



NETWORK SECURITY

BY ABDUL MUQSITH

Covers maximum syllabus for diploma in
Cyber Physical systems and Security
written by Abdul Muqsith

MORE INFO

way_towards_truth

CALL US

Don't call



Introduction to Cryptography

1.0 Introduction to Cryptography.

Cryptography is a study of techniques for protecting the information in a communication from unauthorised access & modifications.

→ It involves transferring data into unreadable format so anyone can't read that format except those with authorised access with decryption key.

→ It ensures confidentiality, integrity & authentication.

1.1 Security and Network Security.

Security: Security generally focusses on protecting the Computer System from unauthorised activities.

* It focusses on both physical & Cyber Security aspects.

* It tries to protect overall system.

Ex: Before entering in a company or system all the security locks & Biometric authentication comes under security.

Network Security: It is a practice of protecting the computer network and information transfers in a network from unauthorised access, modifications & misuse etc.

* It focuss on narrow field i.e Networks, Internet Security.

* It tries to protect network [communication network]

Ex: Whatsapp [end to end Encryption]

1.2 OSI Security Architecture

OSI - open system interconnection. It is a Security architecture or framework developed by ISO - International Organisation of Standardization & defined by ITU - International Telecommunication Union ~~which~~ to secure communication in a network.

* It focusses on study on Security Attacks, mechanisms and services. See.

It has 7 layers:

- 1> physical layer - physical transmission of data
- 2> Data link layer - Ensures error-free transport b/w nodes in network
- 3> Network layer - determines data path (route) for transmission
- 4> Transport layer - provides end-to-end communication b/w devices
- 5> Session layer - manages connections b/w application.
- 6> Presentation layer - translates data b/w application ^{format} & network ^{format}
- 7> Application layer - provide network services to user.

1.3 Security Attack & types

Security Attack: It is an attempt to breach ^(breach = unauthorised access) security against laws to harm ~~see~~ the network, data, & system to gain unauthorised access, modifications of information transmitting in a network.

It is of two types passive and Active Attack.

➤ Passive Attack:

A passive attack refers to an attack in network in which attacker spy and monitor the communication without altering or modifying the information. †

* In this type of attack the attacker doesn't interfere with data modification but simply listens or observes the info. ~~un~~authorizingly.

Ex: * Eavesdropping on an unencrypted Wi-Fi network to steal sensitive information like passwords • Generally public Networks

* masked ~~car~~ traffic analysis :- attacker observes the encrypted information. he can't directly understand it but can get length of message etc.

➤ Active Attack.

In this type of attack the attacker modifies, deletes, changes & manipulates the data with an intention to harm.

* Generally sender & receiver have no clue of that their communication is under attack.

* They can cause lighter to extremely severe danger.

~~car~~ It has 4 categories or Attacks.

Masquerade: Attacker pretends to be authorized user to resource. by having some stolen sensitive info of authorized user.

Replay Attack: The attacker records a valid message

and send it again to the system ~~to~~ • Simply, the attacker sends requests to system multiple times to send some data, money etc.

Denial of Services (DoS):

The attacker floods a system or server with too many requests, making it to crash or server down so real users can't access it.

Man in the middle (MITM).

The Sender's messages reaches attacker or hacker first & hacker modify it & sends to the actual receiver in altered form.

1.4 Active and Passive Threat. (Threat & attack are different)

Passive threat: Risk that an attacker can monitor the ~~data~~ communication over a network

Ex: Hacker trying to steal sensitive info of user like usernames, passwords before performing an active attack.

Active threat: Risk that an attacker can gain unauthorized modifications in communication.

Note: Threat & Attack are different

Threat - possibility to harm.

Attack - Actual event where harm is done.



1.5 Security Goals.

Main Security goals in cryptography is to ensure the Confidentiality, integrity, Availability, Authenticity, Accountability of data being transferred in a network.

Confidentiality: To protect data from unauthorised access.

→ Can be achieved by (i) Encryption
(ii) Access control.

Integrity: Ensures data is protected from altering.

→ Can be achieved by (i) Digital Signature
(ii) Authorization.

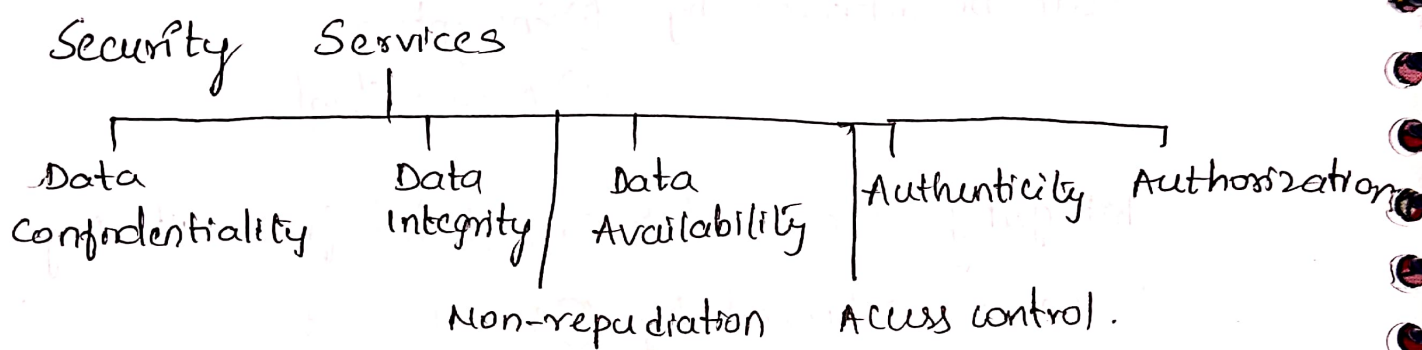
Availability: Ensures network resource data is always accessible for authorized users.

→ Can be achieved by (i) DoS Defense.

Authentication: Ensures access for network resource is given only to authorised users. by checking authenticity of user like passwords & usernames.

Security Services

Security Services & main mechanisms are closely related in cybersecurity. But the difference is security services focus on what security measures should be taken & security mechanism focus how the measures are implemented.



① Data Confidentiality: Ensures data is protected from unauthorized access in a network.

Achieved by

- i) Data Encryption
- ii) Masking

② Data Integrity: Ensure data remains accurate & unaltered during transmit.

~~Other~~ mechanisms like

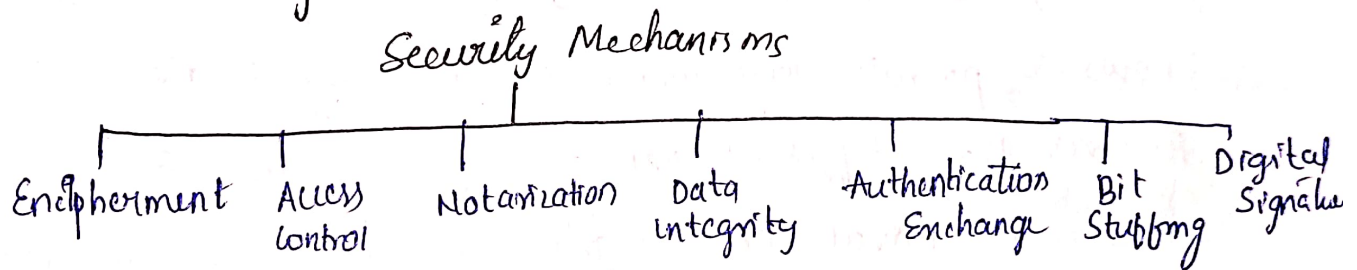
- i) digital signatures
- ii) Checksums

③ Authentication: It is the process of verifying the user, data, device / system before granting Access.

Includes passwords, Biometric, 2FA, OTP's

- ④ Authorization: It is the process of controlling what authorized user can legally access the info.
- ⑤ Access control: Same as Authorization indeed Authorization is also referred as Access control.
- ⑥ Non-repudiation: Prevents denial of communication or service

1.7 List Security Mechanisms.



⑦ Encipherment:

Encipherment refers to converting plaintext into cipher text (un-readable form) before & while transmitting it after reaching desired destination text can be converted into plaintext or irreversible encipherment can also be done [hashing]

⑧ Access control:

It is the process of controlling what an authorized user can legally access the network resource. It can be achieved by mechanisms like

- ① Role-based Access control (RBAC)
- ② Mandatory Access control (MAC)
- ③ Access pin to resource.

⑨ Notarization:

It is a mechanism where trusted third party is there in b/w sender & receiver communication so to prevent

non-repudiation, where a sender denies sending a message.

⑩ Data Integrity.

Data integrity is the main concept which tells data shouldn't be altered at any cost which can be achieved by digital signature, CRC, error detection & correction, Backup etc.

⑪ Digital Signatures.

using private & public keys we can achieve digital signature generally sender & Receiver has public key which they both know & private key which is known by single sender & Receiver has different private key. Sender Encrypt the file with private key & ~~generates~~^{becomes} digital signature

A Receiver checks the file by using decrypting public key if the hash matches with public key then it represents sender is authorized.

1.8) Authentication, Confidentiality, integrity w.r.t data.

Authentication

Authentication is the process of verifying the identity of user, device or system that is attempting to access the data

Types of Authentication

① PIN's - using PIN's, password or any secret info that is known only by legal Entity.

② OTP's & SMS.

③ Biometric.

Confidentiality

Confidentiality refers to protecting data from unauthorised access, it ensures data under a network can only be accessed by authorized entities from reading, copying or altering.

can be achieved by Symmetric or Asymmetric Encryption, access control, data masking.

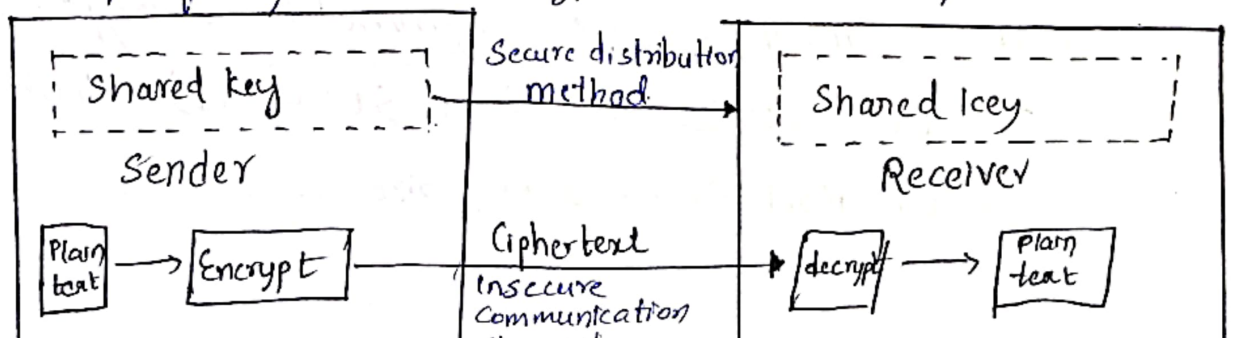
Integrity

Data Integrity refers to protecting data from alteration, modification etc. It ensures data under a network is completely secured & unaltered by any unauthorized entity. can be achieved by Digital Signatures, checksums, CRCs Error-detection & correction techniques.

• 9 Symmetric Encryption:

The Encryption process where same key are used for Encrypting and decrypting the information is known as Symmetric Encryption.

* Study of symmetric Encryption is called Symmetric Cryptography



- * Persons using symmetric key Encryption must share a common key to Exchange of information.
- * Keys are recommended to change regularly
- * A robust mechanism need to be exist to Exchange Secret key between two parties.
- * In a group of n peoples, $\frac{n(n-1)}{2}$ keys required for two party communication

The shared key must be protected or else if the hacker able to get that key then it can decrypt the ciphertext he got from passive attack.

Block Cipher

Block Cipher is a type of Encryption method in which a plain text is divided into fixed number of blocks of specific size & each block is encrypted using a shared secret key & produces a block cipher text using encryption algorithm.

- * This Encryption uses symmetric Encryption Approach ex: DES (Data Encryption Standard) which has 64-bit block size & key size is 56-bit.

