School of Computing Science and Engineering

Course Code : BCA3010

Course Name: Network Security

UNIT I

Introduction: Basic Terminology

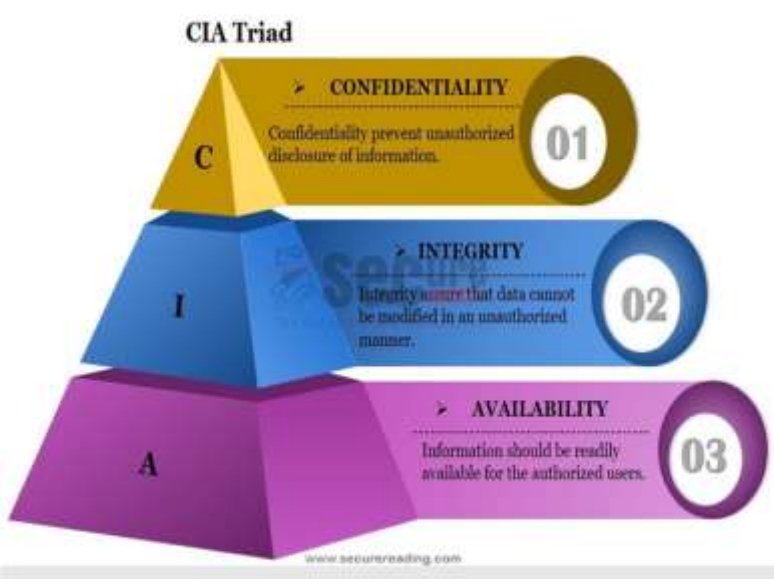
Name of the Faculty: Dr. S.Vijayalakshmi

Program Name: BCA3010

Network Security

Three crucial areas of network security

- ✓ **Confidentiality**
- ✓ **Integrity**
- ✓ **Availability**



➢ CONFIDENTIALITY

Confidentiality prevent unauthorized disclosure of information.

➢ INTEGRITY

Integrity assure that data cannot be modified in an unauthorized manner.

➢ AVAILABILITY

Information should be readily available for the authorized users.

www.securereading.com

CIA Triad

Cryptography

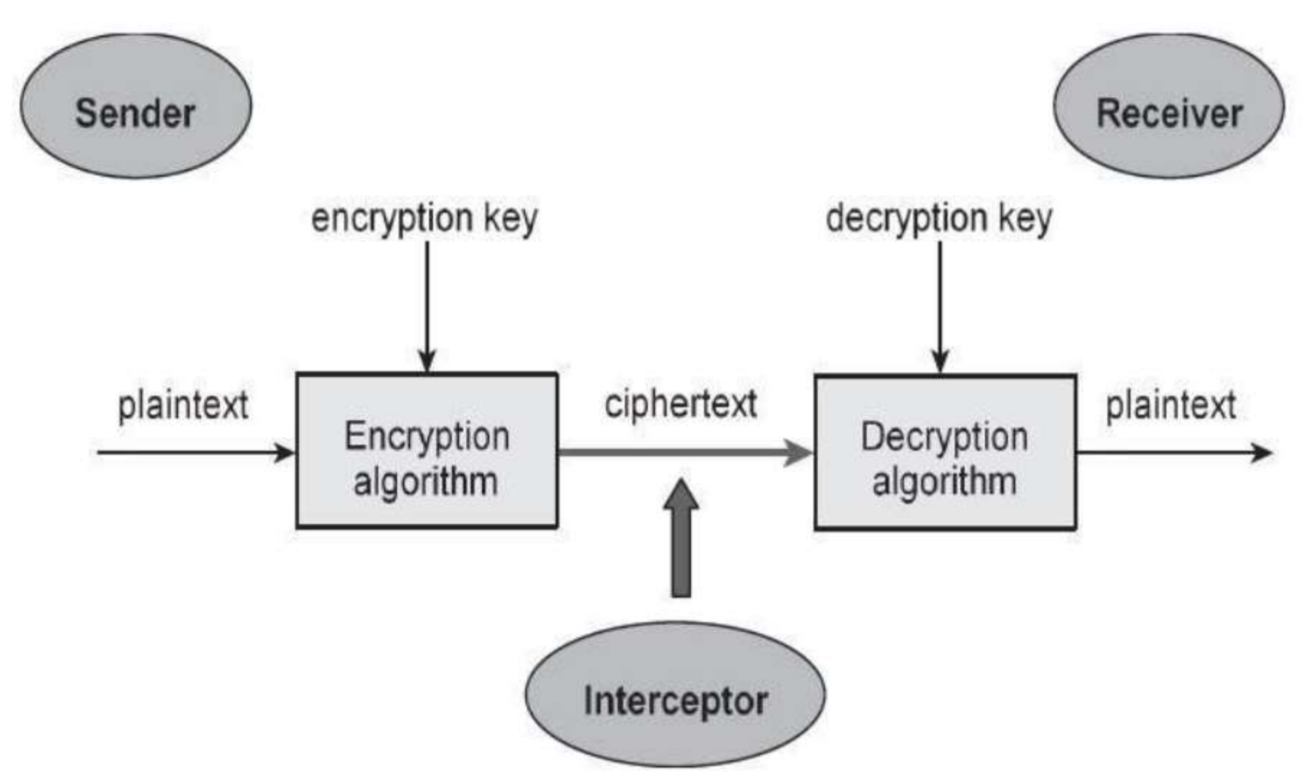
- “crypt” means “hidden” and graphy means “writing”.

