagatpur Varanasi
E-mail ID: vineet.jpgc@gmail.com

SELF DECLARATION

“The content is exclusively meant for academic purpose and for enhancing teaching and learning. Any other use for economic/commercial purpose is strictly prohibited. The users of the content shall not distribute-disseminate are share it with any one else and its use is restricted to advancement of individual knowledge. The information provided in this e-content is authentic and best as per my knowledge”

By:-
Vineet Kumar Singh
Assistant Professor
Department of Computer Application (BCA)
Jagatpur Post Graduate College, Jagatpur Varanasi
E-mail ID: vineet.jpgc@gmail.com

Objectives

- The study of computer network security provides knowledge about the basic structure and framework of computer network security.

- The main objective of computer network security is to Confidentiality (about data and privacy), Integrity (Data and System), Availability, Authenticity and Accountability.

- How to Information communicate in the network? Why is the security required and what are the mechanism are used during the data transmission in a interconnected network.

- What is the requirements of computer network security and model of the computer network security.

Background

- Information Security requirements have changed in recent times

- Traditionally provided by physical and administrative mechanisms

- Computer use requires automated tools to protect files and other stored information

- Use of networks and communications links requires measures to protect data during transmission

Definitions:

- **Computer Network** – Computer network are the collection of two or more computers which interconnected through a network medium either wired or non-wired.

- **Computer Security** – It is the collection of tools designed to protect data, information and privacy from the unauthorised person or hackers.

- **Network Security** – Network Security means protect the data during the transmission or communication.

- **Internet Security** – Protection of data during their transmission or communication over a collection of interconnected networks or interconnected computers.

Course Outline

- Basic Security Concepts:
  - Confidentiality, integrity, availability
  - Others
- Cryptography
  - Secret Key Cryptography: DES, IDEA, AES, etc.
  - Public Key Cryptography: RSA, Diffi-Hellman, Digital Signature, Elliptic Curve, etc.
  - Hashes and Message Digests: MD5, SHA-1 etc.
- Authentication
  - Basic concepts of Authentication Systems
  - Password Authentication
  - Security handshake pitfalls

Basic Security Concepts:

- Confidentiality (Secrecy):
  - Protection of any information from being exposed to unauthorized entities. It means prevent unauthorized use or disclosure of information.
- Integrity :
  - Assurance that the information has not been tampered means prevent /detect improper modification of information.
- Availability :
  - Availability means improper denial of access to services provided by the system.
- Authentication:
  - Assurance that an entity of concern or the origin of a communication is authentic. In other words information is accessible to authorized entities at the proper time.

Cryptography:

- Basic Terminologies:

  - **Plain Text:** A massage in the original form called plaintext.
  - **Cipher Text:** A massage in the encrypted form called cipher text.
  - **Cipher:** An algorithm for transforming plain text to cipher text called cipher.
  - **Key:** Some critical information used in the cipher, known only to sender and receiver is called as key.
  - **Encryption (Encode or Encipher):** The process of converting plaintext to cipher text using a cipher is called as encryption.

Cryptography:

- Basic Terminologies: é Continue

  - **Decryption (Decode or Decipher):** The process of converting cipher text back into plaintext using a cipher is called as decryption.
  - **Cryptanalysis (Code Breaking):** The study of principal and methods of transforming cipher text back into plain text without knowledge of key.
  - **Cryptology:** The union of cryptography and cryptanalysis is called cryptology.
  - **Code:** An algorithm that converting intelligible massage into an unintelligible form using code book is called as code. E.g. ASCII Code.

Cryptography:

- Communication is one of the necessities of human beings. When the massages are transmit in the network for the desired goal, it is necessary to maintain secrecy and authorization during sending and receiving the massages. Cryptography is a technique to solve this problem.
- In other words ñ Cryptography is the art of science of keeping secrets secretò. With the help of cryptography, it is possible to communicate securely through insecure channels or networks. Basically, there are three types of cryptographic algorithms are used based on the key management system, such as:
  - Secret Key Cryptography (Conventional or Symmetric Key)
  - Public Key Cryptography
  - Hash Cryptography

Cryptography:...Continue

- Secret Key Cryptography (Conventional Key Algorithm):
  - The secret key algorithm uses a single key for both encryption and decryption. The set of all secret key algorithm is known as secret key cryptography which is sometime called symmetric key cryptographic (Fig.1.). For example, Data Encryption Standard (DES), Advance Encryption Standard (AES), International Data Encryption Algorithm (IDEA), etc.

