Chapter 1
Introduction and Basic concepts

Er. Shiva Ram Dam

Assistant Professor

Gandaki University

Google class code

- yvneddb

Content:

1. **Basic concepts**
   - ❑ Networking Refresher (The OSI Layer, The TCP/IP Model, Subnetting)
   - ❑ Encryption and Cryptography basics (E2EE, Hashing, Hashing Techniques, the CIA triad, concepts on steganography and cryptocurrency)
2. **Data Backup concepts**
   - ❑ Storage Fundamentals (Understanding File Systems: FAT16, VFAT, FAT32, NTFS, EXT4)
   - ❑ Basics of Data Backup and Restore, the 3-2-1 backup rule, RAID, Disaster Recovery and High Availability
3. **Proprietary and Open-source Systems**
4. **Introduction to Digital Forensics**

1.1 Basic Concepts

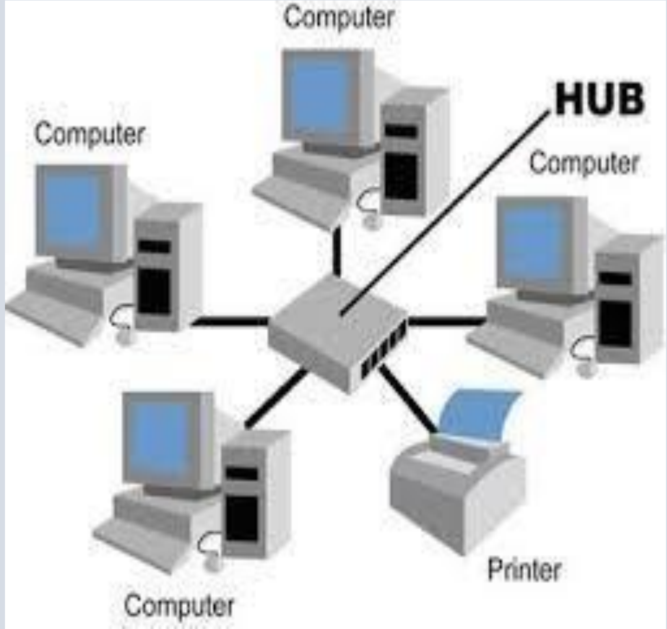
1.1 Basic Concepts

- Networking Refresher
  - The OSI layer
  - The TCP/IP Model
  - Subnetting
- Encryption and Cryptography basics
  - E2EE,
  - Hashing,
  - Hashing Techniques,
  - the CIA triad,
  - concepts on steganography and cryptocurrency)

1.1.1 Networking Refresher

Concept of Computer Network:

- A computer network can be defined as **interconnection between two or more computers so that they can interchange information between them.**
- The connection between the separate computers can be done via a copper wire, fiber optics, microwaves or communication satellite.



Advantages and Disadvantages of Computer Network:

Advantages:

1. **Resource Sharing**

   With computer network, we can share hardware, software and data. For eg: a printer can be shared among many computers in a network.

2. **Communication**

   We can send message, chat, make video call, make teleconference via computer network. Eg: email is possible through computer network. Many applications like viber, skype, whatsapp,etc. can communicate because of computer networking.

3. **Backup and Recovery**

   Data can be stored redundantly in different computers in a network. In case of failure of a single computer, data can be recovered from other computers.

4. **Centralized control**

   Many computers are connected to the server and this server can control other computers.

5. **Flexible access**

   Computer network allows us to access our data from anywhere we go. For eg: we can use our Facebook from any devices and from any place.

6. **More Storage capacity**

   Computer network helps share our hard-disk. So, this collectively increases the storage capacity.

Disadvantages:

1. **Security threat**

   Hackers and other intruders can attack on our data. There are many cyber crimes such as software piracy, hacking, plagiarism, pornography, spoofing, etc.

2. **Rapid virus spread**

   Spreading of virus is only possible when computers are on network.

3. **Expensive initial setup**

   To establish a computer network is complex, difficult and hence requires more cost to set up initially.

4. **Need of technical manpower**

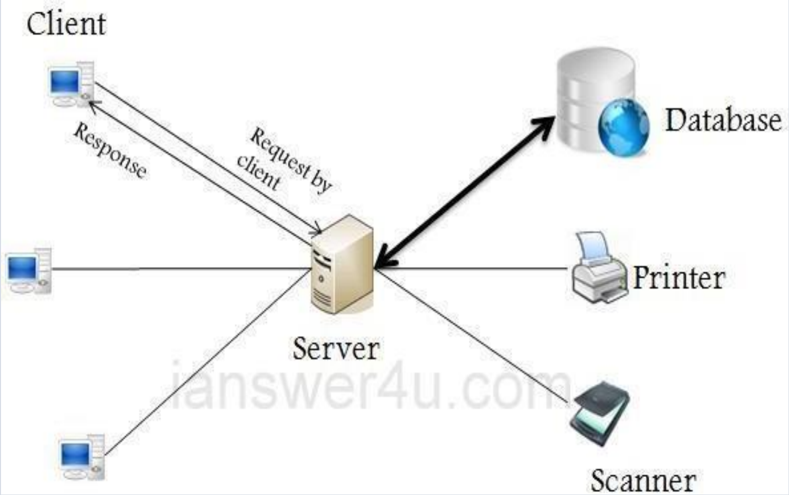
   It requires skilled technical manpower to set, maintain and operate computer network.

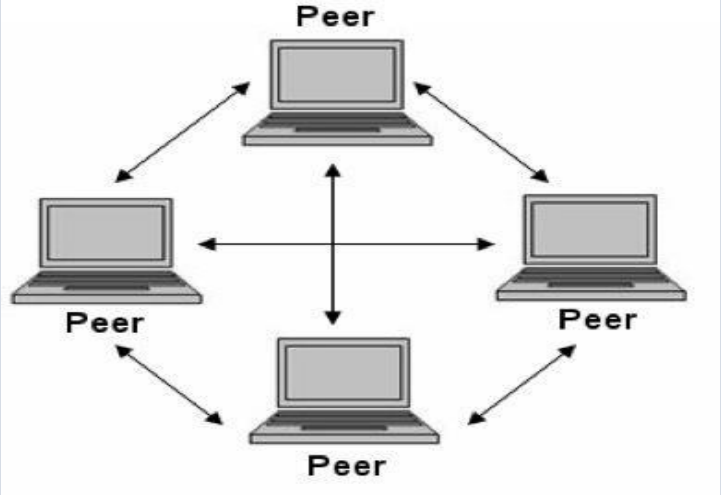
5. **Dependency on server**

   Client computers depend on server. If the server fails, the computer network is affected.

Network Architecture:

- Network architecture refers how the computer communicates or interacts with each other in a computer network.
- On the basis of Network architecture, computer network are of two types:
  1. Client-Server Architecture
  2. Peer-to-peer Architecture





Client-Server Architecture

- Client-Server architecture consists of at least one dedicated server and other client computers. The client requests services to the server.
- The server provides services to the clients.
- Servers are powerful computer or processor dedicated to managing the disk drive, printer or network traffic. Clients are less powerful Pc or workstation on which users run application. Client rely o server for resources such as files, deices and even processing power.

Advantages:

- Centralized administration is possible through the network.
- High security can be provided by using appropriate server.
- Good for large organization having large number of computers.
- Data recovery and backup process is easier

Disadvantages:

- Expensive due to dedicated servers
- Complex to establish and manage.
- Requires experienced and skilled manpower to manage.
- If server fails, network is affected.

Peer-to-peer Architecture

- It is the network architecture where there is no server and clients. All the computers have equal authority to access data.

Advantages:

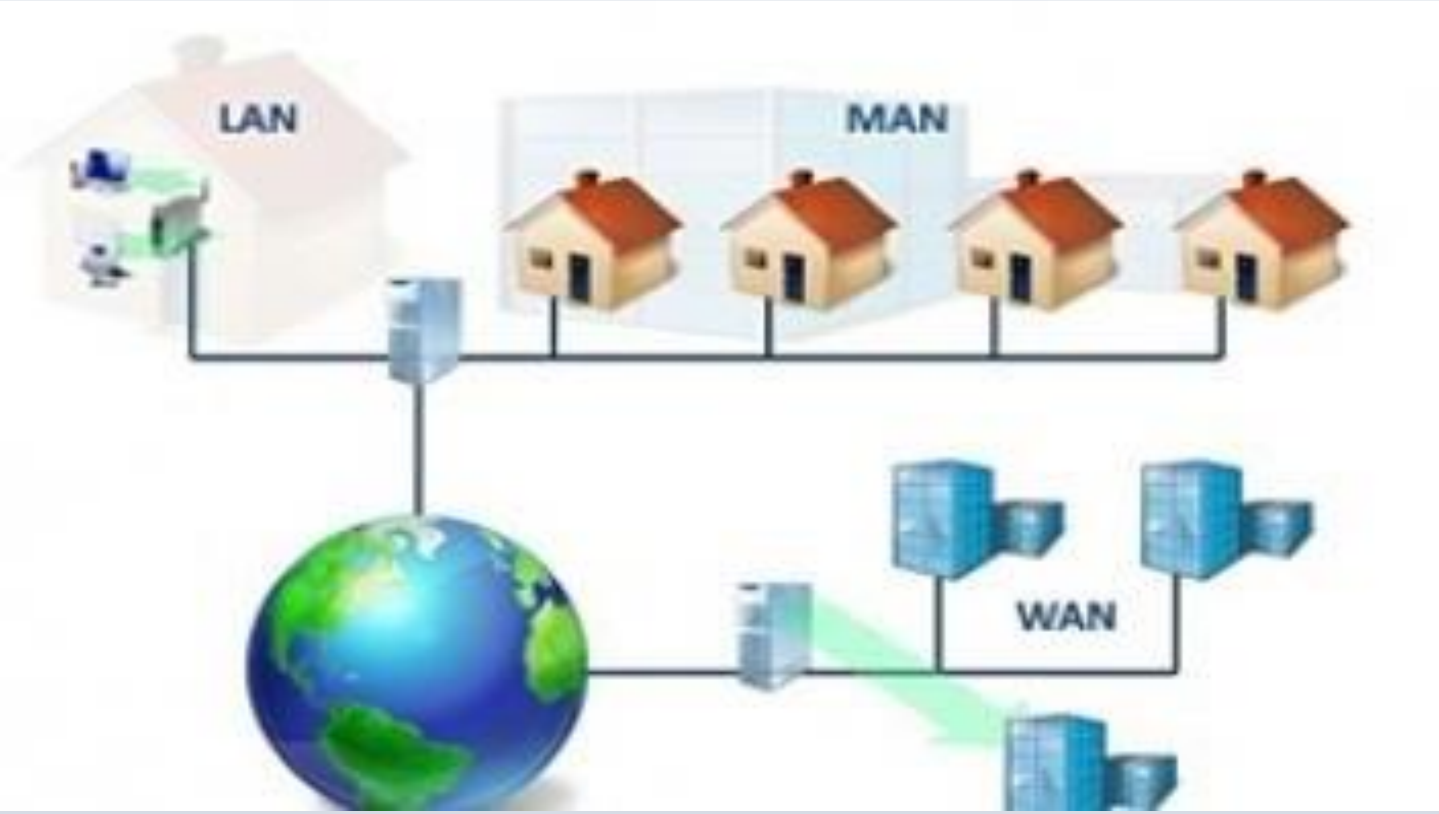
- Simpler and easier to setup.
- Implementation and managing is cheaper.
- Failing of one computer does not affect other computers

Disadvantages:

- Network administration is difficult.
- Data security is poor.
- Data backup and recovery is difficult.
- Not appropriate for large organization having more computers.

Types of Network

- LAN
- MAN
- WAN

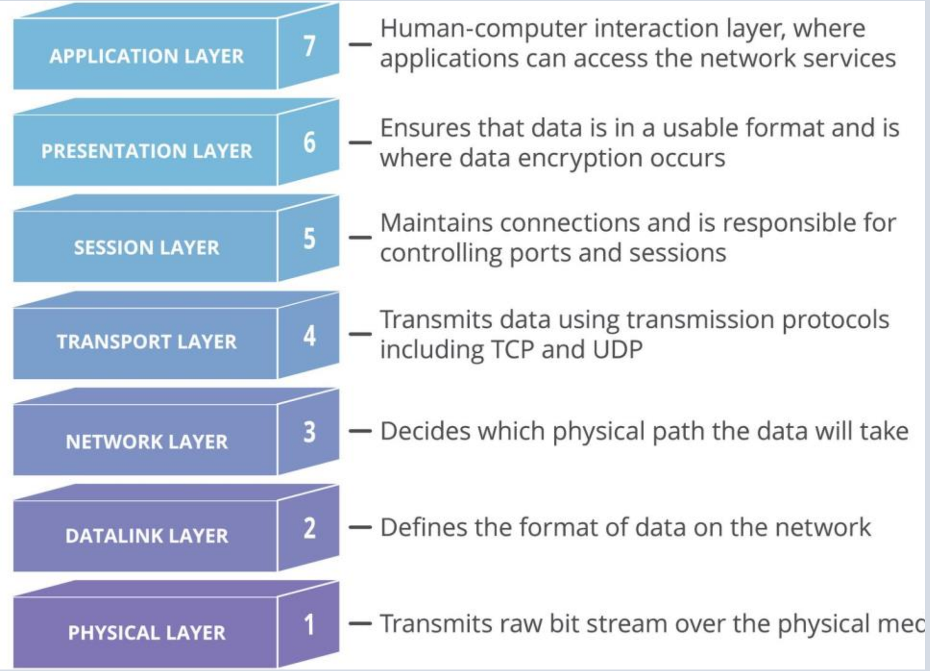


Network Reference Model

- A reference model is a **conceptual layout that describes how communication between devices should occur.** It defines standard for building network components and protocols.
- The two most important reference models are:
  1. The OSI Reference Model
  2. The TCP/IP Reference Model

A) OSI Reference Model

- **OSI stands for Open Systems Interconnection**, where open stands to say non-proprietary.
- It is a 7-layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.
- The OSI reference model was developed by **ISO – 'International Organization for Standardization**', in the year 1984.
- The OSI model provides a **theoretical foundation** for understanding **network communication**. It is a conceptual framework to understand how different networking protocols interact.
- However, it is usually not directly implemented in its entirety in real-world **networking hardware** or **software**.
- Instead, **specific protocols** and **technologies** are often designed based on the principles outlined in the **OSI model** to facilitate efficient data transmission and networking operations.