- The science of protecting information by transforming it into a secure format.

Primary functions of cryptography

- ❑ *Privacy/confidentiality:* Ensuring that no one can read the message except the intended receiver.
- ❑ *Authentication:* The process of proving one's identity.
- ❑ *Integrity:* Assuring the receiver that the received message has not been altered in any way from the original.
- ❑ *Non-repudiation:* A mechanism to prove that the sender really sent this message.
- ❑ *Key exchange:* The method by which crypto keys are shared between sender and receiver.

Cryptosystem



Cryptosystem

Components of a Cryptosystem

- ❑ **Plaintext**
- ❑ **Ciphertext.**
- ❑ **Key**
- ❑ **Encryption**
- ❑ **Decryption**

Components of a Cryptosystem

- ❑ **Plaintext :-** An unencrypted message. Information that can be directly read by humans or a machine

- ❑ **Ciphertext -** The encrypted data.

Plain text to ciphertext

Two primary ways

1. Substitution Technique

- ✓ **Caesar Cipher**
- ✓ **Mono Alphabetic Cipher**
- ✓ **Homophonic Substitution Cipher**
- ✓ **Vigenere Substitution Cipher**

Plain text   to ciphertext

Two primary ways

2. Transposition Technique

- ✓ Rail Fence Technique
- ✓ Simple Columnar Transposition Technique
- ✓ Vernam Cipher

Key

- ❑ Private Key:-Secret key is used for encryption and decryption
- ❑ Public Key:-Method of encrypting data with two different keys

TYPES OF CRYPTOGRAPHIC ALGORITHMS

- ❑ Symmetric Key Cryptography (symmetric encryption.)
- ❑ Asymmetric encryption (asymmetric encryption)
- ❑ Hash Functions

References

1. Stallings, “Cryptography & Network Security, Principles & Practice”, 3rd Edition, Prentice Hall, 2002
2. Bruce, Schneier, “Applied Cryptography”, 2nd Edition, Toha Wiley & Sons, 1996.
3. Man Young Rhee, “Internet Security”, Wiley, 2003.
4. Pfleeger & Pfleeger, “Security in Computing”, 3rd Edition, Pearson Education, 2003.
5. www.tutorialspoint.com/network_security/index.htm
6. www.javatpoint.com/types-of-computer-network
7. https://www.geeksforgeeks.org/cryptography-introduction/

Thank You