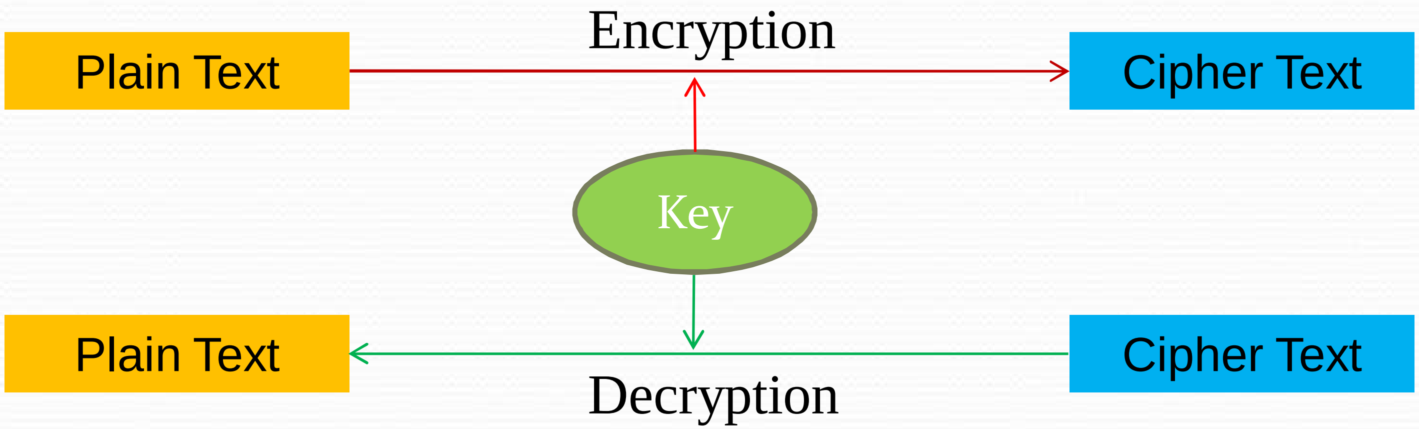

Fig.1. Encryption and decryption process using Secret Key Cryptography

Cryptography:…Continue

- Public Key Cryptography:
  - Over the drawback of symmetric key cryptography Whitefield Diffie and Martin Hellman proposed in 1976 a new cryptosystem called public key cryptography. In this cryptosystem there is no need to exchange the key over a secure channel or network between two users who wish to communicate to each other. Here, two key are used, first Public key are used for encryption and the second, private key are used for decryption process.

  - For example, Rivest-Shamir-Adleman (RSA), Diffi-Hellman, Digital Signature, Elliptic Curve Cryptography (ECC), etc.