APPLICATION LAYER 7 – Human-computer interaction layer, where applications can access the network services

PRESENTATION LAYER 6 – Ensures that data is in a usable format and is where data encryption occurs

SESSION LAYER 5 – Maintains connections and is responsible for controlling ports and sessions

TRANSPORT LAYER 4 – Transmits data using transmission protocols including TCP and UDP

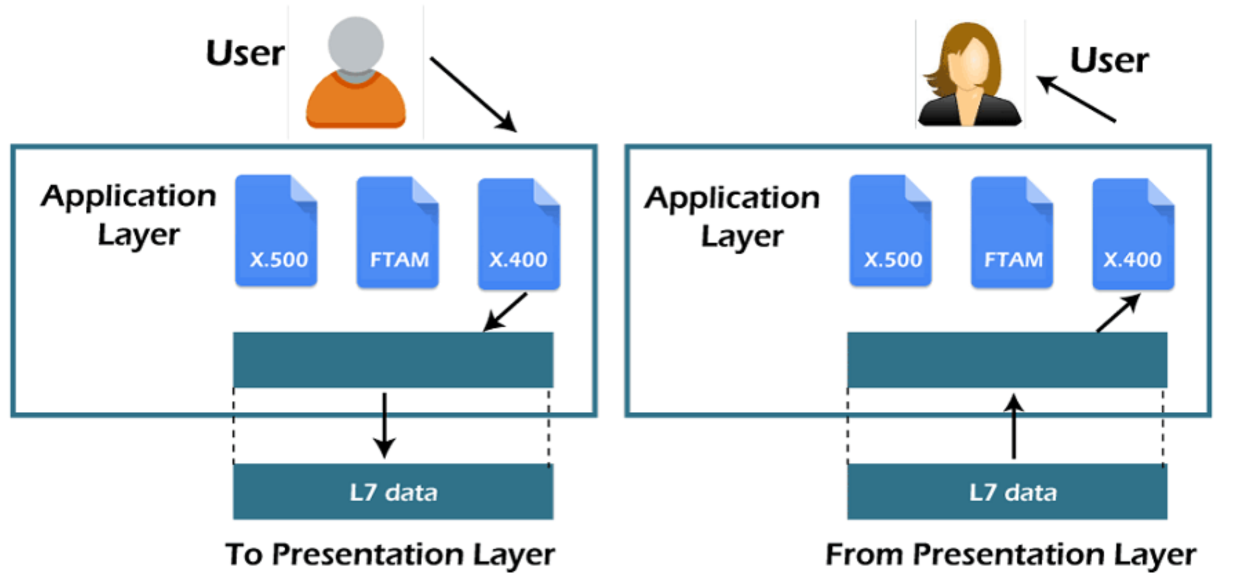
NETWORK LAYER 3 – Decides which physical path the data will take

DATALINK LAYER 2 – Defines the format of data on the network

PHYSICAL LAYER 1 – Transmits raw bit stream over the physical mec

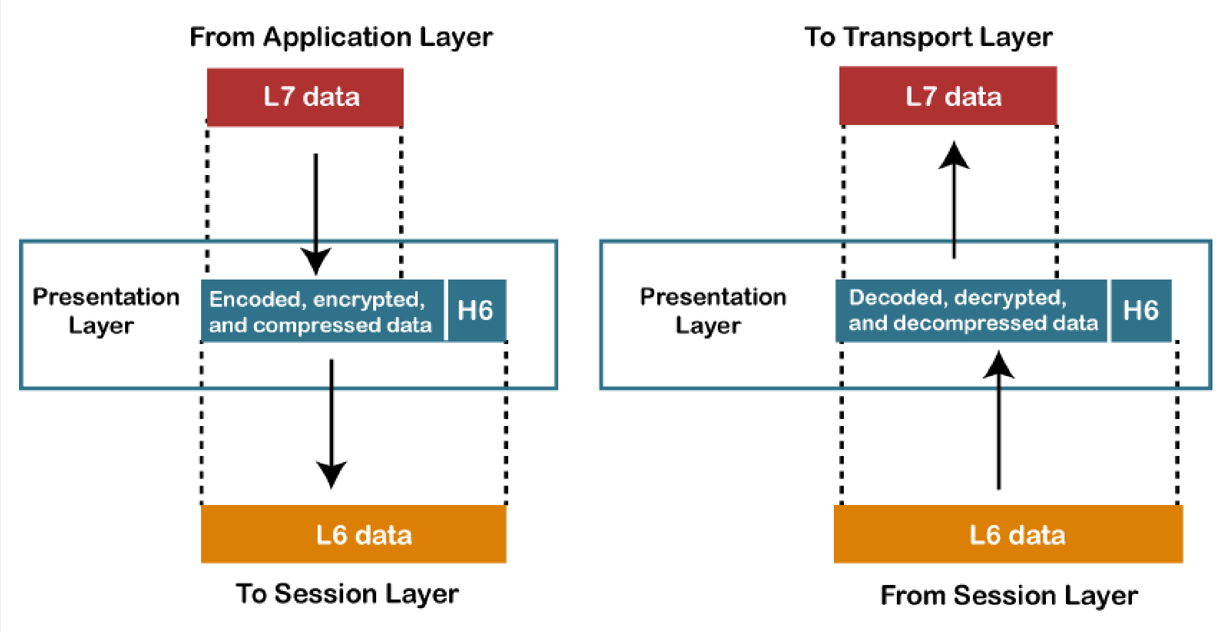
Layer 7: Application Layer

- Application layer supports application and end-user processes to access network service.
- Serves as the interface between user and network.
- An application layer is not an application, but it performs the application layer functions.



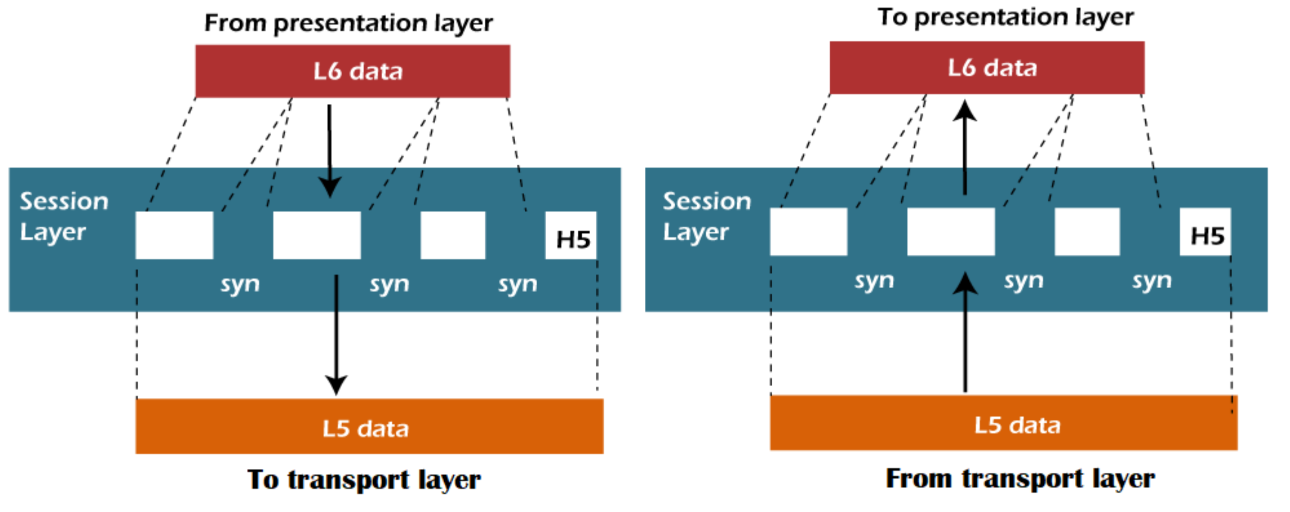
Layer 6: Presentation Layer

- Responsible for data representation on your screen
- Encryption and decryption of the data is done here.
- Data compression and decompression takes place here.
- Presentation layer prepares the data.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.



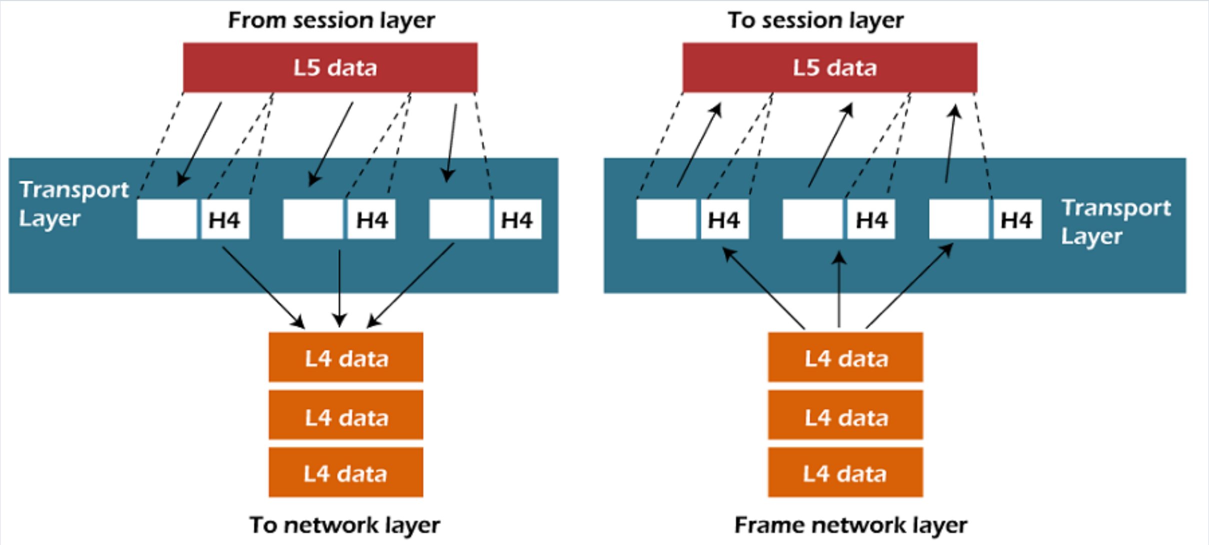
Layer 5: Session Layer

- This layer provides session management capabilities between hosts.
- Session layer deals with connections.
- It establishes, manages, and terminates sessions between two communicating nodes.

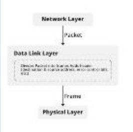


Layer 4: Transport Layer

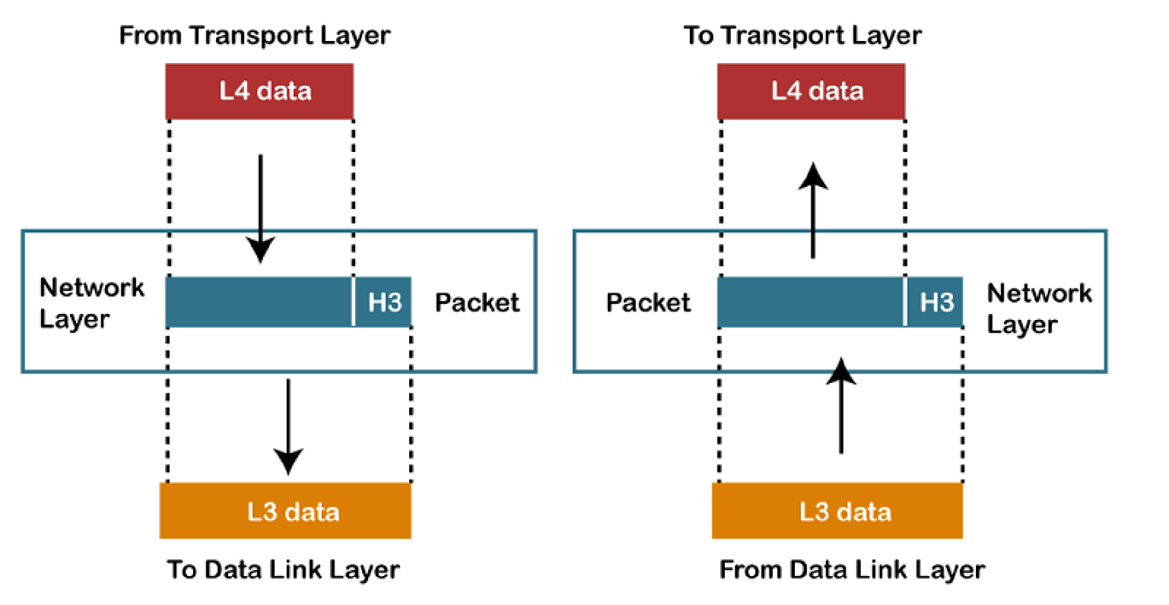
- Responsible for the transparent transfer of data between end systems
- Responsible for end-to-end error recovery and flow control
- Responsible for complete data transfer.
- Protocols like TCP, UDP work here
- This layer takes data from the above layer and breaks it into smaller units called Segments and then gives it to the Network layer for transmission, and vice-versa.



