Cryptography and Network Security

1. Cryptography

- The term cryptography is a Greek word which means "secret writing".
- Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa.
- It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.
- Cryptography can also be used for user authentication.
- Modern cryptography is heavily based on mathematical theory and computer science practice.

1.1 Goal of Modern Cryptography: CIA

- **Confidentiality**
  - Confidentiality means information is not disclosed to any unauthorized entity.
- **Integrity**
  - Integrity means accuracy and completeness of data must be maintained and it cannot be edited in an unautorized way.
- **Avaliablity**
  - Availablity means information must be available when it is needed.
- > There must be balance between all three terms.

- CIA is Acheived by:
  1. **Authentiaction**: Authentication is the process of verifing the credentials of users.
  2. **Autherization**: Autherization reffers to the limitation and permission provided to a user to access some information. It takes place after the user is authenticated successfully.

1.2 Components Cryptographic System

- **Plain Text**
  - Plain text is original message or data that needed to be encrypted and is fed into algorithm.
- **Ciphertext**
  - Ciphertext is the encrypted form of the original message. It is the scrambled message produced as output.
  - Ciphtertext depends upon the plaintext, key and the algorithm applied.
- **Encryption Algorithm**
  - The encryption algorithm is that performs various substitution and transformation on plaintext.
  - It is the process of changing plaintext into ciphertext with the use of key.
- **Decryption Algorithm**
  - Decryption algorithm reverses the effect of encryption and changes the Ciphertext back into plaintext.
  - It takes ciphertext & key and produces the original plaintext.
- **key**
  - It is an important component of cryptography.
  - It acts as input to the encryption as well as decryption algorithm.
  - The exact substitution and transformation performed by algorithm depends on the key.

1.3 Cryptoanalysis

- The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key.
- Also called code breaking

1.4 Cryptology

- It is the study of both Cryptography and Cryptoanalysis

2. Security Attacks

- Network security attacks are unauthorized actions against private, corporate or governmental IT assets in order to destroy them, modify them or steal sensitive data.

2.1 Types of Security Attack

i. Active Attacks
ii. Passive Attacks

- **Active Attacks**
  - An active attack attempts to alter system resources or effect their operations.
  - It involves some modification of data stream or creation of flase statements.
  - Types of Active attacks are:
    - Masquerade: These attack take place when one entity pretends to be a different entity.
    - Modification: It means some portion of message is altered or being delayed or reordered to produce unauthorized effect.
    - Repudiation: These attack takes place when sender or receiver denies sending or receiving a message.
    - Replay: It involves passive capture of message and subsequent transmission to produce an authorized effect by attacker.
    - DOS(Denial Of Service): It prevents normal flow of communication to take palce. It can include disrution of entire network or sending false request to overload the network.
- **Passive Attacks**
  - A passive attack attemps to learn or make use of information from the communication.
  - It does not effect the system resources or their operations.
  - It involves Snooping and Traffic Monitoring
  - Types of Passive Attack:
    - Snooping: These attack takes place when an attacker can obation the confidential data being transferred and read it.
    - Traffic Monitoring: Even if the data is encrypted so that no one can determine the actual content of messages but by analysing the traffic an attacker can determine the location & Identity of host, length of message,
    - These information can ve used in guessing the nature of communication.

2.2 Security Attacks and CIA

- Attack on **Confidentiality**:
  - Passive Attack:
    - Snooping
    - Traffic Monitoring
- Attack on **Integrity**:
  - Modification
  - Masquerading
  - Repudiation
  - Replay
- Attack on **Availability**:
  - DOS (Denial Of Services)

3. Conventional Cryptography

- conventional Encryption is also called secret-key or Symmetric Key Cryptography.
- In this type, one key is used for both encryption and decrytption.
- Data Encryption Standard (DES) is an example of conventional cryptography which is widely used.

3.1 Types of Symmetric Key Cryptogtaphy:

- Substitution Cipher
- Transposition Cipher

Substitution Cipher	**Transposition Cipher**
Secure	Less Secure
Key Required	No key required
Substitution takes place	Shifting takes place
`Ceaser Cipher , PlayFair Cipher , Hill Cipher , Rotor Cipher , Vigenere Cipher,  Vernam Cipher , Affine Cipher`	`RAIL Fence Cipher , Columnar Cipher`