AES (Advanced Encryption Standard)

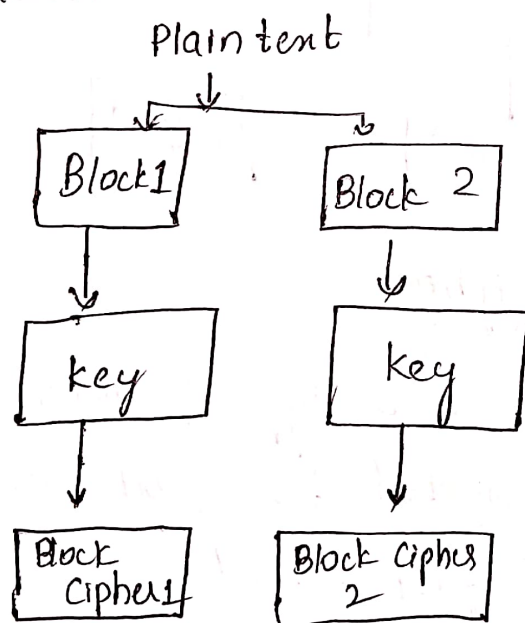
It is a popular block cipher which encrypts data in blocks of 128 bits using 128, 192 and 256 bit Symmetric keys.

Modes of operation.

① Electronic codebook mode (ECB)

Electronic codebook mode is the mode in which each block is encrypted using a fixed symmetric key. & ~~key has no link~~ no previous block has link with successive block in encryption.

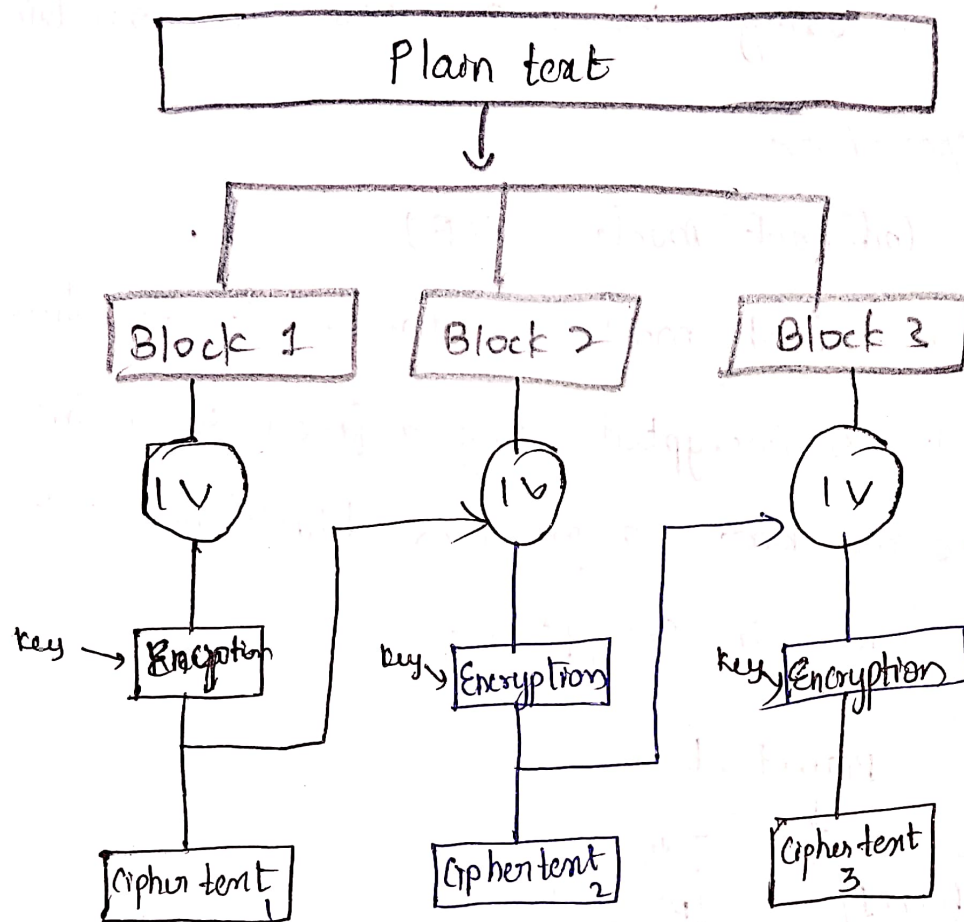
Illustration



② Cipher Block Chaining (CBC)

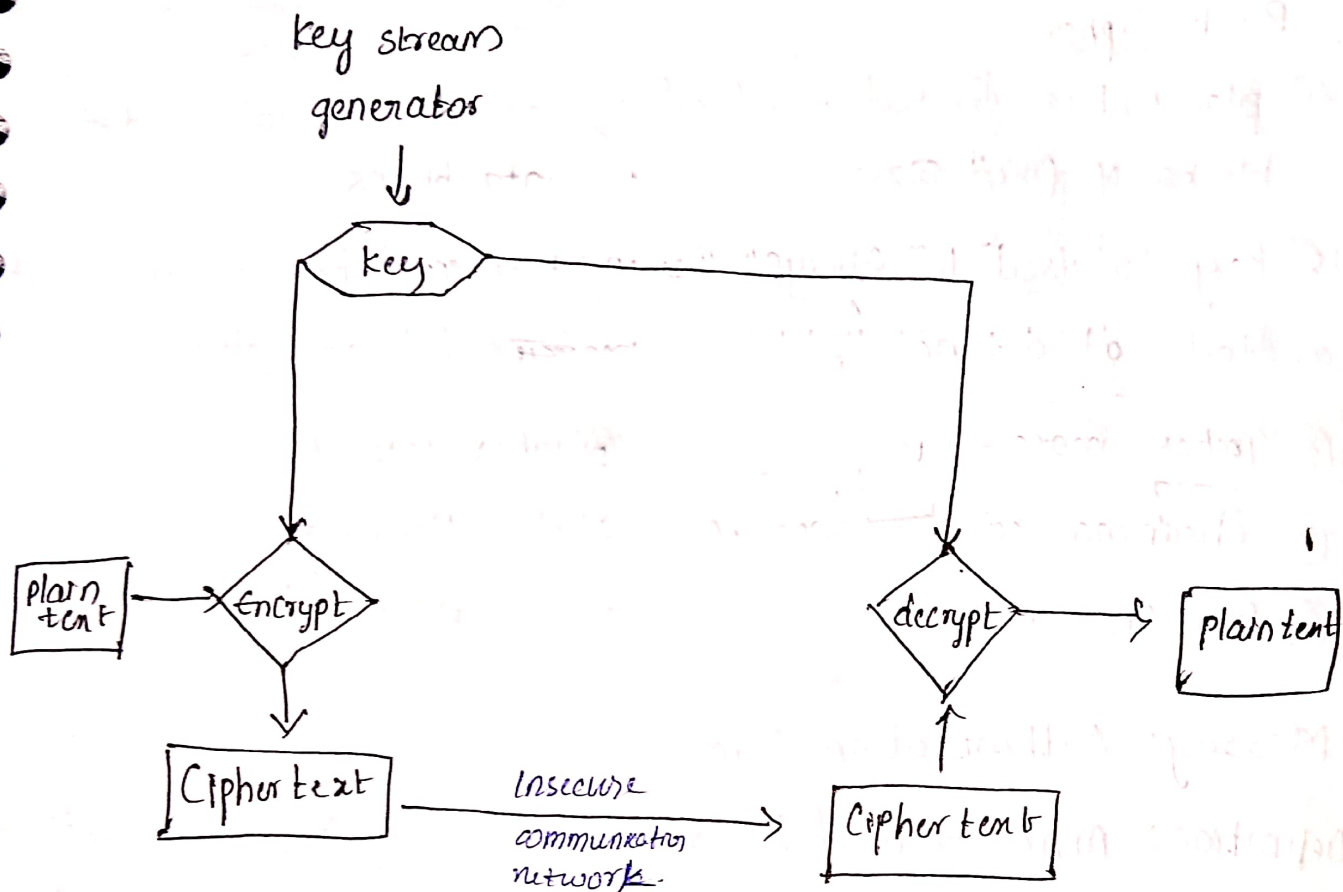
In this mode each Block cipher has link with successive Block. In this mode for ~~first~~ each block has IV (Initialization Vector). For first block IV will be selected randomly & for next block IV will be the ciphertext of previous block. Generally cipher text is generated using

XOR method where Each block is set into binary form & are XORed with IV (Initialized Vector).



Stream Cipher

Definition: Stream Cipher is a type of encryption method in which data is encrypted bit by bit instead of dividing into blocks. So they are fast & used in scenarios where data arrives in a continuous stream like video streaming
Ex: RC4, ChaCha20, Salsa20, SEAL.



Ex: RC4

Let plain text is HELLO ~~WORLD~~.

Then key stream generator generates key as some random number of ASCII like {75, 30, 40, 50, 90}.

Let ASCII of plaintext is {72, 69, 76, 76, 79}

XOR plaintext ~~to ASCII~~ with key

Cipher text Byte = plaintext Byte $\oplus$ key stream Byte

$72 \oplus 75, 69 \oplus 30, 76 \oplus 40, 76 \oplus 50, 79 \oplus 90 = 3, 104, 22, 91, 23$

Let the ASCII 3, 104, 22, 91, 23 is: ?#h\$Z (cipher text)

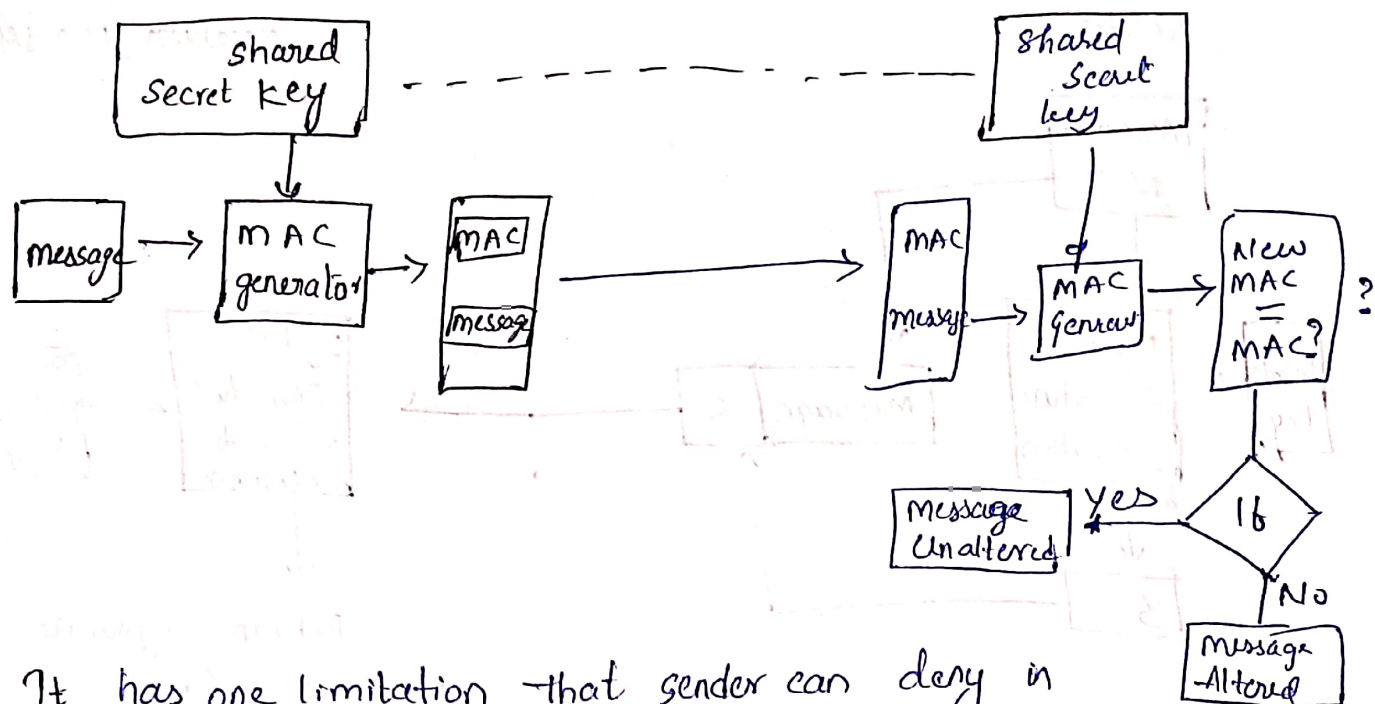
Block Cipher	Stream Cipher
① Plaintext is divided into fixed blocks of fixed size	① Plaintext is not divided into blocks.
② Key is used to Encrypt the one block at a time	② Key used here is to Encrypt one each bit at a time
③ Takes more time	③ Takes less time
④ Chaining can be done (CBC)	④ No chaining.
⑤ Exr CBC, ECB	⑤ Exr RC4, ChaCha20, Salsa20

Message Authentication Code

Definition: MAC is used to verify the integrity & authenticity of a message. It ensures that message is not altered.