Layer 3: Network Layer

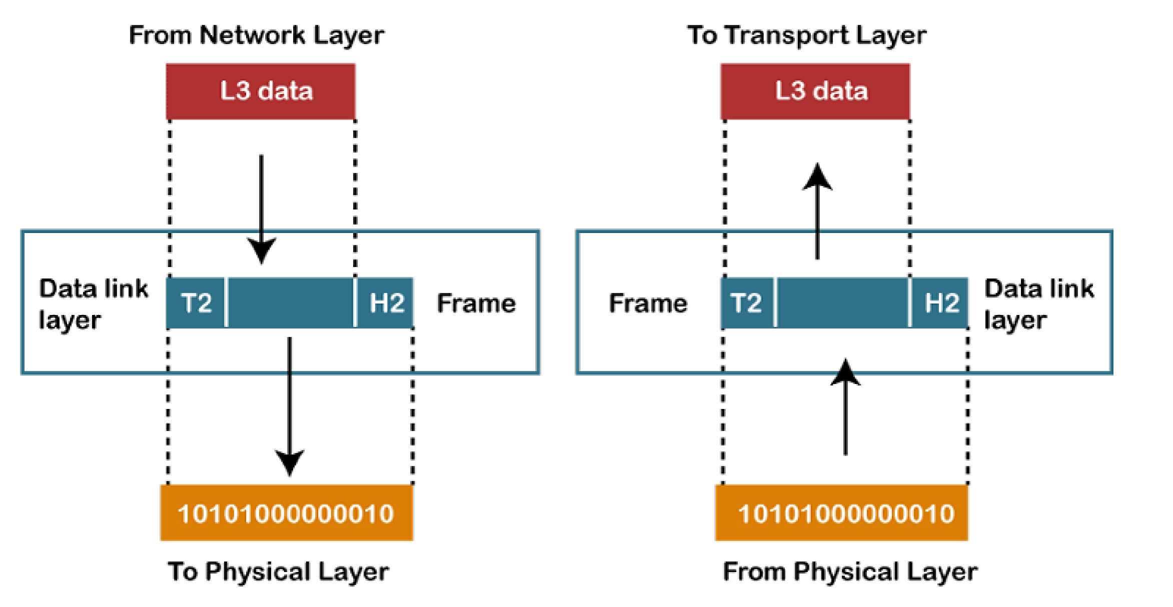


- It is a layer that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.



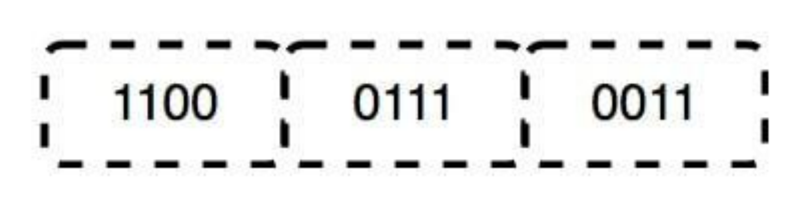
Layer 2: Data Link Layer

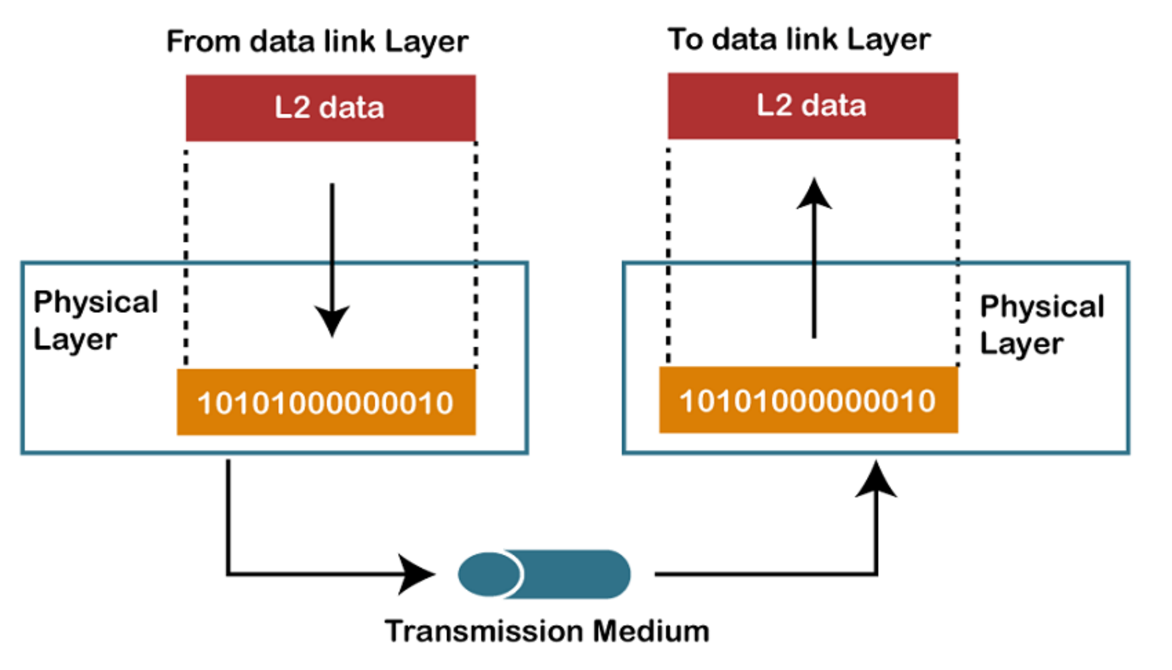
- This layer takes packets from the above layer and divides into frames and then gives it to the Physical layer for transmission, and vice-versa.
- This layer also checks any transmission errors and sorts it out accordingly.
- When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address.
- It contains two sub-layers:
  - **Logical Link Control Layer:** LLC identifies the address of the network layer protocol from the header.
  - **Media Access Control Layer:** MAC is used for transferring the packets over the network.



Layer 1: Physical Layer

- he lowest layer of the OSI reference model is the physical layer.
- It is responsible for the actual physical connection between the devices.
- The physical layer contains information in the form of **bits.**
- It is responsible for transmitting individual bits from one node to the next.
- When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.





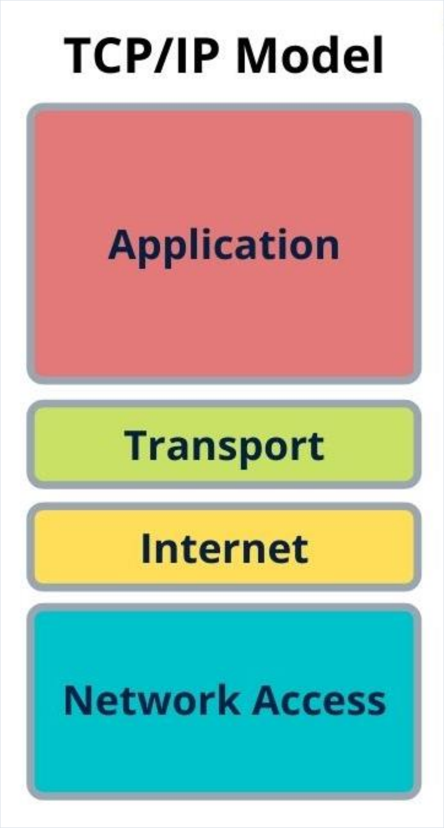
Summary: OSI Layers and their functions

Layer	Name	Functions	Protocols / Technologies
7	Application	Provides network services to end-user applications.	HTTP, FTP, SMTP
6	Presentation	Translates data formats, encryption, and compression.	SSL, TLS, JPEG, ASCII
5	Session	Manages sessions between applications (e.g., establishing, maintaining, and terminating).	NetBIOS, RPC
4	Transport	Ensures reliable data transfer and error recovery (segmentation and reassembly).	TCP, UDP
3	Network	Handles routing, addressing, and delivery of packets between devices.	IP, ICMP, ARP
2	Data Link	Ensures error-free data transfer between adjacent network nodes.	Ethernet, Wi-Fi, PPP
1	Physical	Defines hardware components and data transmission via physical medium.	Cables, Fiber optics, Bluetooth

- **Secure Sockets Layer (SSL)** is standard technology for securing an internet connection by encrypting data sent between a website and a browser (or between two servers)
- **Remote Procedure Call (RPC)** is a protocol that allows a computer program to request a procedure or function from another computer or server.
- **Transport Layer Security (TLS)** is a cryptographic protocol that encrypts data sent over the internet to protect communications.
- **Network Basic Input/Output System (NetBIOS)**: It provides services related to the session layer of the OSI model allowing applications on separate computers to communicate over a local area network.
- **The Internet Control Message Protocol (ICMP**) is a network layer protocol used by network devices to diagnose network communication issues.
- **Address Resolution Protocol (ARP):** It is responsible to find the hardware address of a host from a known IP address.
- **The Point-to-Point Protocol (PPP)** is a data link layer (layer 2) protocol that enables direct communication between two routers without the need for any other networking in between.

B) TCP/IP model

- **TCP/IP** was designed and developed by the Department of Defense (DoD) in the 1960s and is based on standard protocols.
- It stands for Transmission Control Protocol/Internet Protocol.
- It is an implementation model and is used in real-world networking, focusing on practical implementation.
- The TCP/IP model is a concise version of the OSI model.
- It contains four layers, unlike the seven layers in the OSI model.



Layers in TCP/IP model

1. Application layer

- An application layer is the **topmost layer** in the TCP/IP model.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer

2. Transport layer:

- The transport layer is responsible **for maintaining end-to-end communications** across the network.
- TCP **handles communications between hosts and provides** flow control, multiplexing and reliability.
- The transport protocols include **TCP** and User Datagram Protocol (**UDP**).

3. **The Internet layer:**
   - An internet layer is the **second layer** of the TCP/IP model.
   - An internet layer is also known as the **network layer.**
   - The main responsibility of the internet layer **is to send the packets from any network**, and they arrive at the destination irrespective of the route they take.
4. **The Network Access layer:**
   - Also **called Data-Link Layer**
   - A network layer is the **lowest layer** of the TCP/IP model.
   - A network layer is **the combination of the Physical layer and Data Link layer** defined in the OSI reference model.
   - It **defines how the data should be sent physically** through the network.
   - This layer is mainly responsible for the transmission of the data between two devices on the same network.

