Department of Computer Science Engineering
Faculty Name- Jiyaul Mustapha
E-mail- jiyaul.mustafa@monad.edu.in

Students can take help of this YouTube video tutorial link
https://www.youtube.com/playlist?list=PL9FuOtXibFjV77w2eyil4Xzp8eoogsPp8
Or
Scan this QR Code to open the video tutorial link:

CRYPTOGRAPHY & NETWORK SECURITY

Basic concept:-

It is a technique in which we protect the information by transforming it into unreadable format is called cryptography.

Types of Cryptography

It is divided into two parts –

1. Cryptography. 2. Cryptanalysis

Principle of security:-

It provides the following fundamental information security services.

Confidentiality

The principal of confidentiality specifies that only the sender and receiver should be able to access the content of message. Confidentiality gets compromised if an unauthorized person is able to get access the content of message.

Data Integrity

When the contents of message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of message is lost. This type of attack is also called modification.

Authentication

Authentication mechanism helps to establish proof of identity. This process ensures that the origin of an electronic message or document is correctly identified.

Authentication service has divided into two parts –

- Message authentication
- Entity authentication.

Non-repudiation

There are situation where a user sends the message and later on refuses that she or he had not send that message.

Access Control

The principle of access control determines that who should be able to access what.

Availability

It states that resources or information should be available to authorized party all time.

Cryptography primitives in detail:-

It provides the following security services –

- Encryption
- Hash functions
- Message Authentication codes (MAC)
- Digital Signatures

Basic component of cryptosystem in detail:-

A cryptosystem is an implementation of cryptographic techniques.

It provides information security services.

It is also called as a cipher system.

Components of a Cryptosystem:

The basic component of a cryptosystem is following −

- Plain Text.
- Encryption Algorithm.
- Cipher text.
- Decryption Algorithm:-
- Encryption Key.
- Decryption Key.
- Interceptor

Symmetric and asymmetric key encryption.

Symmetric Key Encryption

The encryption process in which same keys are used for both encrypting and decrypting the information is known as Symmetric Key Encryption.

The study of symmetric cryptosystems is called as symmetric cryptography.

Symmetric cryptosystems are also sometimes called as secret key cryptosystems.

The main features of symmetric key encryption are following −

- The user which is using symmetric key encryption must share a common key to exchange of information.
- Keys are suggested to be changed time to time to prevent any attack on the system.
- In a group of n people, to enable two-party communication between any two user, the number of keys required for group is equal to $n \times (n – 1)/2$.

Asymmetric Key Encryption

The encryption process in which different keys are used for both encrypting and decrypting the information is known as Asymmetric Key Encryption.

The main features of this encryption scheme are following –

- Every user has a pair of different keys, private key and public key.
- It is mandatory to keep public key in public repository and the private key as a well-guarded secret. Hence, this encryption is also called Public Key Encryption.
- Public and private keys of the user are related; hence computationally it is not feasible to find one from another. This is the main strength of this scheme.
- When Host1 want to send data to Host2, first he obtains the public key of Host2 from repository, and then encrypts the data, and then transmits.
- Host2 uses his private key to decrypt the plaintext.

Security Mechanism in detail:-

A mechanism that is designed to detect, prevent or recover the data from a security attack.

Different types of security mechanism are:

1. Encipherment

2. Digital Integrity

3. Digital Signature

4. Authentication Exchange

5. Traffic Padding

6. Routing Control

7. Notarization

ATTACKS ON CRYPTOSYSTEM:

In Cryptosystem the attacks are typically two types

- active Attacks
- passive attacks.

Passive Attacks:-

Passive attacks are those where the attacker indulges in eavesdropping or monitoring of data transmission. In other word the attacker aim is to obtain information that is in transit. The term passive indicates that the attacker does not attempt to perform any modification to the data.

Active Attacks

The active attacks are based on modification to original message in some manner, or on creation of false message. This attack cannot be prevented easily. These attacks can be in the form of interruption, Modification and fabrication.