How MAC works

A MAC is generated by combining message with secret code and then applying a cryptographic function (hash function) to produce fixed size MAC. This code is ~~sea~~ attached with message and is sent to Receiver. When the Receiver receives it, then it checks/verify message. The receiver uses same secret key ~~to~~ compute the MAC & generate new MAC code from received message. If received message is unaltered - then new MAC will be equal to given MAC if message is altered then they both differs.



It has one limitation that sender can deny in sending a message to receiver (non-repudiation).

Application

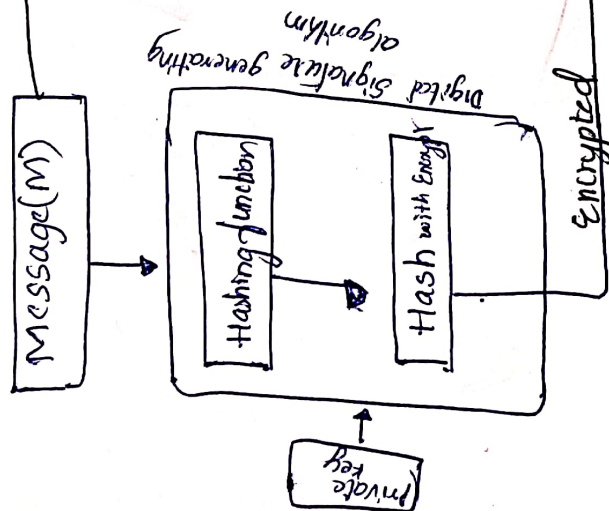
- 1) MAC can be used by digital signatures as part of their structure.
- 2) Payment: MAC is used on transaction details to ensure details have not been changed.

1.12 Define Digital Signature.

A digital Signature is a cryptographic technique used to verify the authenticity & integrity of a digital message or document. It ensures that the message was created by known sender (authenticated sender) & has not been tampered or altered by anyone (integrity) & provides non-repudiation, means the sender cannot deny about the message sent by him/her.

Model of Digital Signature

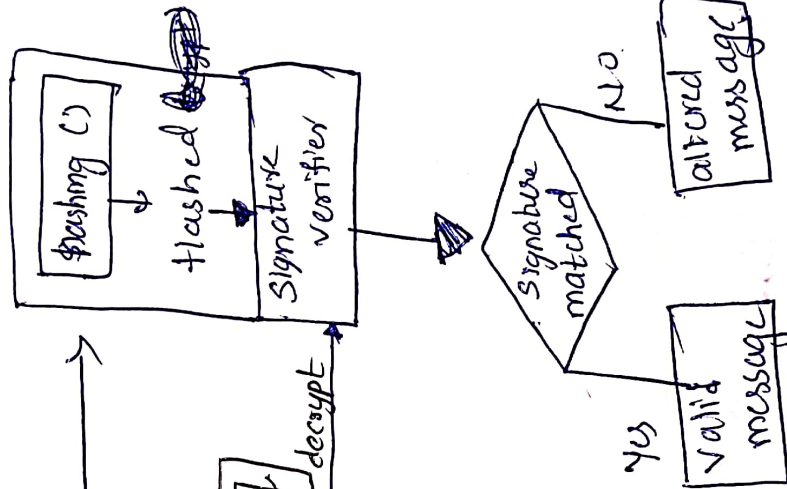
Signer (sender)



Network



Verifier (Receiver)



① Digital Signature follows below structure.

sender side

① message is hashed using hashing function generally hashing function takes message as input & generates fixed sized output known as message digest or hash using

private key $H(M) = \text{Hash function}(M)$

Ex: $M = \text{Hello}$

$H(M) = \text{xy mms} \dots \text{fixed size}$

② Then message digest (hash) is encrypted $E(H(M)) = \text{ay259} \dots$

③ Original message with digital signature output is transmitted

Receiver side

① message & signature at receiver side is verified

② message is input for hashing (1) & it gives hash (message digest) using public key

③ Hash is sent to signature verifier which compares received ^{decrypted} sign & generated signature

④ If both matches then signature is verified & correct if not same then message is altered.

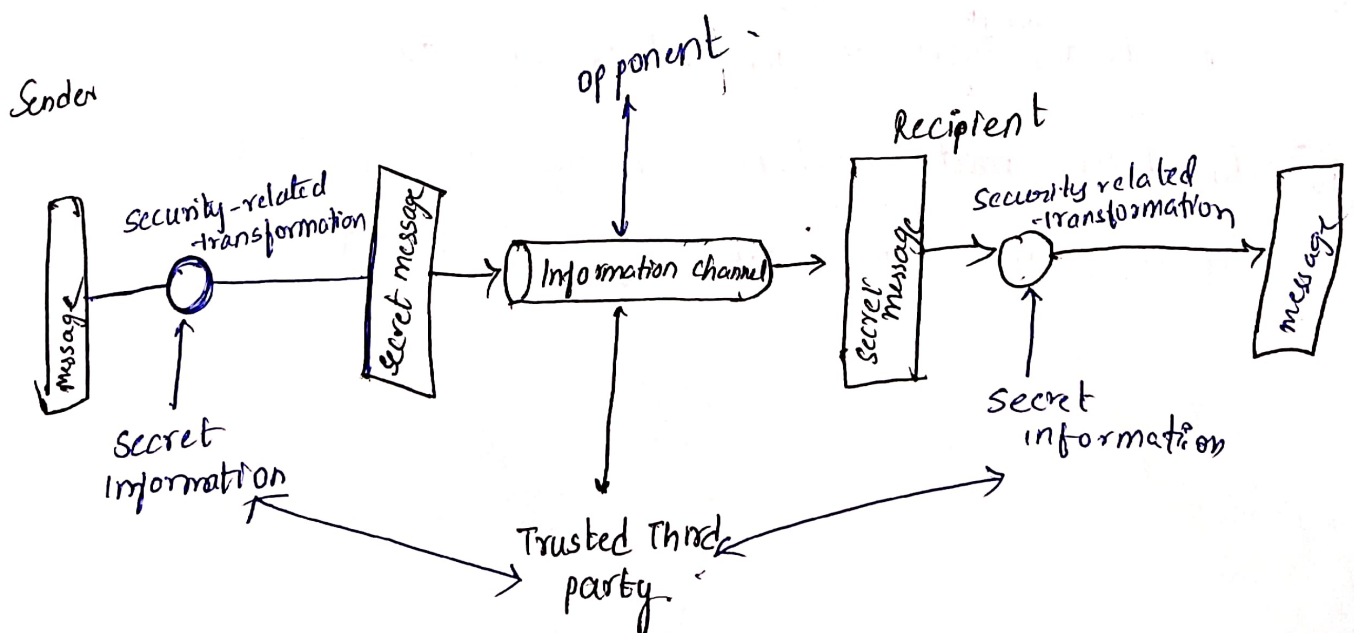
1.14 Explain Encryption with digital Signature.

(A) Message is fully encrypted in digital Signature to provide high confidentiality of message. In fact, the digital Signature is nothing but an encrypted hash of the message. It involves two steps hashing function to hash message & then encrypt the hashed message.

~~Out Hashing function.~~

Generally using SHA-256 & private key message is hashed using hashing algorithm and generates unique message and that unique message is further encrypted using private key to generate or to convert hashed message into highly non-human unreadable format which is called a digital Signature. Encryption.

1.15 Draw the model of network security & explain.



Ch-2 Hardware and Software Security

2.1 Discuss Hardware Security.

Hardware Security

- * Hardware Security focus on protecting physical devices, circuits and systems from unauthorized access, tampering & malicious attacks.
- * The devices can be a network routers, switches, firewalls servers etc.
- * Hardware Security Ensures - the network is secure & resilient against physical & cyber threats
- * focusses on protecting firewalls, VPN hardware, intrusion detection systems
- * Hardware of any device can be protected if we use trusted firmware & software. → Hardware Encryption (like a black strip (magnetic strip on Debit card))

2.2

2.2 List & Explain Smart Cards

A Smart Card is an embedded Integrated circuit (IC) that can store & process some data used for secure identification before giving access to resource. It has more functionality & security than traditional magnetic strips.

1

Ex: Smart Contact card, Contactless card, Hybrid/Dual Interface

Types of smart Cards

i) Contact Smart Card:

Contact smart card works by directly connecting its embedded chip to a card reader via metallic contacts. When card is inserted into reader it generates electrical connections allowing card & reader to exchange data.
Ex: While transactions the reader asks PIN & reader verifies it with the actual PIN stored in unreadable format in chip which adds extra security when card is stolen.

ii) Contactless smart Card.

This type of smart card establishes a connection with a card reader without any physical contact. It has an antenna through which communication is done. If you bring a card near a compatible reader within a few millimeters, the card & reader exchange data through RFID (Radio Frequency Identification) or NFC (Near Field Communication) technology. Ex: transit card.

iii) Dual-Interface Card.

This type of smart card is equipped with both contactless and contact interfaces.

iv) Memory based smart card. This type of smart card is embedded with memory circuit. It stores

and writes data to a particular location except some restricted location that has read only mode.

It is a straight memory card

Micro-processor-based smart cards:

This type of smart card consists of a microprocessor in addition to the memory block, allowing for data processing & manipulations & can be used for multi-functioning.

203 List & Explain Types of Biometrics

Biometrics are the commonly used devices that captures biological & physiological data of user to analyze whether user is authenticated or not.

commonly used biometrics are of fingerprints, facial, voice, iris or palm.

Types

(i) Biological (ii) morphological (iii) Behavioral biometrics

Biological Biometric.

Biological Biometric refers to a type of biometric authentication that uses unique ^{permanent} biological characteristics of an individual to verify their identity.
E.g. fingerprint patterns, iris, DNA, palm veins.

② morphological biometrics

morphological biometrics involves the physical structure of your body. like fingerprint, ear shape, iris, hand geometry. etc which can be measured & static.

Unique

③ Behavioral biometrics

A biometric system that detects actions like voice action, signature, pressure applied from a person for validating authenticity.

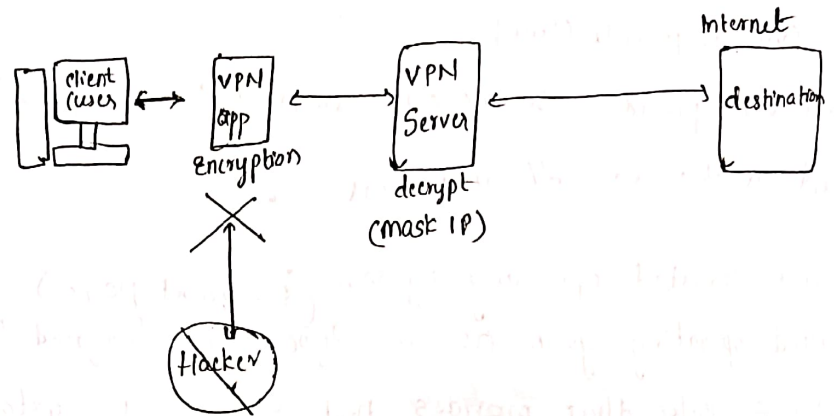
2.4 Discuss Virtual Private Network & Types of VPN

VPN

VPN - Virtual Private network →

VPN is a network provided by VPN server that creates a secure communication between a device & a remote server by masking IP address & encrypting data.

* VPN app encrypts a user's data & send it to VPN server through Internet & VPN server decrypt the data & mask the IP of user or client & provides a separate tunnel to transmit it to destination server or device. In this way in a public Internet a separate private channel is created for secure connections.



Types

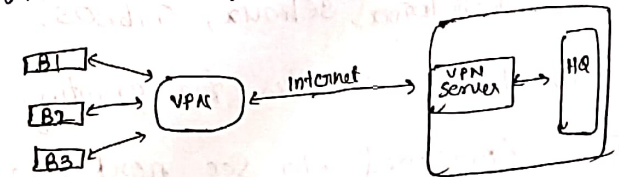
① Remote VPN.

Remote VPN allows users to securely connect to private networks like company's internal network from a remote location. Users connect to VPN through an application, encrypting their internet traffic to secure communication.

Remote VPN is nothing but public network to private network connection through VPN. & VPN server is at private network.

② Site to site VPN.

a connection that securely connects multiple branch office networks with a head office network is called site to site VPN.



③ Personal VPN

Secures users' internet connections & hides their online activities from third parties. Ex: NordVPN

4) VPC (Virtual Private Cloud)

Cloud VPN provides secure connection between user & cloud & that to authorized users.

2.5 Discuss Trusted Operating System. (see next page)

① Trusted operating system (TOS) is a type of OS designed for extra security that provides high security to system memory, files, peripherals etc by giving access to media only for authorized users.

② & TOS keeps a log (eye) on everything happening in system to detect any suspicious attacks on your system.