Summary: TCP/IP Layers and their functions

TCP/IP layers	Corresponding OSI Layers	Functions	Protocols / Technologies
Application	Application, Presentation and Session	Interfaces with applications and ensures data integrity.	HTTP, FTP, SMTP
Transport	Transport	Provides end-to-end communication and error control.	TCP, UDP
Internet	Network	Handles logical addressing and routing packets	IP, ICMP, ARP
Network Access	Data Link and Physical	Deals with hardware communication and data framing.	Ethernet, Wifi

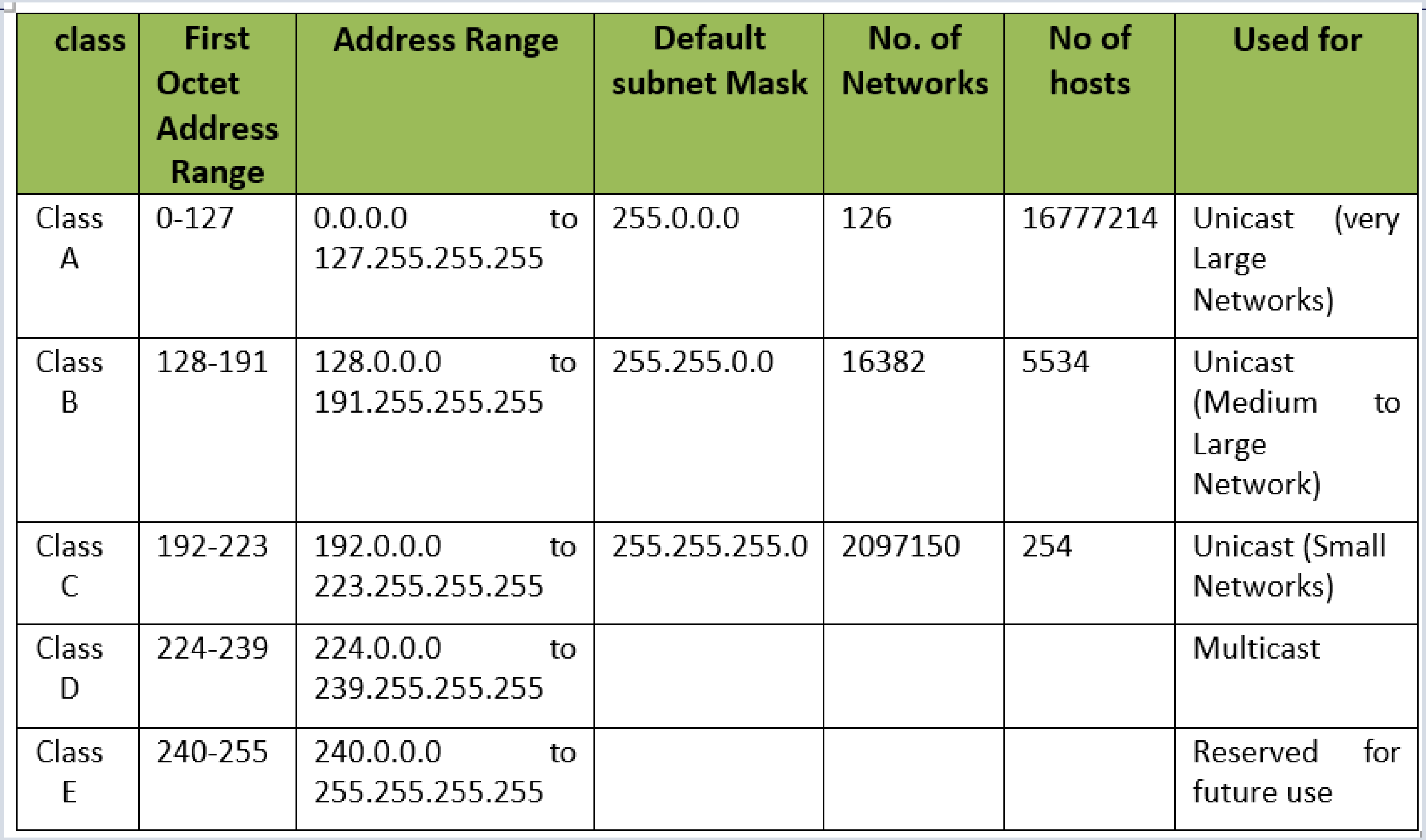
Assignment:

- Differentiate between Client-server and peer-to-peer architectures.
- Differentiate between OSI and TCP/IP models
- Differentiate between TCP and UDP.

IP Addressing

- **An IP address** or IP is **a number used to indicate the location** of a computer or other device on a network using TCP/IP.
- There are two types of addresses used today, **IPv4** and **IPv6**.
- IPV4 uses 32 bits, represented in decimal notation, uses 4 octets.
- IPV6 uses 128 bits, represented in hexadecimal notation, uses 8 octets.
- Example of an IPv4 address: **45.79.151.23**
- Example of an IPv6 address: **2601:681:4200:c5c0:516:f0bb:ac3b:46bd**

IP Addresses and classes



class	First Octet Address Range	Address Range	Default subnet Mask	No. of Networks	No of hosts	Used for
Class A	0-127	0.0.0.0 to 127.255.255.255	255.0.0.0	126	16777214	Unicast (very Large Networks)
Class B	128-191	128.0.0.0 to 191.255.255.255	255.255.0.0	16382	5534	Unicast (Medium to Large Network)
Class C	192-223	192.0.0.0 to 223.255.255.255	255.255.255.0	2097150	254	Unicast (Small Networks)
Class D	224-239	224.0.0.0 to 239.255.255.255				Multicast
Class E	240-255	240.0.0.0 to 255.255.255.255				Reserved for future use

Class A address

- Class A IP addresses **use the first 8 bits (first Octet) to designate the Network address**.
- The **1st bit which is always a 0**, is used to indicate the address as a Class A address & the remaining 7 bits are used to designate the Network.
- There are **128 Class A Network Addresses (i.e. 2^7=128),** but because addresses with all zeros aren't used & address 127 is a special purpose address, 126 Class A Networks are available.
- The **other 3 octets contain the Host address**. No of available host = **(2^n – 2) =** 2^{24}-2 = 16,777,214 Host addresses (minus 2 because 2 addresses are reserved for network and broadcast address)
- Subnet Mask = 255.0.0.0
- Example of Class A IP address: 10.0.0.0

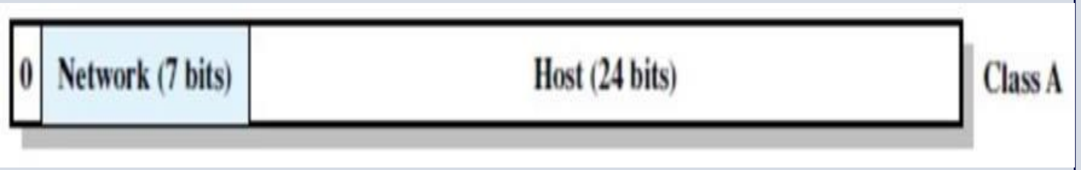


Figure: Class A IP address format

Class B Address

- Class B addresses **use the first 16 bits (two octets) for the Network address**.
- The **last 2 octets are used for the Host address**.
- The **1st 2 bit, which are always 10,** designate the address as a Class B address & **14 bits are used to designate the Network**. This leaves 16 bits (two octets) to designate the Hosts.
- Using our formula, $(2^{14} – 2)$, there can be **16,382 Class B Networks** & each Network can have $(2^{16} – 2)$ Hosts, or 65,534 Hosts.
- Subnet mask: 255.255.0.0
- Example : 135.58.24.17

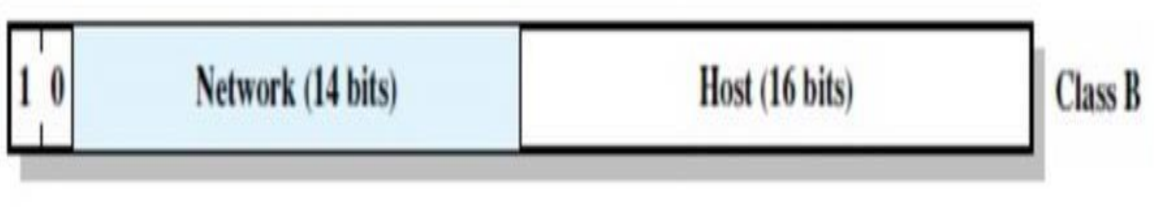


Figure: Class B IP address format

Class C address

- Class C addresses use the **first 24 bits (three octets) for the Network address** & only the last octet for Host addresses.
- The **1st 3 bits of all class C addresses are set to 110**, leaving 21 bits for the Network address, which means there can be **2,097,150** (2^{21} – 2) Class C Networks, but only **254 (2^{8} – 2) Hosts** per Network.
- Subnet Mask: 255.255.255.0
- Eg: 192.168.1.1

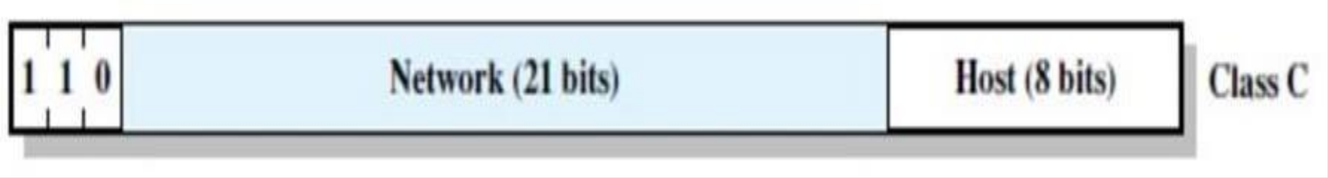


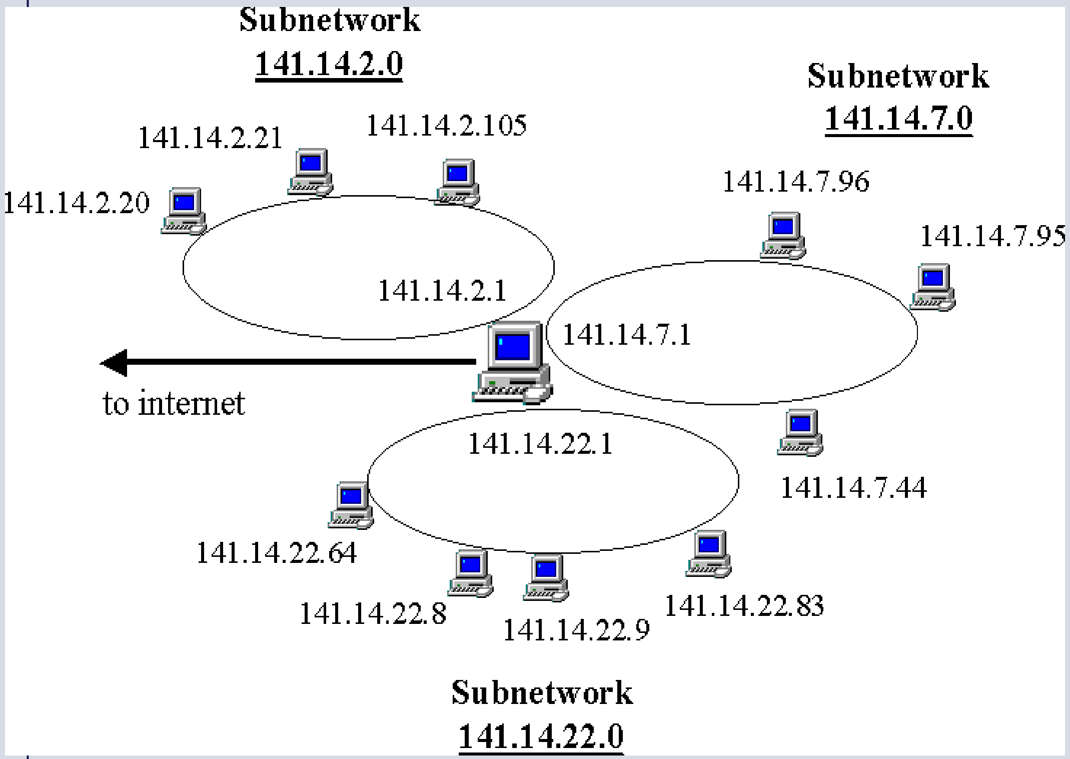
Figure: Class C IP address format

Assignment:

- Differentiate between IPV4 and IPV6.
- Explain the need of IPV6.

Subnet and Subnetting

- Subnetting is **the strategy used to partition a single physical network into more than one smaller logical sub-networks** (subnets).
- And each smaller network inside that network is called its **subnet** or **sub-network**.
- Advantages:
  - Subnetting breaks large network in smaller networks and smaller networks **are easier to manage.**
  - Subnetting **reduces network traffic** by removing collision and broadcast traffic, that overall improve performance.
  - Subnetting allows you to **apply network security** polices at the interconnection between subnets.
  - Subnetting allows you to save money by **reducing requirement for IP range.** i.e. Efficient IP address utilization.



Key Terms in Subnetting

Terms	Description
IP Address	A unique identifier for a device on a network. IPV4 or IPV6
Subnet Mask	Used to determine which portion of an IP address represents the network and which portion represents the host. For eg: 255.255.255.0 (or /24) means the first 24 bits are for the network.
CIDR notation	Classless Inter-Domain Routing (CIDR) is a shorthand representation of the subnet mask. For eg: 192.168.1.0/24 indicates the first 24 bits are fixed for the network.
Network Address	The first address in a subnet, used to identify the subnet itself. Example : For 192.168.1.0/24, the network address is 192.168.1.0
Broadcast Address	The last address in a subnet, used for broadcasting messages to all devices in that subnet. Example : For 192.168.1.0/24, the broadcast address is 192.168.1.255

1.1.2 Encryption and Cryptography Basics

- E2EE,
- Hashing,
- Hashing Techniques,
- the CIA triad,
- concepts on steganography and cryptocurrency

Encryption and Decryption

- **Encryption** is the process by which a **readable message is converted to an unreadable form to prevent unauthorized parties from reading it.**
- **Decryption** is the process of converting an encrypted message **back to its original (readable) format.**
  - The original message is called the **plaintext message**.
  - The encrypted message is called the **ciphertext message**.
- **Purpose:** Ensure **confidentiality**, **integrity**, and **authentication** in communication.
- Digital encryption algorithms work by manipulating the digital content of a plaintext message mathematically, using an encryption algorithm and a digital key to produce a ciphertext of the message.
- The sender and recipient can communicate securely if the sender and recipient are the only ones who know the key.

Key Concepts:

- **Plaintext**: Original readable data.
- **Ciphertext**: Encrypted data.
- **Key**: A piece of information used for encryption and decryption.
- **Cryptanalysis**: The study of breaking encryption algorithms.