Cryptography:…Continue

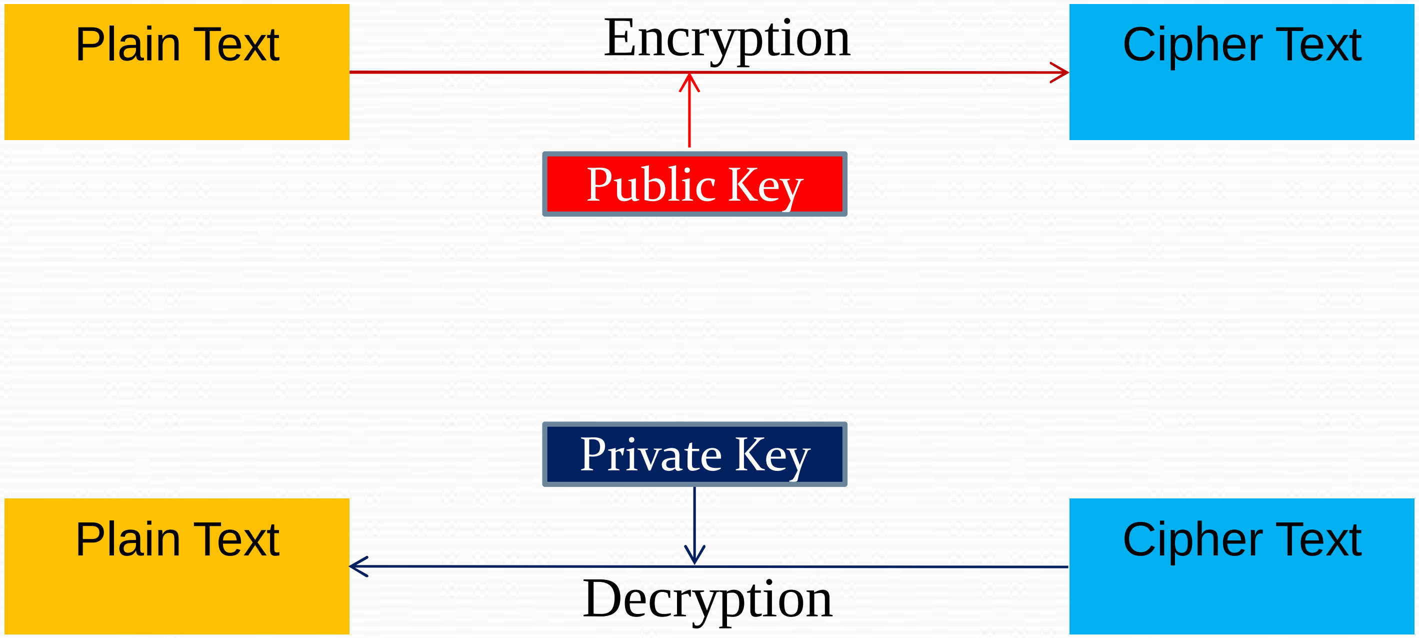

Fig.2. Encryption and decryption process using public and private Key

Cryptography:…Continue

- Hash Cryptography (Algorithm):
  - Hash algorithms are based upon an **one-way function**. One-way function is a function, which takes an input of numbers/plaintext massages/ informations and produces an output such a way that is not possible to figure out what input correspond to a produced output. So hash function is known as **one-way function**.

    Mathematically, a function $y = f(x)$ is said one function if for every x, it is easy to find y, but for a given y, it is computationally infeasible to get corresponding x.

  - A cryptographic hash function h is a mathematical transform that takes a massage m of any length (a string of bit) and convert it into a number of fixed length. For example, Massage Digest (MD4, MD5), Secure Hash Algorithm (SHA, SHA-1), etc.

Authentication:

- Basic Concepts of Authentication Systems
  - Assurance that an entity of concern or the origin of a communication is authentic. In other words information is accessible to authorized entities at the proper time.
- Password Authentication
  - Secure authentication can be done with the help of shared secret key which is called a key or password and this type of authentication is known as password authentication.
- Security Handshake Pitfalls:
  - Security Handshake Pitfalls is a mutual authentication means that both communication parties/partners are able to identify each other. For example, a simple protocol for mutual authentication is based on shared secret.

Related Questions:

1. What is Cryptography?
2. Define the basic terminologies of cryptography.
3. What is the secret key cryptography and public key cryptography.
4. Define hash cryptography.
5. What do you meant by authentication.

References:

1. Manoj Kumar, Cryptography & Network Security, Krishna Publication.
2. William Stallings , Cryptography and Network Security, Third Edition.
3. Dr. Bo Sun, Computer Security.
4. www.i4.informatik.rwth-aachen.de/content/teaching/lectures.
5. https://courseware.stanford.edu/pg/courses/CS155.
6. Dania Alomar, Introduction to Computer & Network Security.
7. Dr. Saleem Al-Zoubi, A lecture on Cryptography and Network Security.

KEEP LEARNING

&

THANK YOU