③ & TOS ~~helps you to~~ ^{system} avoid changes in settings without the permission of authorized user.

④ & TOS disallow unauthorized users to open files, share files etc without the permission ~~by~~

⑤ & TOS are generally used in banking or govt systems.
Ex: ~~Kali Linux~~, SELinux, QubesOS.

⑥ TOS has strict rules for granting access

⑦ (preferred - to see next page)

Trusted Operating System.

A Trusted Operating System (TOS) is an OS that has multiple securities which ensures that the system resources are highly secured like files, applications, memory, processor, etc.

① TOS is an OS which has ~~set~~ strictly set predefined security rules set by system administrator so no user can add or subtract security rules to their files & all users must need to follow rules of Admin called MAC mandatory Access control.

② TOS keeps a log on everything that user do so to detect & restrict any suspicious activity.

③ TOS prevents unsafe files to be downloaded.

④ It provides high data integrity & confidentiality.

⑤ It gives limited access to users & doesn't give access to unauthorized users of system resources.

Ex - SELinux, Qubes OS, Trusted Solaris, Windows 11, AIX

2.6 - explain pretty good privacy (PGP).

PGP- (Pretty Good privacy) : PGP is a framework designed by Phil Zimmermann for secure communication of Emails, files in a network.

* PGP provides i) Integrity
ii) Confidentiality
iii) non-repudiation
iv) authentication of message & data.

* It ^{uses} Encryption & digital signature concept.

It follows below steps (at sender side)

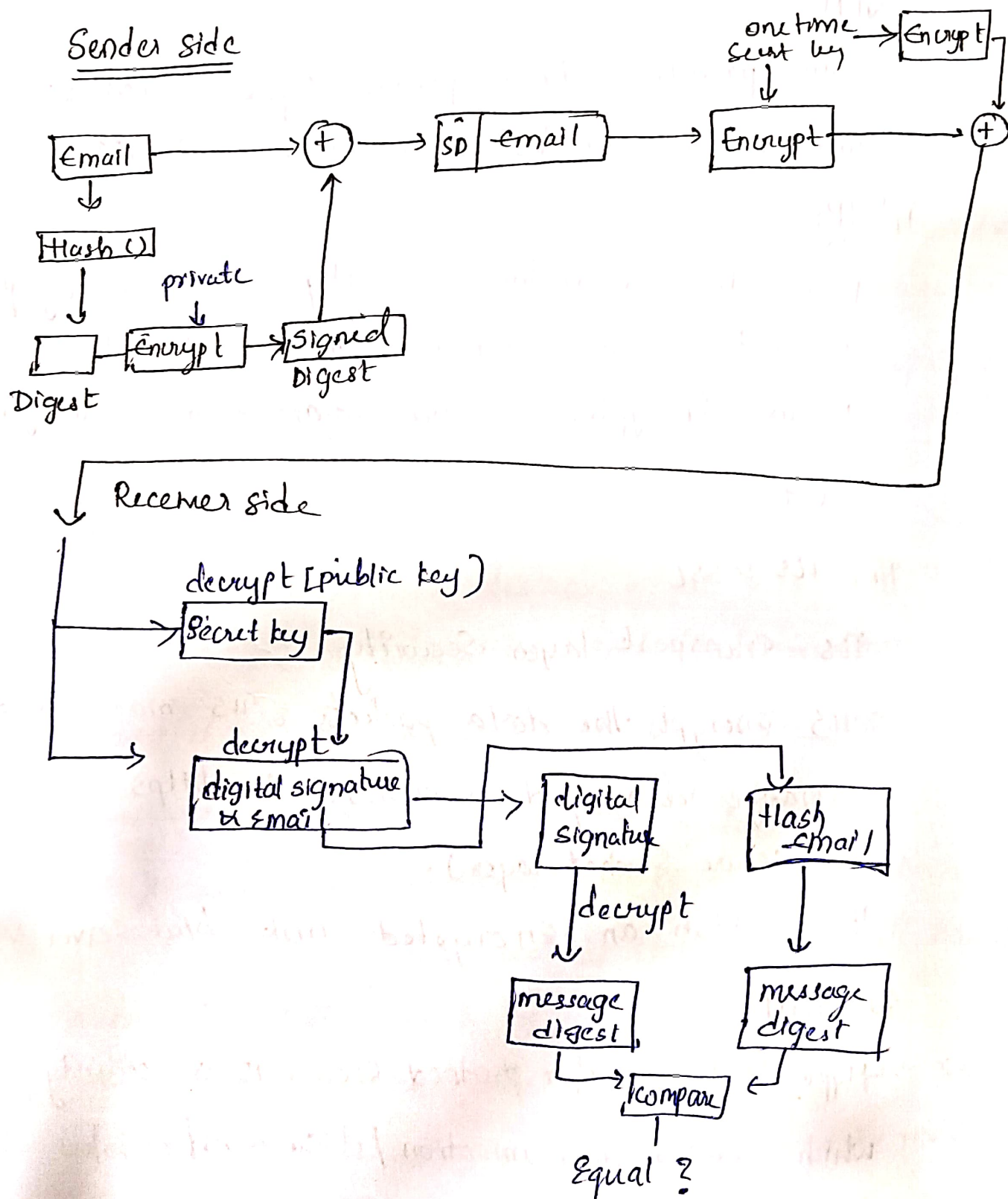
- ① Generate message digest of email using hash function
- ② Encrypt the message digest which is nothing but digital signature
- ③ Encapsulates the signed digest + Email.
- ④ using one-time secret key encryption is done to encapsulated digest & email
- ⑤ one-time secret key is encrypted using Public key & sent to Receiver.

at Receiver side

- ⑥ Reached Encrypted encapsulated info is decrypted after decrypting secret key by using public key
- ⑦ then the message digest is decrypted.

③ The Email is sent to hash () generator to generate message digest.

④ Both the message digest of received Email & message digest of sender is compared if same then message is unaltered but if differ it means altered message



2.7 Explain Security protocols.

Security protocols are set of rules & procedures designed to protect data integrity, confidentiality, authentication during data exchange.

Ex: VPN, IPsec, TLS & SSL, HTTPS, PGP,

i) VPN

Virtual private network provides separate tunnel for communication & masks the IP Address & encrypt data

ii) IPsec

IPsec - Internet protocol Security is a security protocol used to secure communication over IP network.

It uses Encryption, authentication & ensure integrity of data.

iii) TLS & SSL

TLS - Transport layer Security

TLS encrypts the data packets & TLS make data doesn't change during transmission Ex: https.

SSL (Secure Socket Layer)

It establish an encrypted link b/w server & client

iv) HTTPS

Hypertext transfer protocol Secure is a security protocol which secures communication / data transfer b/w browser & server. (website server)

it authenticates Webpage is secured or not also the user is legal or not & also encrypt the data transfer by using many rules & regulations.

Kerberos

Kerberos is also a security protocol used for authenticating the devices that are communicating in an insecure network like internet. It authenticates that both sender & receiver are who they claim to be.

2-8 Explain various hardware Securities (Smartcard & Biometrics)

Hardware security refers to use of physical devices to enhance security in a system. They are of many types but commonly used are Smart Card & Biometrics.

Smart Card

Smart Cards are portable devices whose size is ~~is~~ nearly equal to credit card which has embedded microprocessors & memory chip & is able to store some data & process data.

- * They generally store PINs & cryptographic keys etc.

- * Specific card has specialized devices to read data.

- * If card is physically damaged or stolen you can't have access to even your legal purpose.

- ^{Some} * cards have some features like PIN ~~protection~~ etc so card will give access only if PIN is given to reader.

Biometrics

Biometrics are the devices which are ~~also~~ used for authentication.

They are the devices that give access ~~only to~~ only to users whose unique biological character is recognized as authorized.

They depend on permanent & unique biological character of humans in order to detect user is authorized or not.

Biometrics don't need cards etc so physical presence of user is must & user need not to carry any special ~~card~~ device etc so it gives high security & authenticity.

209) Describe VPN and its types with a neat diagram.

VPN is a virtual private network that provides a safe & secure transmission tunnel for data ^{to travel} between your device & destination device like server etc in internet.

• VPN has its server which when you connect to it your IP address will be masked & a separate way is Types

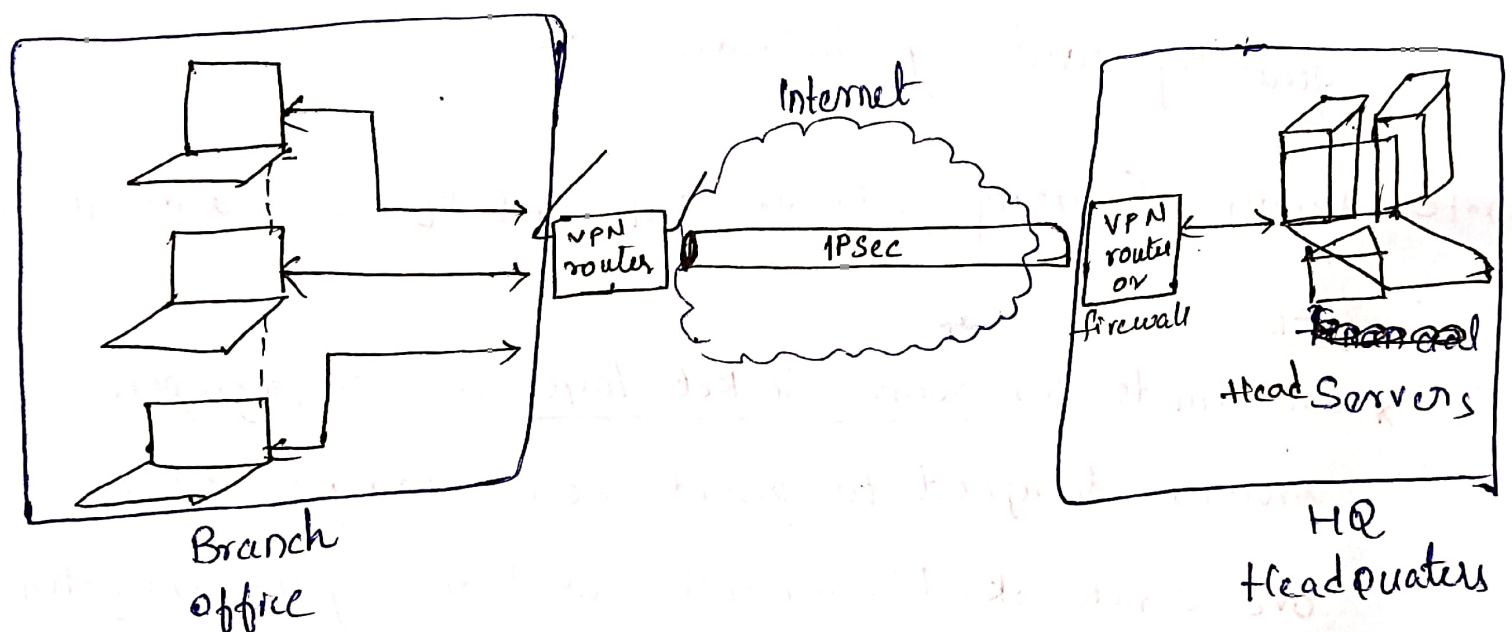
1) Site-to-site VPN.

Site to Site VPN is a type of network connection that links two or more ~~network~~ private networks at different locations securely ^{under} in secure ~~net~~ internet etc.

① ~~Two or more~~ branch offices.

① Two or more physical location (like branch office to main office) uses VPN devices like routers or VPN appliances

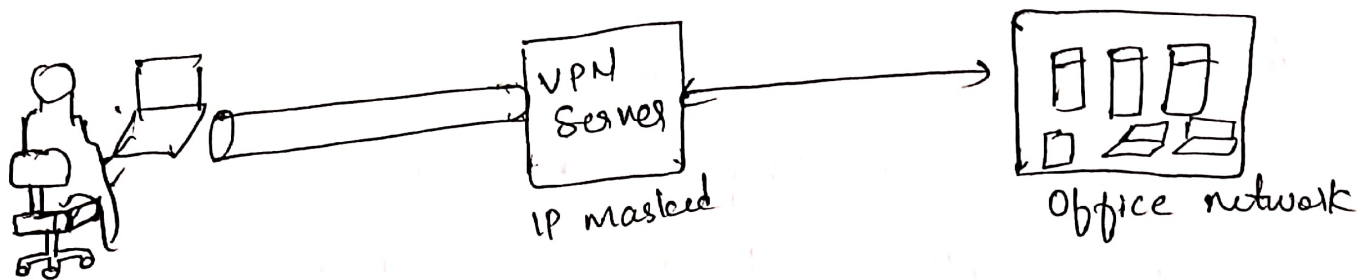
② These devices create a secure, encrypted tunnel between them over public internet - for data transfer & no one can intercept b/w them -



Remote Access VPN

Remote access VPN allows users to connect securely to a private network from a remote location, allowing employees or users to work from home or any location & access data from the company etc safely

* Only a legal employee or user with credentials can connect to private network of company or HQ or server through VPN provided by them ~~through~~ under internet using specific VPN software.