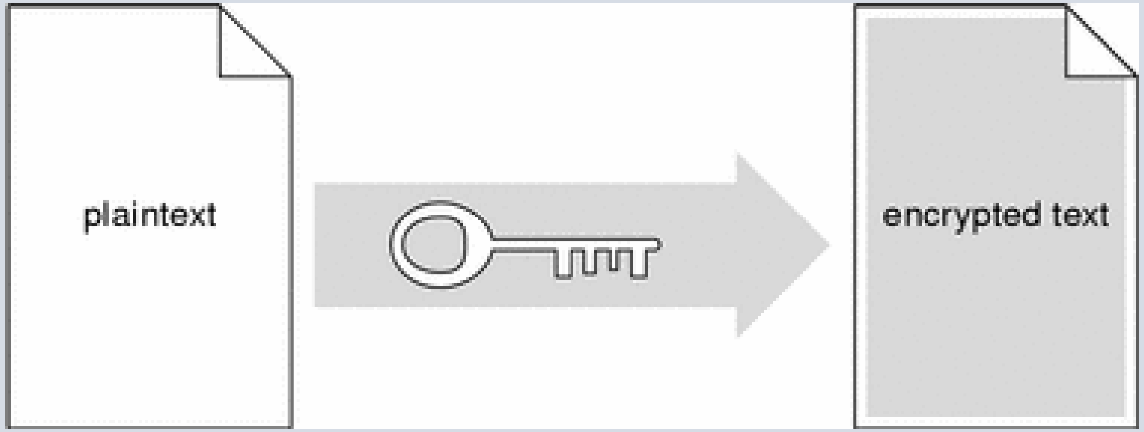


Figure: Sender Uses Key to Encrypt Plaintext to Ciphertext

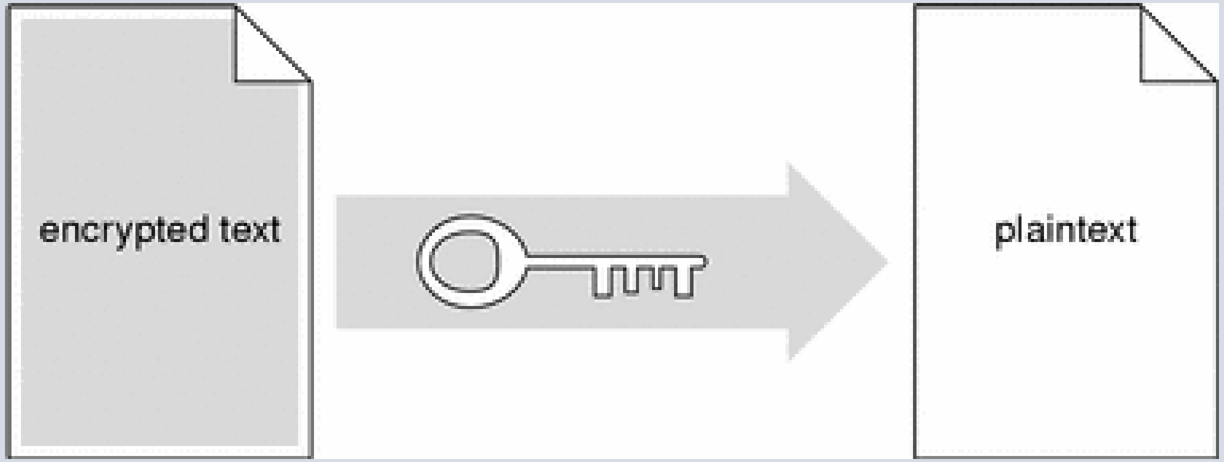


Figure: Recipient Uses Key to Decrypt Ciphertext to Plaintext

Cryptography

- Cryptography is the **study of securing communications from outside observers.**
- **Encryption algorithms** take the original message, or **plaintext**, and converts it into ciphertext, which is not understandable.
- The key allows the user to **decrypt** the message, thus ensuring on they can read the message.
- The strength of the randomness of an **encryption** is also studied, which makes it harder for anyone to guess the key or input of the algorithm.
- Cryptography focuses on four different objectives:
  1. **Confidentiality**: Ensures that only authorized parties can access the information.
  2. **Integrity**: Protects data from being altered during transmission or storage.
  3. **Authentication**: Confirms the identity of the sender and receiver.
  4. **Non-repudiation**: Prevents denial of actions, such as a sender denying sending a message.

An example of cryptography

Vigenère Cipher

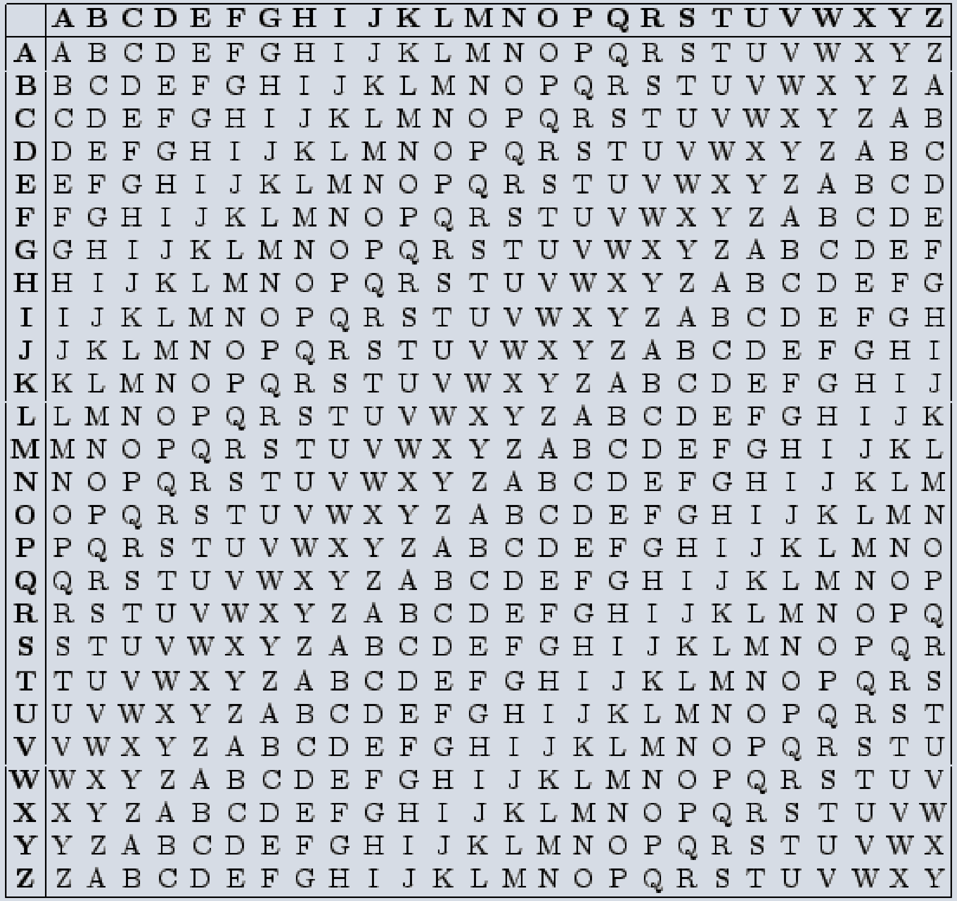
key: VIGVIGVIGVIGVIGV

Plain: THEBOYHASTHEBALL

Cipher: OPKWWECIYOPKWIRG

key

Plain



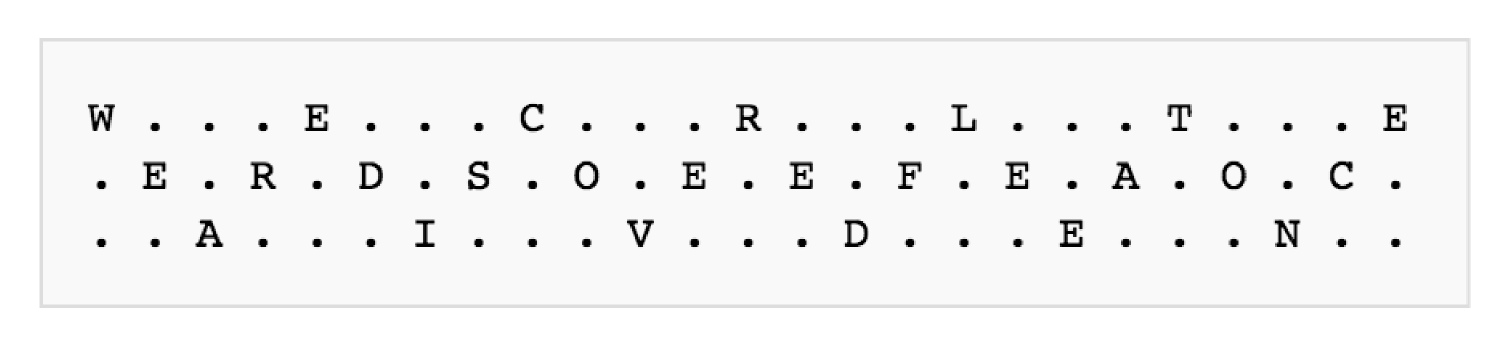
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

An example of cryptography

Rail-fence cipher

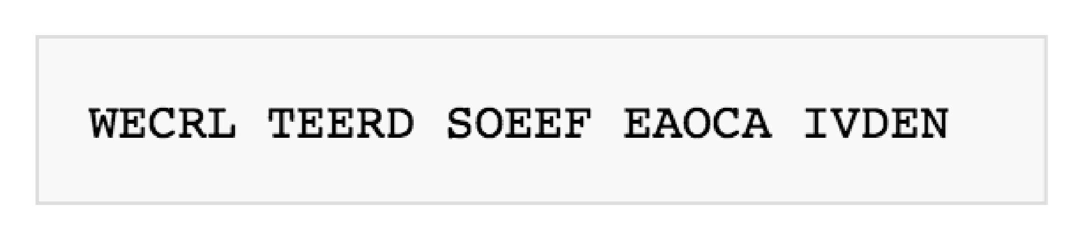
- Plain Text: 'WE ARE DISCOVERED. FLEE AT ONCE’

key



```
W . . . E . . . C . . . R . . . L . . . T . . . E
. E . R . D . S . O . E . E . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . .
```

Cipher



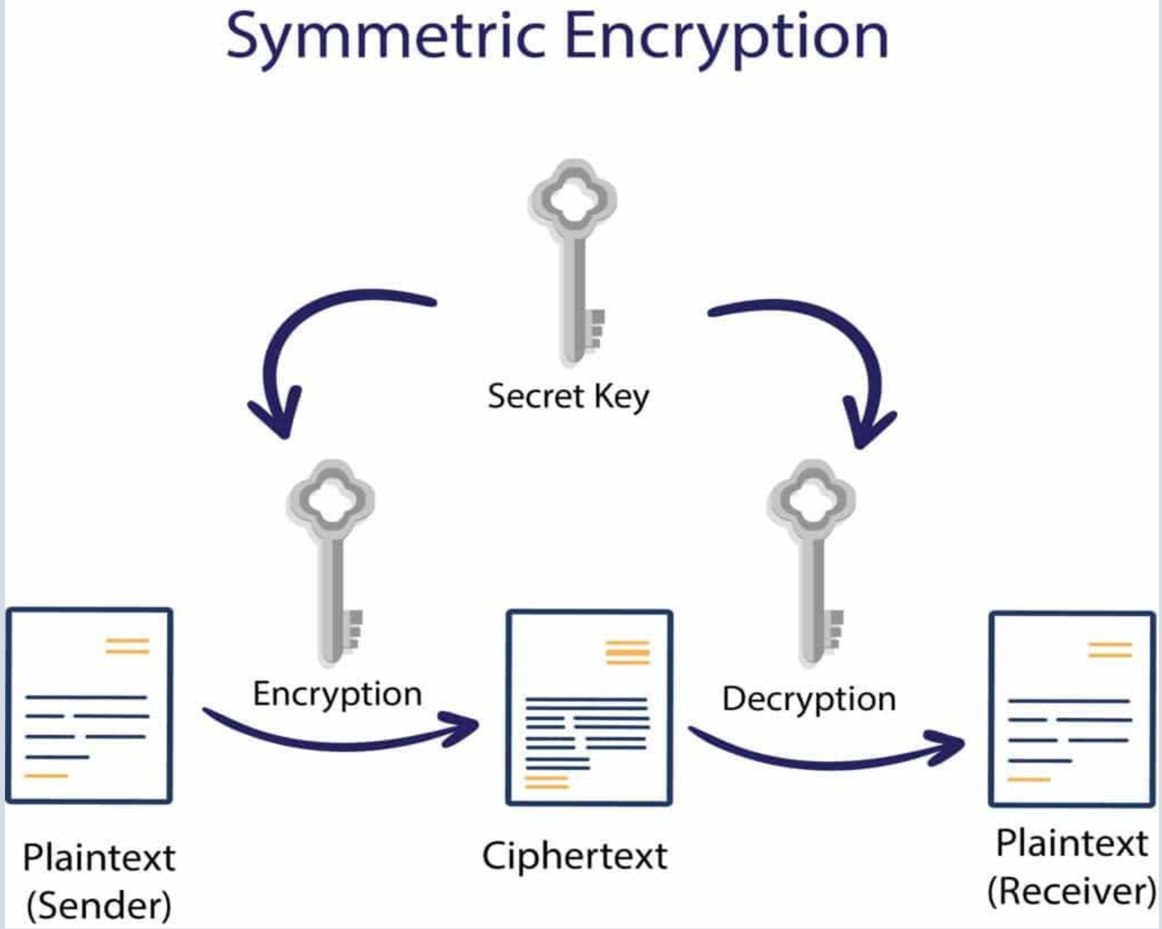
```
WECRL TEERD SOEEF EAOCA IVDEN
```

Types of Cryptography

- Cryptography can be broken down into three different types:
  1. Secret Key Cryptography
  2. Public Key Cryptography

i) Secret Key Cryptography (Symmetric)

- **Features:**
  - The same(single) key is used for encryption and decryption.
  - Faster but requires secure key exchange.
- **Example:** AES, DES, Triple DES.
- **Advantages**: Faster encryption/decryption.
- **Challenges**: Key distribution and management are challenging
- **Application:** Secure file storage, data transmission in closed networks



Methods for key exchange:

a. Physical Delivery

- The key is exchanged using a secure physical channel (e.g., a USB drive, in-person meeting).
- Limitation: This method is impractical for remote communication or large-scale networks.

b. Encrypted Communication

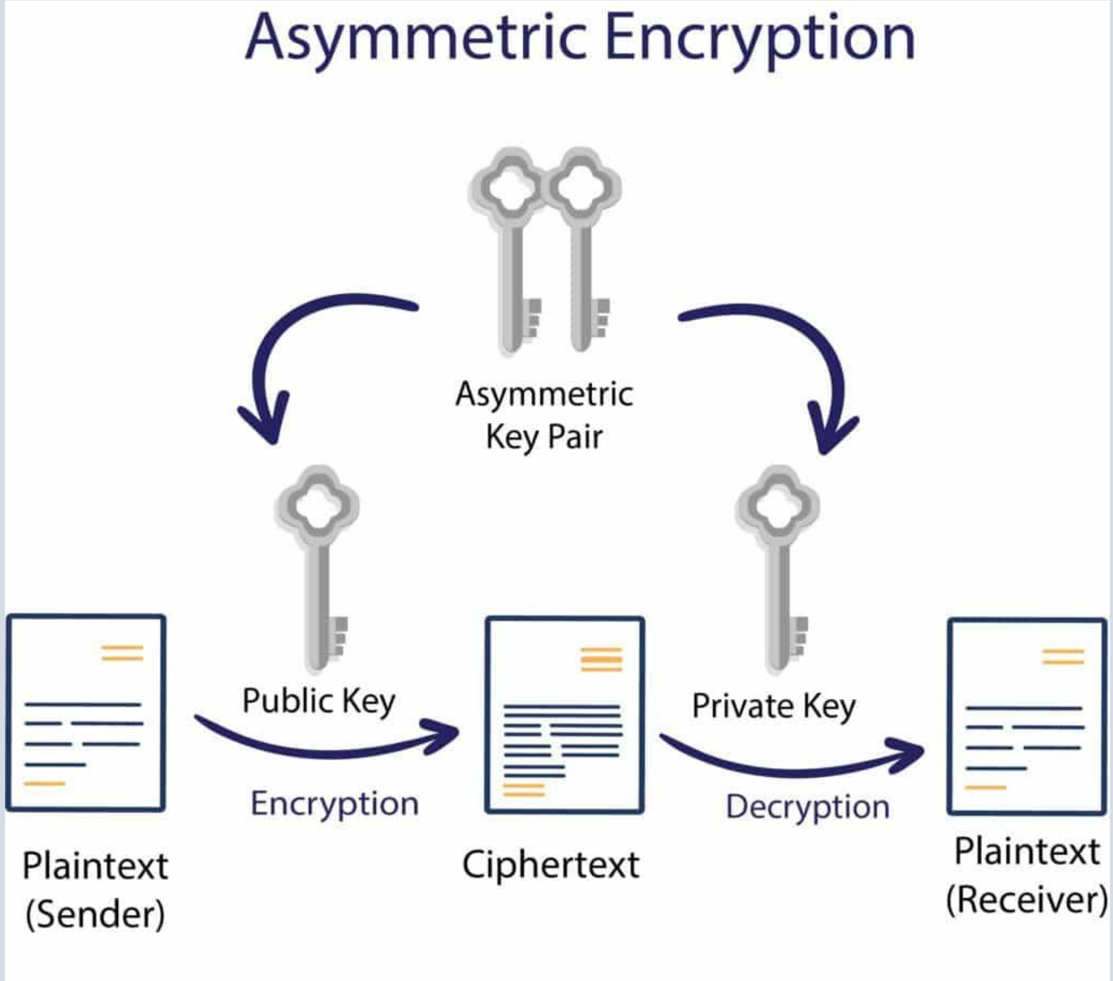
- The key is encrypted using another secure method (e.g., a pre-shared key or asymmetric encryption) before being transmitted.

c. Diffie-Hellman Key Exchange

- A widely used method that allows two parties to establish a shared secret key over an insecure channel without transmitting the key itself.

ii) Public Key Cryptography (Asymmetric)

- **Features:**
  - Uses two keys: **Public Key** for encryption and **Private Key** for decryption.
  - Solves key distribution problem but slower than symmetric.
- **Example:** RSA (Rivest–Shamir–Adleman), ECC (Elliptic Curve Cryptography).
- **Advantages**: Solves the problem of key distribution.
- **Disadvantages**: Slower than symmetric cryptography.
- **Applications:** Digital signatures, secure email communication.



Methods for key exchange:

a. Public Key Exchange

- The sender encrypts the symmetric session key with the receiver's **public key**.
- The receiver decrypts the session key with their **private key**.

b. Key Management Protocols

- Protocols like TLS/SSL are used to exchange keys securely during online communication.
- The server provides its public key in a certificate.
- The client uses the server's public key to encrypt a randomly generated session key.

c. Hybrid Systems

- A combination of symmetric and asymmetric methods: asymmetric cryptography is used to establish a secure channel, and symmetric keys are exchanged for bulk data encryption due to their efficiency.

Hashing

- Hashing is a technique used to efficiently store and retrieve data.
- It transforms input data (keys) into a fixed-size value called a *hash code* or *hash value*, typically using a mathematical function known as a *hash function*.
- Hash functions **are irreversible, one-way functions which protect the data,** at the cost of not being able to recover the original message.
- **Hashing** is a way to transform a given string into a **fixed length string.**
- A hash can be used for hashing data (such as passwords) and in certificates.
- Irreversible, used for data integrity.
- Some of the most famous hashing algorithms are: SHA (Secure Hash Algorithm), Message Digest 5 (MD5)

Hash functions

- A function that takes input data (key) and returns a fixed-size string or number (hash value).
- One of the common method is Division method. The **Division Method** is a simple and widely used technique for designing a hash function.
- The Hash function formula is: **h(k) = k mod m**
- Where: h(k) is the hash value or index

  K is the key to be hashed.

  m: The size of the hash table (number of slots or buckets).

- Example:
- Let,

Hash Table Size (mmm): Assume m = 7 (a prime number)

Keys: k=10, 20, 30, 15

Hash Values:

h(10) = 10 mod 7 = 3

h(20) = 20 mod 7 = 6

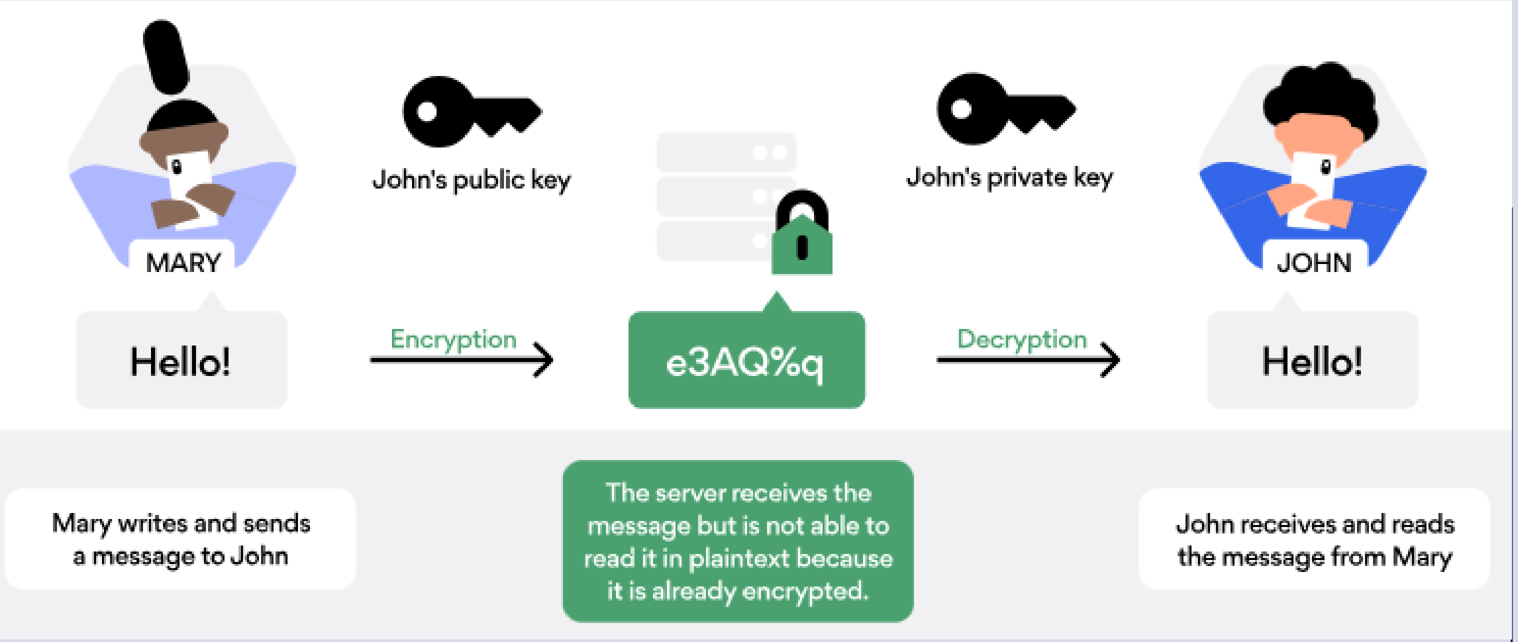
h(30) = 30 mod 7 = 2

h(15) = 15 mod 7 = 1

End-to-end encryption (E2EE)

- End-to-End Encryption (E2EE) ensures that messages or data are encrypted on the sender's device and decrypted only on the recipient's device.
  - No intermediary, including service providers, can access the content.
- **Objective**: Provides confidentiality, ensuring only the intended parties can access the communication.

How E2E encryption works?



Mary writes and sends a message to John

The server receives the message but is not able to read it in plaintext because it is already encrypted.

John receives and reads the message from Mary

1. **Key Generation**: Each user generates a pair of keys:
   - **Public Key**: Shared openly.
   - **Private Key**: Kept secret.
2. **Message Encryption**: The sender encrypts the message using the recipient's public key.
3. **Message Decryption**: The recipient decrypts the message using their private key.
4. **Secure Channels**: Algorithms like Diffie-Hellman or Elliptic Curve Cryptography **(ECC)** may establish shared secrets for session-based encryption.

Assignment:

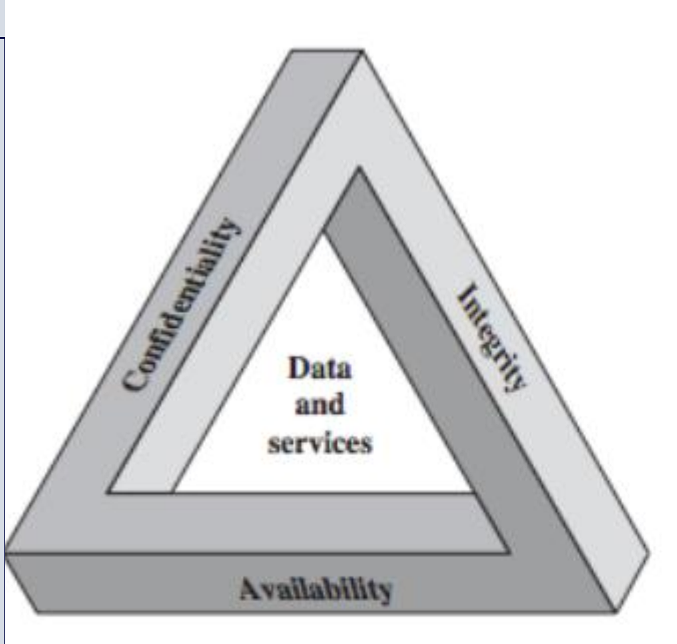
1. Mention the advantages and limitation of E2EE technique.
2. Why E2EE is important for modern digital communication? Explain with some usecases.