Personal VPN

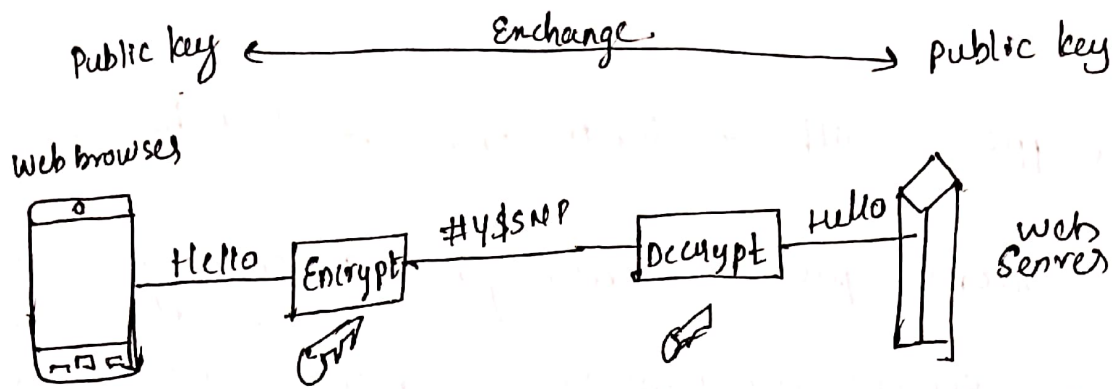
A personal VPN masks the user's IP address & encrypts their internet traffic, making it harder for 3rd parties to track their online activities.

generally used by individual users.

2-10. Explain Security protocols SSL and TLS with a diagram.

SSL

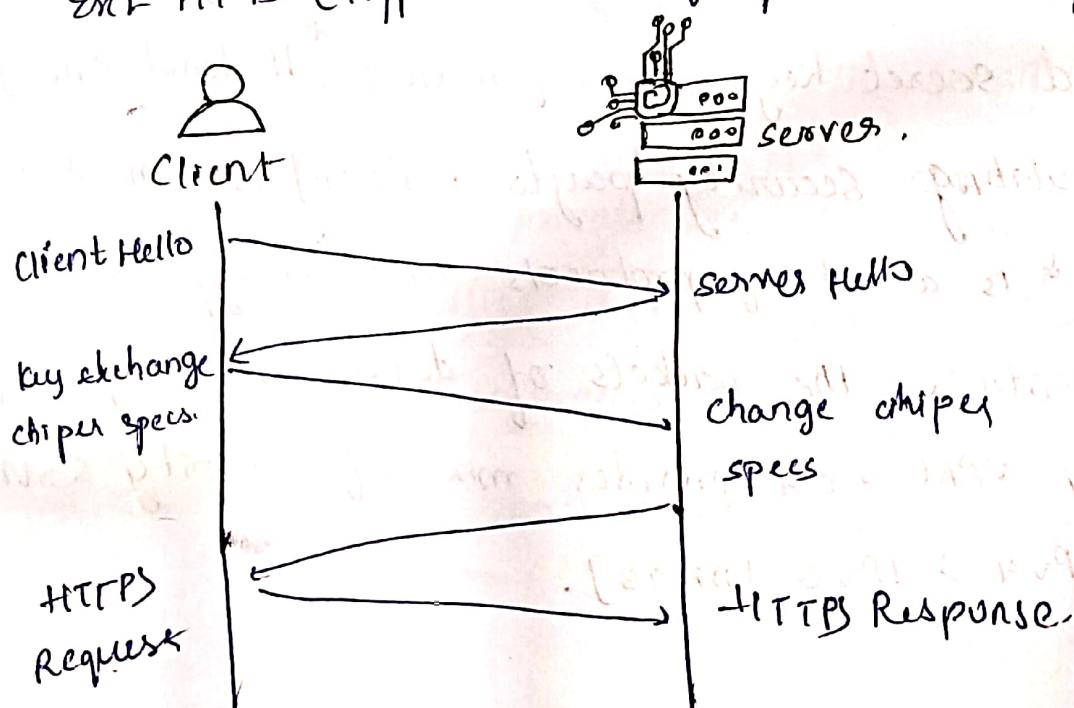
- * SSL stands for Secure Socket Layer is a cryptographic protocol designed to provide secure communication over a network, like internet. used mainly for encrypting data during data exchange between web browser & server.
- * Ensuring all credentials are well protected from unauthorized access.
- * It has symmetric & asymmetric combination of encryption.
- * It is now outdated due to vulnerabilities found in it & replaced by TLS.



SSL protocol

TLS

- * TLS - Transport layer protocol is also a communication & cryptographic protocol designed for secure communication.
 - * It is a ~~super~~ successor to SSL & is more secure & efficient protocol used for encrypting data.
 - * TLS has stronger encryption mechanism than SSL. It is also mainly used to exchange data b/w web browser & server. Also b/w server to server, VPNs, messaging apps etc.
- Ex: HTTPS (Hypertext transfer protocol security).



2.11 Discuss IPsec with Authentication & ESP header

IPsec (Internet protocol Security) is a security protocol used to secure communication over IP networks. It provides confidentiality, integrity & authentication for data at IP layer.

It uses two key methods i) Authentication header (AH)
ii) Encapsulating header (ESP)

Authentication header (AH).

This protocol provides Authentication, data integrity & replay protection. Data integrity is done using MAC algorithm, HMAC-MD5 algorithm. Data

authentication is done by MAC, Digital Signature, Shared secret key, hash function. * It does not Encrypt

Encapsulating security payload (ESP) is a member of IPsec & is a set of protocols that * Encrypt &

* authenticate the packets of data b/w computers using VPN. ESP provides max of security service in IPv4 & IPv6 [DH98].

Q.12 Explain the purpose of S/MIME

[Secure/multipurpose Internet Mail Extension]

* S/MIME is a technology that allows you to encrypt your emails.

* It uses asymmetric cryptography to protect your emails from unwanted access

* provides email authentication, data integrity & confidentiality

* It uses digital signatures, encryption, public key infrastructure

It works as below

* Sender obtains Receiver's public key from digital certificate (usually attached to previous email or directory)

* Data is encrypted.

* Data is hashed to get digest & encrypted (Digital signature)

* Digital signature is attached with email & sent to server

* mail server stores it.

* Receiver using private key decrypts the email & makes its hash

* Receiver verifies digital signature by decrypting digital signature received to get hash.

* It compares hash to verify its integrity & authenticity



NETWORK SECURITY

**Prepared by:
Abdul Muqsith
Prepared for:
C-21**



INTRUSION DETECTION SYSTEM AND FIREWALLS

1.) DEFINE INTRUSION DETECTION SYSTEM

- **IDS (Intrusion Detection System)** is a security system designed to detect attacks, malicious activities, unauthorized access OR anomalies within a network or computer system.
- It helps organizations identify potential threats before they cause significant damage.

1.1) Discuss Infrastructure of IDS.

Main Components of IDS

The infrastructure of IDS includes several key components that work together to detect and respond to threats.

A. Sensors

- Two types of sensors are used i.e. network sensor and host sensor
- Network sensor : used to collect data from data packets and inspect it
- Host sensor: Monitor logs, system processes, and application behavior.

B. Detection Engine

- This is the **brain of IDS**. It analyzes the data collected from sensors to find suspicious activity in real time.
- It uses two main methods:
 - **Signature-Based Detection** – Compares activities with a database of known attack patterns.
 - **Anomaly-Based Detection** – Identifies unusual behavior that might indicate a new attack.

C. Alert System

- If a threat is detected, the IDS sends **alerts** to system administrators.
- Alerts can be in the form of messages, logs, or email notifications.

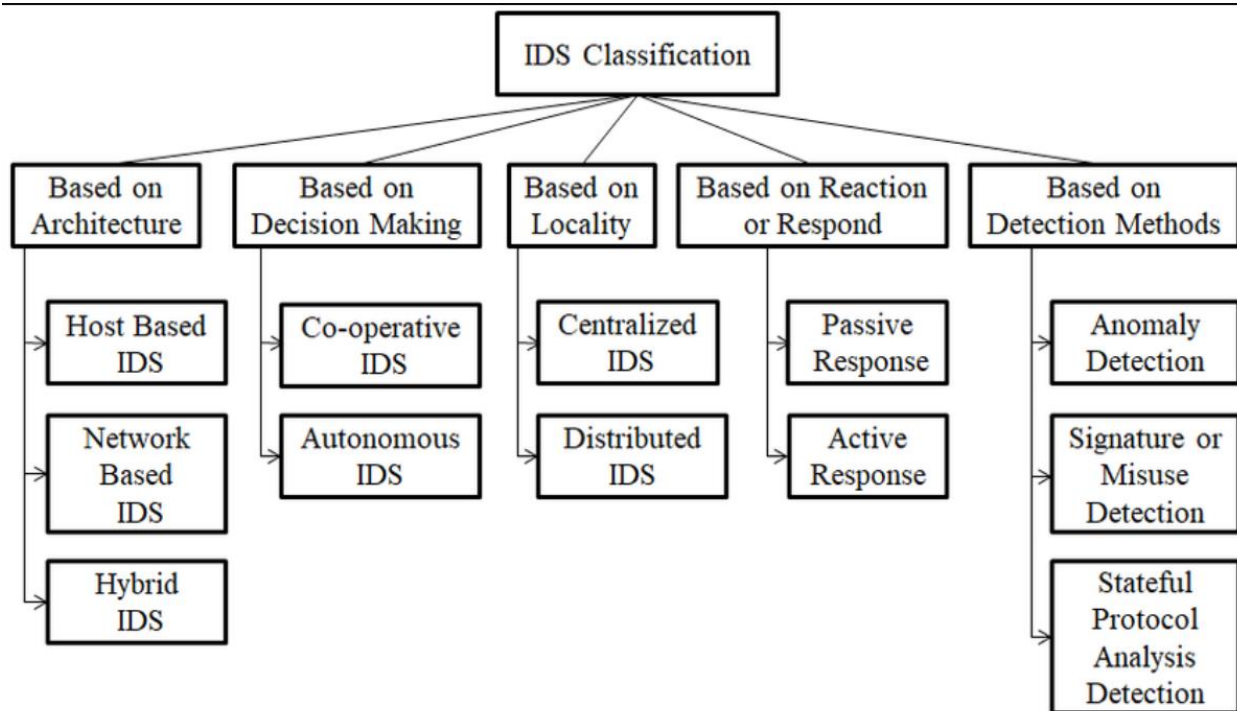
D. Logging and Reporting

- IDS records suspicious activities in log files.

E. Response System

- IDS can take **automatic actions** to stop attacks, such as blocking suspicious traffic.

3.3 Classification of IDS



3.4 Host-Based Intrusion Detection System (HIDS)

A **Host-Based Intrusion Detection System (HIDS)** is a security mechanism that monitors and analyses activities on an individual computer, server, or workstation to detect suspicious behaviour or cyber threats. Unlike a **Network-Based IDS (NIDS)**, which inspects network traffic, HIDS focuses on system-level events and logs.

Structure of HIDS

A typical HIDS setup includes:

- Agent Software** installed on the host machine to gather security data.
- Detection Engine** that analyses the collected data using signature-based or anomaly-based methods.
- Alert System** that notifies administrators about potential threats.

Examples

1. **Tripwire** – A security tool used by companies to detect unauthorised changes to important system files.
2. **AIDE (Advanced Intrusion Detection Environment)** – A simple tool for Linux computers that checks if files have been altered.
3. **Microsoft Defender for Endpoint** – A security tool for Windows computers that helps detect and stop threats.

3.5 Network based IDS

Definition of NIDS

A **Network-Based Intrusion Detection System (NIDS)** is a security solution that continuously monitors network traffic for malicious activities or policy violations. It detects cyber threats such as hacking attempts, malware infections, and Denial-of-Service (DoS) attacks by analyzing data packets flowing through the network.

Structure of NIDS

- **Network Sensors** – Placed at key points (firewalls, routers) to capture network traffic.
- **Detection Engine** – Analyzes data using **signature-based** (known attacks) and **anomaly-based** (unusual behavior) methods.
- **Alert System** – Notifies security teams via email, SMS, or dashboards when a threat is detected.
- **Logging & Reporting** – Records network activities for future investigation and security improvement.