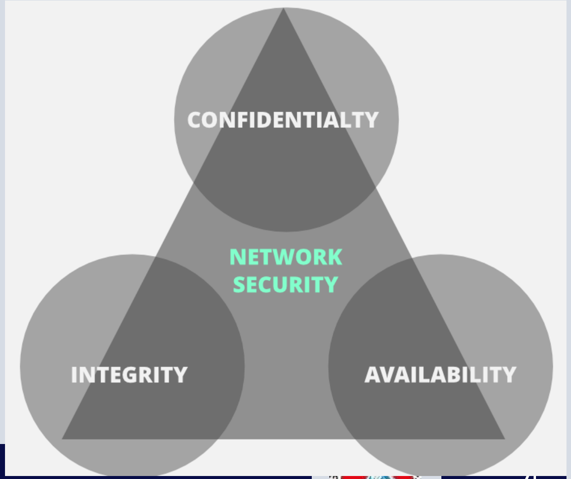
Hashing techniques/types

- cryptography uses multiple hash functions to secure data. Some of the most popular cryptographic hashes include the following:
  - Secure Hash Algorithm (SHA-1, SHA -2, SHA-3)
  - Message Digest (MD2, MD4, MD5)

CIA triad

- CIA: **Confidentiality- Integrity- Availability**
- The **CIA** triad is one of the most important models which is designed to guide policies for information security within an organization.
- The CIA **triad provides a high-level framework** for cybersecurity professionals to consider when auditing, implementing, and improving systems, tools, and programs for organizations.
- It is a powerful way to identify weak points and form solutions to strengthen policies and programs.





i) Confidentiality

- The attacker may try to capture the data using different tools available on the Internet and gain access to your information.
  - A primary way to avoid this is to use encryption techniques to safeguard your data so that even if the attacker gains access to our data, he/she will not be able to decrypt it.
  - Encryption standards include **AES**(Advanced Encryption Standard) and **DES** (Data Encryption Standard).
  - Another way to protect your data is through a VPN tunnel. VPN stands for Virtual Private Network and helps the data to move securely over the network.
- Confidentiality **involves protecting sensitive data** private and safe from unauthorized access.
- This includes **protecting information from bad actors** with malicious intent, as well as limiting access to only authorized individuals within an organization.
- For example: Passwords, locks, and tokens are some common measures to keep our sent email confidential.

ii) Integrity

- Maintaining data integrity is important to make sure data and business analysts are accessing accurate information.
- Integrity refers to **maintaining the accuracy and trustworthiness of data** throughout its lifecycle.
- It involves protecting data from unauthorized modification, deletion, or tampering.
- Data integrity measures aim to **ensure that information remains unaltered and reliable.**
- Techniques like **checksums, digital signatures, and access controls** help enforce data integrity.
- The idea here is to make sure that data has not been modified.

iii) Availability

- This means that the **network should be readily available** to its users.
- Availability concerns **ensuring that information and resources are accessible and usable when needed** by authorized users.
- This **includes preventing disruptions, downtime, or denial of service attacks** that could compromise access to data or systems.
- Availability measures **involve implementing redundancy, fault tolerance, disaster recovery plans**, **and network security mechanisms** to maintain continuous access to services and resources.

Assignment:

- Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system. In each case, indicate the degree of importance of the requirement.

Steganography

- A steganography technique **involves hiding sensitive information within an ordinary, non-secret file or message**, so that it will not be detected.
- The sensitive information will then be extracted from the ordinary file or message at its destination, thus avoiding detection.
- Steganography is an additional step that can be used in conjunction with encryption in order to conceal or protect data.
- We can use steganography to hide text, video, images, or even audio data.
- Steganography Examples Include
  - ➢ Writing with invisible ink
  - ➢ Embedding text in a picture (like an artist hiding their initials in a painting they've done)
  - ➢ Backward masking a message in an audio file (remember those stories of evil messages recorded backward on rock and roll records?)
  - ➢ Concealing information in either metadata or within a file header
  - ➢ Hiding an image in a video, viewable only if the video is played at a particular frame rate
  - ➢ Embedding a secret message in either the green, blue, or red channels of an RRB image

Types of Steganography:

- Different types of Steganography:
  1. Text Steganography
  2. Image Steganography
  3. Audio Steganography
  4. Video Steganography
  5. Network or Protocol Steganography

1. **Text Steganography**
    - There is steganography in text files, which entails secretly storing information.
    - In this method, the hidden data is encoded into the letter of each word.
2. **Image Steganography**
    - This entails concealing data by using an image of a different object as a cover.
    - Pixel intensities are the key to data concealment in image steganography.
3. **Audio Steganography**
    - It is the science of hiding data in sound. Used digitally, it protects against unauthorized reproduction.
    - Watermarking is a technique that encrypts one piece of data (the message) within another (the "carrier").
    - Its typical uses involve media playback, primarily audio clips.

4. Video Steganography

- Video steganography is a method of secretly embedding data or other files within a video file on a computer.
- Video (a collection of still images) can function as the "carrier" in this scheme. Discrete cosine transform (DCT) is commonly used to insert values that can be used to hide the data in each image in the video, which is undetectable to the naked eye.
- Video steganography typically employs the following file formats: H.264, MP4, MPEG, and AVI.

5. Network or Protocol Steganography

- It involves concealing data by using a network protocol like TCP, UDP, ICMP, IP, etc., as a cover object.
- Steganography can be used in the case of covert channels, which occur in the OSI layer network model.

Cryptocurrency

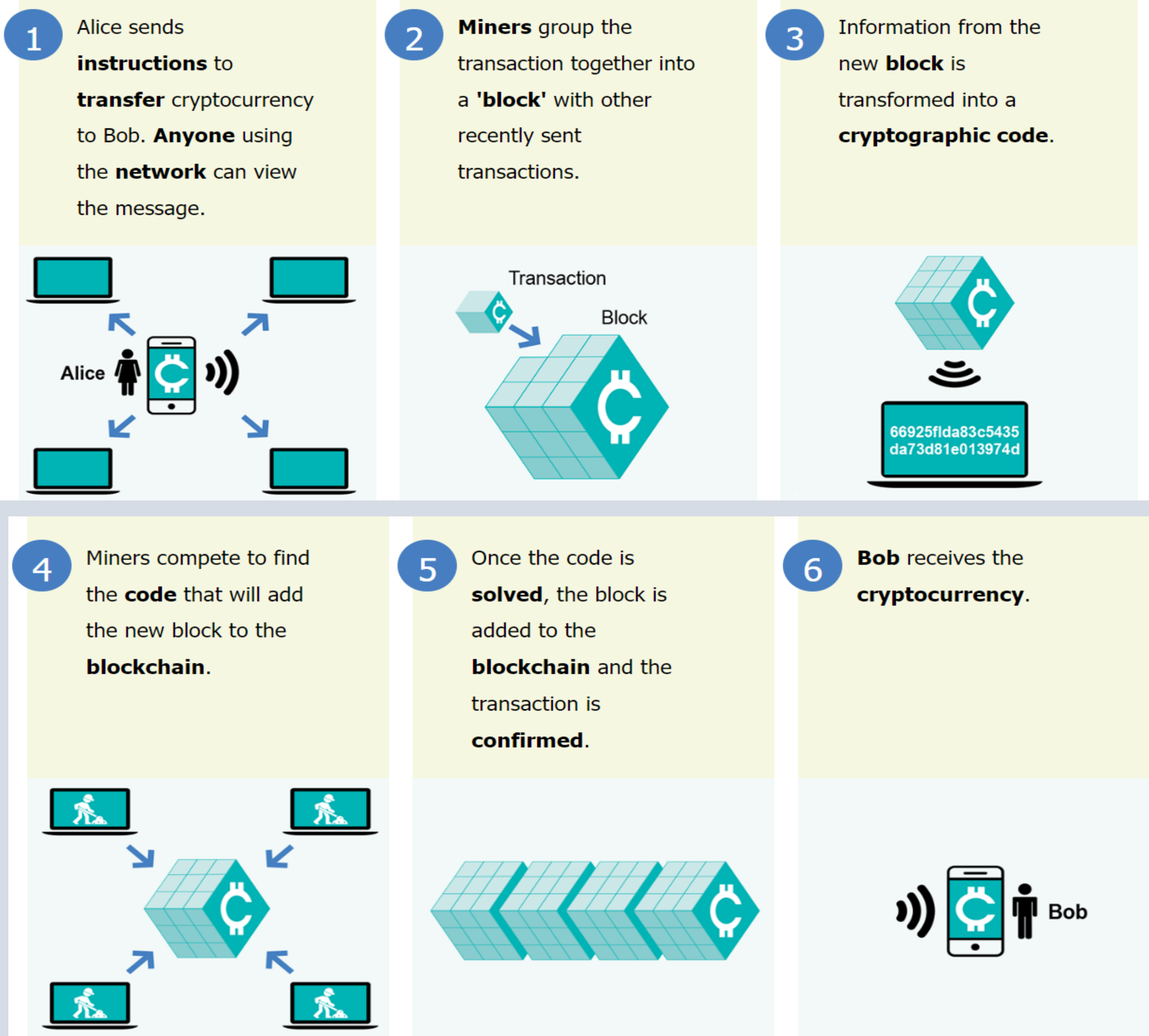
- Cryptocurrency, sometimes called crypto-currency or crypto**, is any form of currency that exists digitally** or virtually and **uses cryptography to secure transactions**.
- Cryptocurrencies **don't have a central issuing or regulating authority**, instead using a decentralized system to record transactions and issue new units.
- Cryptocurrency is a digital payment system that **doesn't rely on banks to verify transactions**.
- It's **a peer-to-peer system** that can enable anyone anywhere to send and receive payments.
- When you transfer cryptocurrency funds, the **transactions are recorded in a public ledger.**
- The first cryptocurrency was **Bitcoin**, which was founded in 2009 and remains the best known today.
- Some other are: **Ethereum, Dodgecoin, Tether, Litecoin, Ripple** and many more

How it works?

- Cryptocurrency transactions occur through **electronic messages that are sent to the entire network with instructions about the transaction.**
- The instructions **include information such as the electronic addresses** of the parties involved, **the quantity of currency** to be traded, **and a time stamp.**
- Cryptocurrencies **run on a distributed public ledger** called **blockchain**, a record of all transactions updated and held by currency holders.
- Units of cryptocurrency are created through a process called **mining**, which involves using computer power to solve complicated mathematical problems that generate coins.
- Users can also buy the currencies from brokers, then store and spend them using cryptographic wallets.
- If you own cryptocurrency, you don't own anything tangible. What **you own is a key that allows you to move a record or a unit of measure from one person to another without a trusted third party.**

Suppose Alice wants to transfer one unit of cryptocurrency to Bob.

1. Alice starts the transaction by sending an electronic message with her instructions to the network, where all users can see the message.
2. Alice's transaction is one of a number of transactions that have recently been sent.
3. Since the system is not instantaneous, the transaction sits with a group of other recent transactions waiting to be compiled into a block (which is just a group of the most recent transactions).
4. The information from the block is turned into a cryptographic code and miners compete to solve the code to add the new block of transactions to the blockchain.
5. Once a miner successfully solves the code, other users of the network check the solution and reach an agreement that it is valid.
6. The new block of transactions is added to the end of the blockchain, and Alice's transaction is confirmed. (This confirmation is not instant as it takes time for six blocks of transactions to be processed so that users can be certain that their transaction has been successful.)



1 Alice sends **instructions** to **transfer** cryptocurrency to Bob. **Anyone** using the **network** can view the message.

2 **Miners** group the transaction together into a **'block'** with other recently sent transactions.

3 Information from the new **block** is transformed into a **cryptographic code**.

4 Miners compete to find the **code** that will add the new block to the **blockchain**.

5 Once the code is **solved**, the block is added to the **blockchain** and the transaction is **confirmed**.

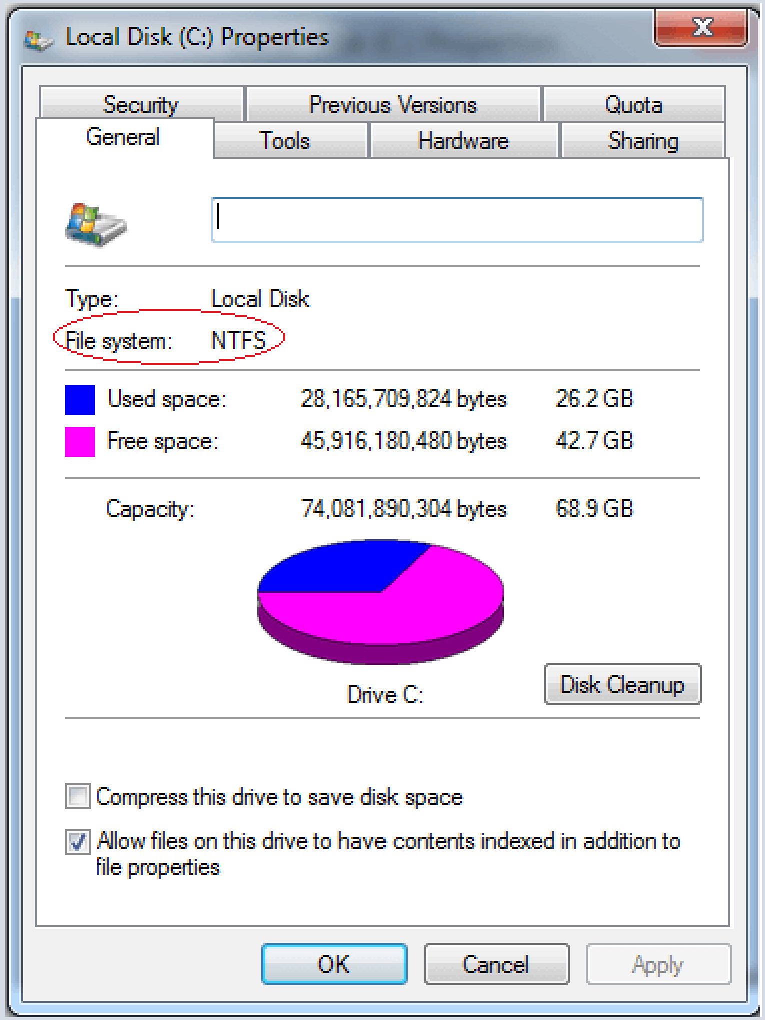
6 **Bob** receives the **cryptocurrency**.