Examples:

Snort , Suricata, Bro (Zeek) , IBM QRadar.

3.6 Differentiate Anomaly based detection and Signature Based Detection.

Feature	Anomaly-Based Detection	Signature-Based Detection
definition	Detects unusual behavior in the system.	Detects attacks by comparing with known attack patterns in a database.
Best For	Catching new, unknown attacks (zero-day threats).	Finding already known attacks (malware, viruses).
False Alarms	More false alarms (normal actions may be flagged as threats)	Fewer false alarms (only detects exact attack patterns)
Speed	Slower, needs time to analyze behavior	Faster, as it just compares with known patterns
Weakness	Can misTakenly flag safe activity	Misses new, modified, or unknown attacks.
Examples	Multiple Incorrect attempts for pins or passwords, monitoring unusual login behavior.	Antivirus software, firewall rules that block known viruses.

- **Normal Behavior Patterns:**
 - Shoppers enter, walk around, buy things, and leave normally.
 - Security cameras watch the usual activities and record them.
- **Anomaly Detection:**
 - If someone suddenly runs inside the mall, starts grabbing items, or enters a restricted area, security detects this unusual behavior.
 - Security guards investigate because it **doesn't match normal shopping behavior**.

Now, let's see this in a simple **network security table**:

Feature	Normal Behavior Patterns (Safe Activities)	Anomaly Detection (Suspicious Activities)
What it means?	Expected and usual network activities	Unusual or unexpected network activities
Example in Network Security	A user logging in from their office at regular hours	A user logging in from another country at midnight (possible hacking)
Traffic Pattern	Consistent, predictable data flow	Sudden spikes in data usage (possible cyberattack)
File Transfers	Normal file sharing between employees	Large amounts of data being sent to unknown locations (possible data theft)
Methods Used	Monitoring regular network activity over time	Intrusion Detection Systems (IDS), AI-based threat detection

Simple Conclusion

- **Normal Behavior = Safe, expected actions.**
- **Anomaly Detection = Finds weird, risky actions.**

feature	Misbehavior Signatures	Signature Detection
Definition	It is a Predefined patterns of malicious or abnormal behavior	A technique used to identify misbehavior by comparing it to known signatures
Purpose	Defines known attack patterns or suspicious activities	Detects security threats by matching against known misbehavior signatures
How it Works?	Stores signatures of attacks, malware, or policy violations	Scans network traffic, logs, or files to find matching attack signatures
Example in Security	A pattern of multiple failed login attempts (brute-force attack)	An intrusion detection system (IDS) detecting repeated failed logins and blocking the attacker
Dependency	Requires prior knowledge of misbehaviors and attacks	It just use the database of known signatures to detect threats
Use Cases	Helps in preparing database for malicious activity	Used in antivirus software, firewalls, and IDS/IPS for real-time threat detection using the database of misbehave signatures

Simple Explanation

- **Misbehavior Signatures = List of known bad behaviors** 📄
- **Signature Detection = The process of finding those bad behaviors** 🔍

Parameter Pattern Matching in Network Security (NS)

Definition:

Parameter Pattern Matching in **Network Security (NS)** is a method used to analyze incoming **data packets, network requests, or system parameters** to detect predefined patterns. These patterns help identify normal behaviors and potential security threats like cyberattacks.

How It Works:

1. Data Collection 📊

- Network traffic, user requests, or system logs are continuously collected for analysis.

2. Pattern Definition

- Security rules (also called **signatures**) are predefined to recognize normal and malicious activity.
- Examples of patterns include:
 - **Known attack signatures** (e.g., SQL injection, brute-force login attempts).
 - **Blacklisted IP addresses**.
 - **Unusual request formats** (e.g., malformed HTTP requests).

3. Matching Process

- The incoming data is **compared** with predefined patterns using detection algorithms.
- If a match is found:
 - The system flags the request as **malicious**.
 - Further actions (blocking, logging, or alerting security teams) are taken.

4. Action Taken

- **If normal:** The data is processed and allowed through.
- **If abnormal:** Security mechanisms take action, such as:
 - **Blocking traffic** (firewalls, Intrusion Prevention Systems - IPS).
 - **Generating alerts** for administrators (Intrusion Detection Systems - IDS).
 - **Logging** the event for further investigation.

How to manage ids

1 Define security requirements

- Decide security goals.

2 Choose IDS Type

- Choose IDS type (**Network-based** or **Host-based**).
- Install IDS software/hardware (e.g., **Snort, Suricata**).

3 Configuration

- Place IDS sensors in key locations (e.g., **before the firewall**).
- Set detection methods (**Signature-based & Anomaly-based**).
- Choose how to receive alerts and logs.

4 Monitoring & Analysis

- Check IDS logs and alerts regularly.
- Investigate any suspicious activity

5 Maintenance & Updates

- Update IDS with new attack signatures.
- Upgrade IDS software regularly

FIREWALL

A **firewall** is a network security system that monitors and controls incoming and outgoing network traffic based on predefined security rules.

- It acts as a barrier between a trusted internal network and untrusted external networks (such as the internet) to prevent unauthorized access, cyberattacks, and malware threats.

List and explain types of firewalls

Proxy Firewall

- Acts as an intermediary between the user and the internet.
- Receives requests, inspects them, and forwards only safe traffic.
- Works at the application layer (e.g., HTTP, FTP).

Software Firewall

- **How it Works:**
 - Installed on individual devices to monitor and control incoming and outgoing traffic.
 - Secures individual system from malicious attacks.
 - Ex: windows defender firewall

Hardware Firewall

A **hardware firewall** is a physical device that acts as a security gateway between an internal network and external networks (such as the internet). It is typically placed at the perimeter of a network to filter incoming and outgoing traffic based on predefined security rules.

Next-Generation Firewall (NGFW)

Firewall that Provides advanced security features like intrusion prevention, deep packet inspection, and malware detection is called next generation firewall.

- Used by large organizations and cloud environments for enhanced security.

Cloud-Based Firewall (Firewall-as-a-Service - FWaaS)

A **Cloud-Based Firewall**, also known as **Firewall-as-a-Service (FWaaS)**, is a security solution hosted in the cloud that protects networks, applications, and devices of users from cyber threats.

- Protects only online networks of devices , offline malware cant be protected like infected device attack

- No need to install in physical device.

Firewall Characteristics

- 1 **Traffic Filtering** – Monitors and controls incoming/outgoing network traffic.
- 2 **Access Control** – Blocks or allows traffic based on security rules.
- 3 **Stateful Inspection** – Tracks active connections for better security.
- 4 **Deep Packet Inspection (DPI)** – Scans packet (including data not just header) content for threats.
- 5 **Intrusion Detection/Prevention (IDS/IPS)** – Detects and blocks cyber threats.

Analyze the importance of firewall

1. Protects system from cyber attack
2. Blocks suspicious traffic
3. Enhance system security
4. Secures network when installed on network perimeters like routers etc
5. Makes more difficult for hackers to hack your system

Explain the steps to design a firewall

1 Define Security Requirements

- Identify threats and risks.
- Set rules for allowed and blocked traffic.

2 Choose Firewall Type

- **Hardware** (e.g., network firewall) or **Software** (e.g., Windows Firewall).
- Decide between **Packet Filtering, Stateful, or Next-Gen Firewall (NGFW)**.

3 Configure Firewall Rules

- Allow only necessary traffic (**whitelist approach**).
- Block suspicious IPs, ports, and protocols.

4 Test the Firewall

- Install the firewall at the **network perimeter (router, gateway, etc.)**.
- Test for **leaks, vulnerabilities, and false positives**.

5 Monitor & Maintain

- Regularly check **logs and alerts**.
- Update firewall rules and security patches.

CH-4 WirelessLAN Security

Discuss different versions of IEEE 802.11.

The **IEEE 802.11** standard defines **Wi-Fi technologies** for wireless communication. Over time, multiple versions have been introduced, improving **speed, range, and security**.

1 IEEE 802.11 (1997) – The First Wi-Fi Standard

- Speed: **2 Mbps**
- Frequency: **2.4 GHz**
- **Limited range and slow speed** compared to modern Wi-Fi.

2 IEEE 802.11a (1999) – Faster but Shorter Range

- Speed: **Up to 54 Mbps**
- Frequency: **5 GHz**
- The **5 GHz band** is used by fewer devices compared to **2.4 GHz**, so there's **less congestion** and **fewer chances of signal disruption**

3 IEEE 802.11b (1999) – Popular Wi-Fi standard

- Speed: **Up to 11 Mbps**
- Frequency: **2.4 GHz**
- **Better range**, but more disruption from devices like microwaves.

4 IEEE 802.11g (2003) – Faster & More Reliable

- Speed: **Up to 54 Mbps**
- Frequency: **2.4 GHz**
- Backward compatible with **802.11b** but with higher speeds.

5 IEEE 802.11n (2009) – Wi-Fi 4 (Better Speed & Range)

- Speed: **Up to 600 Mbps**
- Frequency: **2.4 GHz & 5 GHz (Dual-band)**
- Introduced **MIMO (Multiple Input Multiple Output)** for better performance.

6 IEEE 802.11ac (2013) – Wi-Fi 5 (Super Fast & Efficient)

- Speed: **Up to 6.9 Gbps**
- Frequency: **5 GHz only**
- Supports **MU-MIMO (Multi-User MIMO)** for better multi-device performance.

7 IEEE 802.11ax (2019) – Wi-Fi 6 (Next-Gen Wi-Fi)

- Speed: **Up to 9.6 Gbps**
- Frequency: **2.4 GHz & 5 GHz (Dual-band)**
- More devices, **better efficiency, lower latency.**
- Ideal for **smart homes, IoT, and gaming.**
-

Discuss Wireless LAN components: Radio NIC, Access Point, Router, Repeater.

1. Radio NIC (Wireless Network Interface Card)

- A **Radio NIC (Network Interface Card)** is a hardware device in a computer, laptop, smartphone, or IoT device that enables wireless communication.
- It contains a **radio transceiver** and **antenna** to send and receive data over Wi-Fi.

2. Access Point (AP)

- An **Access Point (AP)** is a device that connects wireless devices to a **wired network**.

3. Router

- A **Router** is a device that connects a local network (home or office) to the **internet**.
- **Functions:**
 - Routes data between devices and the internet.

4. Repeater (Wi-Fi Extender)

- A **Repeater** is a device that **Receives Wi-Fi signals, amplifies them, and re-transmits** them.

Understand WLAN CONFIGURATION



A **Wireless Local Area Network (WLAN)** is a type of network that allows devices to connect and communicate wirelessly using **Wi-Fi** instead of physical Ethernet cables.

WLAN Configuration Means:

It is the **process of setting up a wireless network** device:

1. Set Up the Router or Access Point (AP)

- A **wireless router** or **access point (AP)** is needed to create the WLAN.
- Connect the router to a **modem** (for internet access) or to a **wired network** via Ethernet.

2. Configuring (Wi-Fi Network Name)

- **Set the SSID (Service Set Identifier)** which is the name of the WLAN.
- It should be **unique and easily recognizable**.

3. Security Settings (Encryption & Authentication)

- Use **WPA2** or **WPA3** encryption for **secure connections**.
- Set a **strong password** (Pre-Shared Key, PSK) to restrict access.

4. Frequency Band Selection –

- Choosing between **2.4 GHz**, **5 GHz**, or **6 GHz**

5. IP Address Configuration (DHCP or Static IPs)

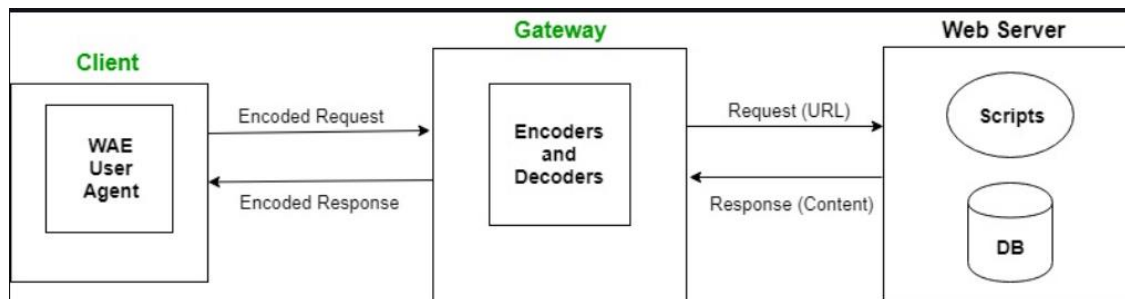
- **DHCP (Dynamic Host Configuration Protocol)** assigns IP addresses automatically.

7. Save & Reboot

- After making changes, **save settings** and **restart the router**.
- Connect devices to the newly configured WLAN using ethernet or wireless media

Understand Wireless Application Protocol (WAP) Architecture.

Wireless Application Protocol (WAP) is a communication protocol used by early mobile phones to access web applications over **wireless networks** (2G, 3G).



- WAP provides a **mini web browser** (microbrowser) that allows users to send web requests.
- The request is sent using **Wireless Hypertext Protocol (WHP)** to the **WAP Gateway**.
- The **WAP Gateway** translates the WHP request into an **HTTP request** and forwards it to the **web server**.
- The **web server processes the request** and sends an **HTTP response** back to the WAP Gateway.
- The WAP Gateway **converts the response into WHP/WML format** and sends it to the mobile device.
- The mobile browser **displays the content** in a format optimized for small screens.

Summarize Wireless Application Protocol (WAP) stack

is a layered architecture that enables wireless devices, such as mobile phones, to access the internet and other network services efficiently. It consists of the following key layers:

1. **Application Layer** – Uses WML (Wireless Markup Language) and WMLScript, similar to HTML and JavaScript, for displaying content on mobile devices.
2. **Session Layer** (it uses **WSP - Wireless Session Protocol**) – Manages connections between the client and server
3. **Transaction Layer** (it uses **WTP - Wireless Transaction Protocol**) – It makes sure the request from your mobile phone reaches the server and gets a response if needed.
4. **Security Layer** (it uses **WTLS - Wireless Transport Layer Security**) – Provides data encryption, authentication, and integrity, similar to TLS in traditional internet communication.
5. **Transport Layer** (it uses **WDP - Wireless Datagram Protocol**) – Acts as the interface between WAP services and different wireless networks (like GSM, CDMA), making WAP adaptable to various transport technologies.

WAP Security Requirements

Wireless networks are more vulnerable to attacks than wired ones, so **WAP security** is crucial to protect data. The three main security requirements in WAP are **Authentication, Integrity, and Confidentiality**.

1. Confidentiality

- ◆ Ensures that only **authorized users** can read the data.
- ◆ Prevents eavesdropping by hackers.

How it works in WAP?

- Uses **encryption** (like AES, DES) to encrypt data so that only the authorised recipient can read it.
- WTLS encrypts data before sending it over the network.

2. Authentication

- ◆ Ensures that the sender and receiver are **who they claim to be**.
- ◆ Prevents attackers for pretending them as authorized users.

✓ **Example:** When logging into a banking app, the server checks your username and password to verify your identity.

How it works in WAP?

- Uses **WTLS (Wireless Transport Layer Security)** for authentication.
- Can use digital certificates and cryptographic keys.

3. Integrity

- ◆ Ensures that data is **not altered or tampered with** during transmission.
- ◆ Protects against unauthorized modifications or corruptions.

How it works in WAP?

- Uses **message hashing** (e.g., SHA, MD5) to create a unique digital fingerprint of the data.
- If the hash doesn't match at the receiver's end, it detects tampering.

Wireless Transport Layer Security (WTLS)

WTLS is the **security layer of WAP** that protects data while being transmitted over wireless networks. It works similarly to **TLS (Transport Layer Security)**

Why is WTLS Needed?

Wireless networks are more vulnerable to:

- ✓ **Eavesdropping** (Hackers monitoring data transmission)
- ✓ **Data Tampering** (Changing messages during transfer)
- ✓ **Impersonation Attacks** (Fake users pretending to be real ones)

WTLS **protects against these threats** by providing **encryption, authentication, and data integrity**.

How WTLS Works – Step by Step

💬 Imagine you're sending a **secure server request** via a WAP-enabled mobile app:

1 Handshake Process 🤝

- The mobile device and server exchange security information like digital **certificates or secret keys**. (ensures authenticity)

2 Encryption Starts 🔒

- Data is **encrypted** before being sent over the network.
- If a hacker intercepts it, they only see unreadable text (ciphertext). (ensures confidentiality)

3 Integrity Check 🛡️

- A **hash value** (part of digital signature (irreversible encryption)) is attached to the message.
- The receiver checks it by comparing received hash with the hash generated by receiver with received message to ensure **data wasn't changed**.

4 Decryption & Data Use ✓

- The receiver decrypts the message and confirms its authenticity.

Illustrate WLAN Authentication Process

WLAN (Wireless Local Area Network) Authentication means **granting connection for authorized devices with WLAN network in order to access internet**

Types of WLAN Authentication:

1 Open System Authentication (OSA) – No Security

- Any device can **connect freely** without verification.
- Used in **public Wi-Fi** networks (e.g., cafes, airports, malls).
- **No encryption**, making it vulnerable to security threats.

2 shared key authentication (SKA)

- When you connect to WLAN, you select the **WLAN (SSID-service set identifier)** and enter a **password**.
- The **Access Point (router)** checks if the password matches the one stored in its settings.
- If correct, the AP **grants access and connects you to the internet** via broadband.
- **This is called WPA2/WPA3-Personal (PSK Mode)** because it uses a **Pre-Shared Key (PSK)** for authentication.

Discuss security measures

1. SSID Hiding

The Service Set Identifier (SSID) is the name of a wireless network. By default, WLANs broadcast their SSID, allowing nearby devices to detect and connect. However, hiding the SSID prevents the network name from being advertised, making it less visible to casual users.

2. MAC Address Filtering

Media Access Control (MAC) filtering :based on device MAC addresses network access is given. Only pre-approved devices with specified MAC addresses can connect.

Wired Equivalent Privacy (WEP)

WEP was one of the first security protocols developed for WLANs to provide encryption. However, it has significant weaknesses due to its static encryption keys and vulnerabilities in the RC4 encryption algorithm.

. Wi-Fi Protected Access (WPA2/WPA3)

WPA2 and WPA3 are modern security protocols that provide enhanced encryption and authentication.

- **WPA2:** Uses AES encryption, offering strong security but vulnerable to brute-force attacks if weak passwords are used.
- **WPA3:** Introduces Simultaneous Authentication of Equals (SAE) for better protection against brute-force attacks and forward secrecy to secure past communications even if credentials are compromised.

. Temporal Key Integrity Protocol (TKIP)

TKIP was introduced as an improvement over WEP, providing dynamic key changes and integrity checks. However, it is now considered obsolete and less secure than AES.

Lightweight Extensible Authentication Protocol (LEAP)

LEAP was developed by Cisco as an authentication protocol but is now considered weak due to vulnerabilities in its password-based authentication.

Protected Extensible Authentication Protocol (PEAP)

PEAP enhances security by encapsulating authentication within a TLS (Transport Layer Security) tunnel. It prevents direct exposure of credentials, reducing the risk of attacks.

Discuss few best practices to safeguard Wireless LAN

Use Strong Encryption (WPA3 or WPA2-AES)

- Always enable **WPA3** (if supported) or **WPA2 with AES encryption**.
- Avoid outdated protocols like WEP and WPA with TKIP, as they are highly vulnerable.
- Ensure all connected devices support modern encryption standards.

Change Default SSID and Disable SSID Broadcasting

Set strong passwords

Ch-5 WEB SECURITY

5.1 Explain Client / server architecture

Client/Server Architecture is a model used in network computing where multiple clients (users or devices) request and receive services from a centralized server.

1. Client:

- A device or program that sends a request to the server.
- Examples: Web browser, mobile app, or a computer requesting a web page.

2. Server:

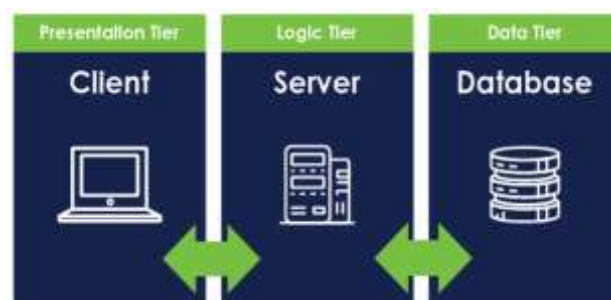
- A powerful system or software that provides services or resources to clients.
- Examples: Web server, database server.

Types of Client-Server Architectures

1. Two-tier architecture: Client and server are the only two tiers.
2. Three-tier architecture: Client, application server, and database server are the three tiers.

CLIENT/SERVER ARCHITECTURE

- Client is used to send request to server
- User using client services like web browser sends the request like login, submit, access data etc to server through public/private network.
- Server here check authenticity of user and if user is authorized it analyses what user want and send query to database server for accessing data
- Database response
- Server response
- web



This Photo by Unknown Author is licensed under [CC BY-NC](#)

server sends
to server
gives back web
to user through
interface (browser).

5.2 DISCUSS WEBSECURITY CONSIDERATIONS AND THREAT

Web security is all about **protecting websites, web applications, and data** from being accessed or manipulated by unauthorized users (attackers). It ensures **confidentiality, integrity, and availability** of web systems.

Web Security Considerations (Things to Keep in Mind):

These are practices and technologies to protect web systems:

1. Authentication & Authorization

- Make sure only authorized users can access certain areas.

2. Data Encryption

- Use HTTPS (SSL/TLS) to encrypt data during transmission.
- Protect sensitive data like passwords and credit card info.

Threats : possibility of following attacks

Threat	Description
SQL Injection	Attacker sends harmful SQL queries to access or modify database.
Cross-Site Scripting (XSS)	Injects malicious scripts into web pages to run in other users' browsers.

5.3 LIST AND Explain Web Traffic security approaches

Web Traffic Security refers to methods used to **protect data as it travels between users (clients) and web servers** over the internet

Web Traffic Security Approaches:

1. HTTPS (Hypertext Transfer Protocol Secure)

- **What it does:** Encrypts the communication between browser and server using **SSL/TLS** protocols.
- Protects against man-in-the-middle attacks and eavesdropping.
- **Example:** <https://www.example.com> is secure, while <http://www.example.com> is not.

2. SSL/TLS (Secure Sockets Layer / Transport Layer Security)

- **What it does:** Provides encryption and authentication for data transmission.
- Uses digital certificates to establish a secure session between client and server.
- **Note:** TLS is the modern version of SSL (SSL is outdated).

Discuss twin concepts SSL connection and SSL session

SSL Connection

- A **secure temporary communication link** between a client and a server.
- It's **temporary** — created for one data exchange (like loading a webpage).
- It is used for handshake between client and server & It **transfers encrypted data**.

SSL Session

- A **longer-lasting secure relationship** between the client and server.
- Stores information like encryption settings and keys, digital certificates.
- It can be **reused** for multiple SSL connections to **save time** (no need to re-handshake every time).

LIST the parameters of SSL SESSION STATE

Following parameters defines ssl session state: all about id, certificate, keys, cipher, keys, version of protocols, algorithms

#	Parameter	Description
1	Session ID	A unique identifier code assigned for the SSL session.
2	Peer Certificate	The certificate of the peer (either the client or server).
3	Cipher Suite	The encryption algorithm and key exchange protocol used for the session.
4	Master Secret	It's used to generate session keys — like encryption keys, MAC keys, etc.

Parameter	Description
Session ID	The identifier of the SSL session associated with the connection.
Cipher Suite	The encryption algorithm and key exchange protocol used for the connection.
Protocol Version	The version of the SSL/TLS protocol being used.
Key Exchange Algorithm	The algorithm used for exchanging keys between the client and server.
MAC Keys	The keys used for generating and verifying message authentication codes (MACs). Client /server uses their own key

5.7 Discuss SSL Record Protocol

The SSL Record Protocol is responsible for securing and formatting application data before it's transmitted over the network. It ensures confidentiality, integrity, and reliability.

Done before sending to handshake protocol

1. Fragmentation

- Breaks data into manageable blocks (max 16 KB). Like data packets

2. Compression (*optional*)

- Compresses data to reduce size before encryption.

3. MAC (Message Authentication Code) Addition

- Adds a MAC to ensure data integrity (data prevention from alteration)

4. Encryption

- Encrypts the data (and MAC) using symmetric encryption. Ensures confidentiality.

5.8 Discuss SSL Handshake Protocol

 **What is the SSL Handshake Protocol?**

It is protocol responsible for establishing trust between the client and server, decides encryption parameters (such as which algorithms and versions to use), and securely generating shared keys that will be used to encrypt and authenticate data during the session.

- It ensures both parties are ready to communicate
- Used in web protocols, database connections ,API service & cloud service

Key features:

- Handshake protocol provides Authentication that both parties(client and server) are trusted through digital certificate exchange
- **Securely exchange** or generate a shared secret key
- **Decides encryption algorithm and version of protocol**

Important Steps in SSL Handshake

1. **Client Hello** – Initiates handshake, sends supported versions and cipher suite.
2. **Server Hello** –Server responds with chosen cipher ,version, and certificate..
3. **Server Certificate** – Server sends its digital certificate for identity verification.
4. **Client Key Exchange** – Client sends encrypted Pre-Master Secret.
5. Encryption and MAC keys are generated.

5.9 What is S-HTTP (Secure Hypertext Transfer Protocol)?

Secure Hypertext Transport Protocol (S-HTTP) was a protocol designed to provide secure communication over the web. It is better than **HTTP**, as it sends data in **encrypted** form so that unauthorized parties couldn't read it.

Key Points:

1. **Confidentiality:** : S-HTTP encrypted the data to ensure that the communication between the client and server was secure, as data was encrypted , no one can understand it .
2. **It supports multiple encryption** methods, such as RSA, DES, etc.
3. **Message Integrity:** S-HTTP also ensures that data is not altered during transmission. This is achieved by using techniques like message authentication codes (MACs) to verify that the received data is unchanged.
4. **Message-level security:** S-HTTP encrypted the entire message, including headers and body, which means security was applied at the message level, but do not protects entire session data .
5. Encryption in S-HTTP **was optional**. Both the client and server had to agree whether they wanted to use encryption or not.

5.10

What is Secure Electronic Transaction (SET)?

SET is a protocol developed by major companies like **Visa** and **MasterCard** in the late 1990s to ensure secure online credit card transactions. It was designed to provide confidentiality, integrity, and authentication in electronic payment systems.

Business Requirements for SET:

SET was created to address the following business needs:

1. **Security** – Ensure that transactions are secure and can't be intercepted or altered by attackers.
2. **Authentication** – Verify the identity of both the cardholder (buyer) and the merchant (seller).
3. **Privacy** – Protect the sensitive information like credit card details from unauthorized access.
4. **Non-repudiation** – Guarantee that the parties involved cannot deny the transaction once it's completed.

SET participants**Main People Involved in a Secure E-Transaction (SET):**

1. **Cardholder (Buyer):**
2. **Merchant (Seller):**
3. **Issuer:** The buyer's bank or credit card company
4. **Acquirer:** The seller's bank
5. **Certificate Authority (CA):** Confirms if both buyer and seller are genuine by giving digital certificates

SET Transaction Flow:

1. **Cardholder Initiates Transaction:**
 - The cardholder (buyer) selects items for purchase on the merchant's website.
 - The cardholder's browser sends a request to the merchant's server.
2. **Merchant Sends Invoice (BILL):**

- The merchant's server generates an invoice (including the total cost, item details) and sends it to the cardholder's browser.
- The invoice is digitally signed by the merchant to ensure authenticity.

3. **Cardholder Sends Payment Information:**

- The cardholder's browser then prepares the payment message. This includes:
 - The **payment information** (credit card number, expiration date)
 - A **secure digital signature**.
 - The payment details are **encrypted** to ensure confidentiality.
-

4. **Payment details Goes to Bank:**

- The buyer's payment details (encrypted) are forwarded to the buyer's bank through.

5. **Buyer's Bank Checks and Approves:**

- The buyer's bank checks if the card details are correct and if there's enough money.
- If all looks good, they send an approval message back to the seller's bank, then to the seller.

6. **Seller Confirms the Order:**

- Once the seller gets approval, the order is confirmed.
- The buyer gets a message saying the payment and order were successful.
- Both buyer and seller get digital receipts for record.

7. **Done Deal – Payment Finished:**

- The money is moved from the buyer's account to the seller's account.

CH-6 Security and Law, Internet Governance and Email Policy

6.1 Discuss the importance of Cyber security.

Cybersecurity refers to the practice of protecting systems, networks, applications and data from digital attacks. In today's world, cybersecurity is the most important need for citizens, businesses, and governments.

- Nowadays everything is became **online from entertainment to payment, from shopping to business and from manufacturing to marketing**. etc as we are dependent on cyber devices and internet much so their must be highly protection of our transaction details, login credentials and personal information stored in our mobiles, cloud or in servers
- As dependency on cyber devices increases there is a high possibility **of data breaches** , cyber attacks etc done by hackers **in-order to get data of users and gain unauthorized control on authorized user's applications** which can lead to digital arrest, money theft etc
- These hackers can also perform **terrorist attacks on government servers**, applications and military data base which can ,lead to NATIONWIDE INSECURITY .
- Due to ABOVE reasons we need cybersecurity engineers to safeguard networks, transactions, communications, databases etc.

6.2 Understanding Cybersecurity Vulnerability

A **cybersecurity vulnerability** is a weak point in a computer, network, or software that hackers can use to attack or steal information.

Key Aspects of Cybersecurity Vulnerabilities:

1. Types of Vulnerabilities:

- Software Bugs:** Errors in code that can be cause system faults (e.g., buffer overflows).
- Outdated Software:** Lack of updates makes hacker easy to attack due to outdated securities in it.

- iii. **Weak Passwords:** Easily guessable or reused passwords make systems vulnerable.
- iv. **Unsecured Networks:** Open public Wi-Fi or poor firewall settings can be entry points for attackers.

2. Common Vulnerability Examples:

- **SQL Injection:**
Hackers attack the **database** by typing special code into input boxes (like login forms). This can let them **see, steal, or delete** important data.
- **Cross-Site Scripting (XSS):**
Hackers add **bad scripts** (malicious code) to a website. When a user visits the site, the script runs and may **download malware** to their device without them knowing.
- **Phishing:**
Hackers **pretend to be trusted people** (like bank staff, police, or government officers). They send fake emails or messages to trick people into **sharing passwords, OTPs, or personal info**.

6.3 Common Types of Cyber Threats (Summary)

Cyber threats are dangers that try to damage computers, networks, or steal data. Here are some of the most common types:

1. Malware

Malicious software like **viruses, worms, trojans**, or **spyware** that harms your computer or steals your information.

2. Phishing

Fake emails, messages, or websites used by hackers to trick you into sharing **passwords, OTPs, or personal details**.

3. Ransomware

A type of malware that **locks your files** and asks for money (ransom) to unlock them.

4. Denial of Service (DoS) Attacks

Hackers flood a website or server with too much traffic so it **crashes or becomes slow**.

5. Man-in-the-Middle (MitM) Attacks

Hackers secretly **intercept communication** between two people or systems to **steal data**.

6. SQL Injection

Hackers use special code to attack **databases** and steal or change stored information.

7. Cross-Site Scripting (XSS):

Hackers add **bad scripts** (malicious code) to a website. When a user visits the site, the script runs and may **download malware** to their device without them knowing.

What is OWASP?

OWASP means Open Web Application Security Project.

It is a non-profit group that helps make websites and software more secure. By revealing risks

🛡️ OWASP Top 10 – 2021

Here are the top 10 web application security risks from OWASP for 2021:

🌐 OWASP Top 10 – 2021 (Simple & Indian Style Explanation)

1. **Broken Access Control**
 - People can access things but actually they shouldn't have to give access.
(Example: Normal user can see admin info)
2. **Cryptographic Failures**
 - Weak or no encryption makes Easy for hackers to steal data like passwords, credit card numbers, etc.
3. **Injection**
 - Hacker insert malicious codes (like SQL) into forms or links to steal or change data.
4. **Insecure Design**
 - App is not properly planned in security aspect.
5. **Security Misconfiguration**
 - Wrong or lazy settings. Like open admin panel, default passwords, etc.
6. **Vulnerable and Outdated Components**
 - Using old or unsafe software parts. Hackers can easily break in.
7. **Identification and Authentication Failures**
 - Login system is weak. No OTP, weak passwords, etc.
8. **Software and Data Integrity Failures**
 - Trusting unverified updates or third-party code which may be hacked.
9. **Security Logging and Monitoring Failures**
 - No system to catch or report attacks. Attack happens and no one knows.

6.5 Cyber Security Safeguards (Short & Simple)

Cybersecurity safeguards are **protective steps** to keep data, devices, and systems safe from hackers and attacks.

1. Strong Passwords

- Use complex passwords with numbers, symbols, and capital letters.
- Change them regularly.

2. Antivirus & Firewall

- Install antivirus to block malware.
- Firewalls help control incoming and outgoing traffic.

3. Regular Updates

- Keep your software, apps, and OS updated to fix security bugs.

4. Avoid Phishing

- Don't click on unknown links or emails asking for OTPs or personal info.

5. Backup Data

- Always keep a copy of your important data in case of attack or loss.

6.6 CIA Security Triad Model

The **CIA Triad** is a basic model in cybersecurity that helps protect data and systems. **CIA** stands for:

CIA Security Triad Model

1. C – Confidentiality

Definition:

Confidentiality ensures that **unauthorized persons are prevented from reading** information that is traveling across networks or stored in applications, databases, or cloud systems.

Goal:

Only **authorized people** should be able to access the data in communication or storage.

Ensured by:

- **Encryption**
- **Data classification**
- **Access control**
- **Advanced cryptographic methods**

Example:

No person except the **sender and receiver** should be able to see the communication between them.

2. I – Integrity**Definition:**

Integrity ensures that **unauthorized persons cannot modify** information during transmission or when stored in databases, applications, or cloud systems.

Goal:

Only the **right and authorized users** should be allowed to alter the data.

Ensured by:

- **Digital signatures**
- **Checksums**
- **Message Authentication Code (MAC)**
- **Pretty Good Privacy (PGP)**

Example:

No one except **authorized users** should be able to change the content stored on any digital platform.

3. A – Availability**Definition:**

Availability ensures that **data and services are always accessible** to authorized users — anytime, anywhere, and on any allowed device — even in adverse conditions.

Goal:

Authorized users should be able to access the system **without delay or failure**.

Ensured by:

- **DoS / DDoS defense systems**

Example:

A website or service should remain available even if many users access it at once, or during a **DoS / DDoS attack**.

6.7 Summarize open source cyber security tools.

What are Open Source Cybersecurity Tools?

Open source cybersecurity tools are security software that are **freely available** and their **source code is open to everyone**.

Tool Name	Use / Purpose
Wireshark	Monitors entire network packets and analyze them
Nmap	Scans the network ports to finds open ports ,O.S and other information
Kali Linux	A full OS with hacking tools — used by ethical hackers and cybersecurity experts
Snort	Network Intrusion detection system (IDS) — finds threats in network traffic
OSSEC	Host-based Intrusion Detection System (HIDS) — monitors system logs
Dumpsec	Used to identify files and folders permissions, user accounts ,services etc
Free firewall	A firewall with various configurations

6.8

What is Blockchain?

Blockchain is a **distributed ledger** technology (DCT) or **database** that stores information in a **chain of blocks**. where each block is a individual computer or server database

- Data is not stored in a centralized system ,instead data is stored in various distributed systems called blocks. **(DE-CENTRALIZED)**
- Each and every block are interconnected with each other **(CHAINING)**
- Once data is stored in this blockchain its almost impossible to change or delete it. **(IMMUTABILITY)**

HOW is applicable in CYBER SECURITY?

Why not ,in every scenario its following principles of cybersecurity

1. **(CONFIDENTIALITY) Secure Data Storage:** Decentralization makes it much harder for hackers to attack ,Since data is **distributed** across many computers, it's **difficult to tamper with**.
2. **DATA INTEGRITY:** data is highly protected from tampering as once data is entered into blockchain system its NEARLY impossible and much complicated to change it even for legal entities also.
3. **AUTHENTICATION :** data is accessible only for legal verified entities
4. **Anti-Fraud & Anti-Counterfeiting :**Blockchain keeps a **permanent record** of every step in the journey of a product or a transaction.

6.10 Define **Cyber Crime**:

It is an illegal activity done using the internet or digital platforms, aiming to **steal data or money, hack systems or servers, access unauthorized data**, or even **blackmail people digitally**.(digital arrest).

6.9 C-DAC Services with Examples

1. **NAYAN (Network Analysis for Yuva Awareness and Nurturing)**
 - A real-time **video surveillance and analytics system** used for monitoring.
 - Example:** police command centre Hyderabad.

-
2.  **GYN (Government e-Yantra Network)**
 - A platform for **secure communication and file exchange** within government.
 - Example:** Government officers use GYN to send confidential files between ministries safely.
-

3.  **CHAKRA (Cyber Swachhta Kendra)**
 - Provides **malware detection and removal tools** for common users.

Example: A user downloads a tool from CHAKRA to clean their infected laptop.

4. **DARPAN S3**

– A framework for **building secure e-governance websites and apps.**

Example: Digilocker, mAdhaar, GOVT banking etc.