Data Backup concepts

- 1.2.1. Storage Fundamentals (Understanding File Systems: FAT16, VFAT, FAT32, NTFS, EXT4)
- 1.2.2. Basics of Data Backup and Restore, the 3-2-1 backup rule, RAID, Disaster Recovery and High Availability

File Systems

- A file system **is a process of managing how and where data on a storage disk,** which is also referred to as file management or FS.
- It is a logical disk component that compresses files separated into groups, which is known as directories.
- Although there are various file systems with Windows, **NTFS** is the most common in modern times.
- A disk (e.g., Hard disk drive) has a file system, despite type and usage. Also, it contains information about file size, file name, file location fragment information, and where disk data is stored and also describes how a user or application may access the data. The operations like metadata, file naming, storage management, and directories/folders are all managed by the file system.



Type: Local Disk

File system: NTFS

🟦	Used space:	28,165,709,824 bytes	26.2 GB
🟪	Free space:	45,916,180,480 bytes	42.7 GB
	Capacity:	74,081,890,304 bytes	68.9 GB

Drive C:

☐ Compress this drive to save disk space

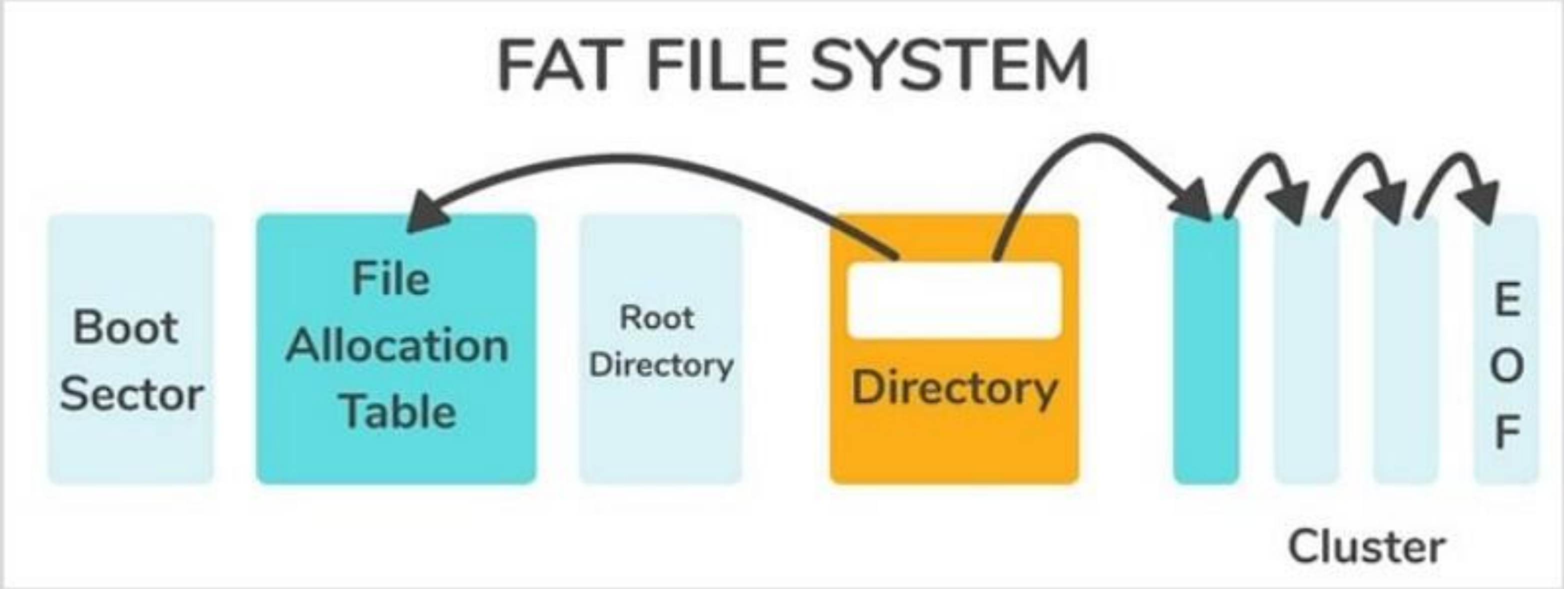
☑ Allow files on this drive to have contents indexed in addition to file properties

Common examples of File systems:

- **File Allocation Table (FAT):** FAT is a type of file system, which is **developed for hard drives.**
- **Global File System (GFS):** It has the ability t**o make enable multiple computers to act as an integrated machine**.
- **Hierarchical File System (HFS):** It is the file system that is used on a Macintosh computer **for creating a directory at the time a hard disk is formatted.**
- **NT File System (NTFS):** It is the file system, which stands for NT file system and **stores and retrieves files on Windows NT operating system** and other versions of Windows like Windows 2000, Windows XP, Windows 7, and Windows 10.

FAT File System

- **File Allocation Table (FAT)** is a file system created by Microsoft in 1977 for hard drives that initially relied on 12- or 16-bits.
- Operating systems utilize FAT to control documents on hard drives and other PCs.
- FAT File system is compatible with almost all popular operating systems such as Windows, Mac OS X, Unix, etc.
- There are typically four sections of the FAT File System listed below, each as a structure in the FAT partition.

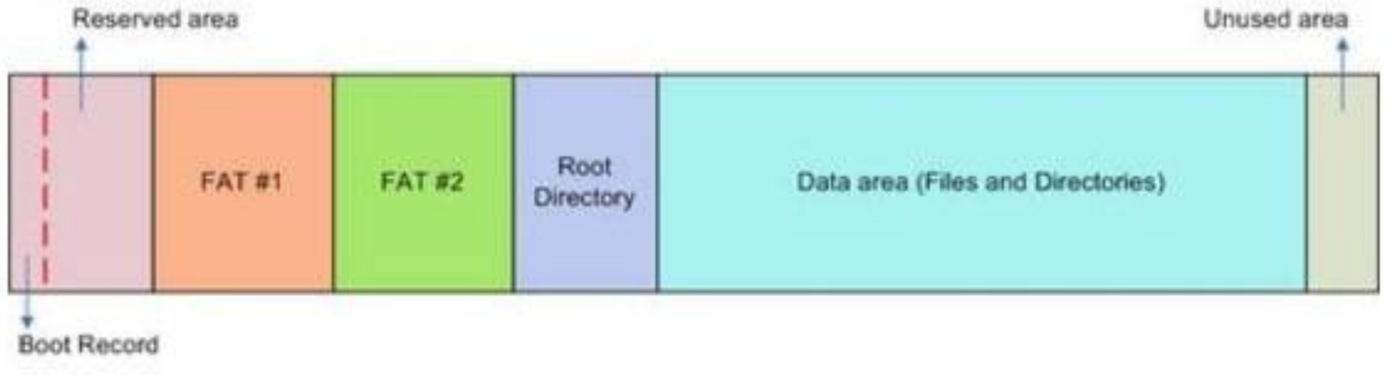


Boot Sector	Boot Sector contains machine startup code. It possesses information that the file system relies on for accessing the volume.
File Allocation Table	A FAT is a table that an operating system maintains on a hard disk that provides a map of clusters that a file has been stored in. Clusters are the basic units of logical storage on a hard disk.
Root Directory	The root directory has information about the files and directories located in the first cluster of that root directory. But it is only available in the FAT12 or FAT16 file system.
File Data Region	File Data Region is where the file data is stored. When we write a new file to a hard disk, the file is stored in one or more clusters that are not necessarily next to each other, they may be rather widely scattered over the disk.

- The OS creates a FAT entry for the new file that records where each cluster is located and their sequential order.
- When we read a file, the OS reassembles the file from clusters and places it as an entire file where we want to read it.

FAT 16

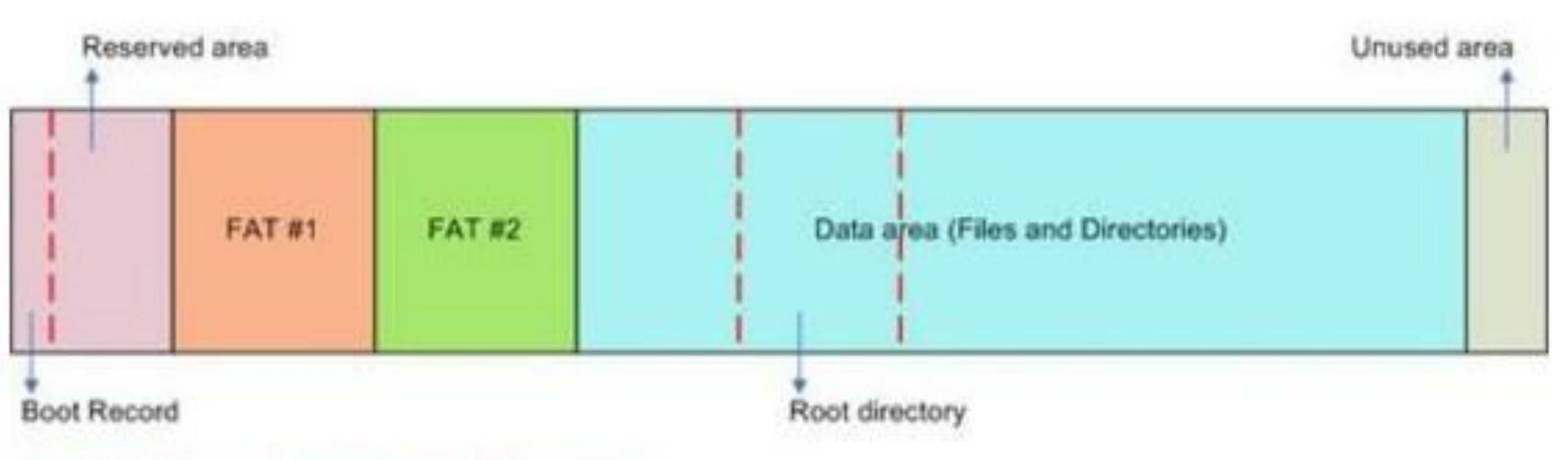
- This is the **16-bit version of the FAT file system.**
- The 16-bit part describes the way units are allocated on the drive.
- The FAT16 file system **uses a 16-bit number to identify each allocation unit** (called cluster), and this gives it a total of 65,536 clusters (ie. 2^{16})
- FAT16 was the default system for DOS and Linux systems that used hard drives up to a capacity of 4 GB.
- It was used in the first generation of flash memory portable devices, including MMC cards, SD cards, and flash drives.



The structure of FAT16 file system

FAT 32

- **FAT32** is the most recent version of the FAT file system, which was introduced in 1996 with the release of Windows 95 OSR2.
- It was designed to support larger disks than FAT16, with a maximum size of 2TB and a cluster size of up to 32KB.
- FAT32 is still widely used today, particularly on removable storage devices such as USB drives and SD cards.
- The FAT32 file system **uses a 32-bit number to identify each allocation unit** (called cluster), and this gives it a total of 4,294,967,296 clusters (ie. 2^{32})



The structure of FAT32 file system

VFAT

- A virtual file allocation table (VFAT) is an extension to the file allocation table (FAT) from Windows 95 and onward **for creating, storing and managing files with long names.**
- VFAT is the extension of the FAT12 and FAT16. It **addressed the major problem** that both FAT12 and FAT16 had – **the limit of filename size.**
- VFAT **enables a hard disk drive to store files with names** that are more than eight characters long.
- Unlike FAT, which restricts file names to having no more than eight characters, VFAT expanded that range to accommodate up to 255 characters.
- VFAT is also supported by other operating systems and is installed as a driver extension for all of them.

File Systems: NTFS

- NT file system (NTFS), which is also sometimes called the **New Technology File System**, is a process that the Windows NT operating system uses **for storing, organizing, and finding files on a hard disk** efficiently.
- NTFS was developed by Microsoft and launched in 1993 to replace its predecessor, the file allocation table (FAT) system, for better performance and enhanced data support.
- Recent Windows versions and various Windows Server use NTFS as the primary system.
- New Technology File System or NT File System (NTFS) provides virtual space to organize and store files.
- It also notes file positions in folders, creation dates, and details about access and provides data encryption.

File Systems: EXT4

- A widely **used file system in the Linux operating system.**
- It is the successor to Ext3 and offers several improvements in terms of performance, scalability, and reliability.
- Ext4 is the default file system for many Linux distributions.
- It was first introduced in 2003.

References:

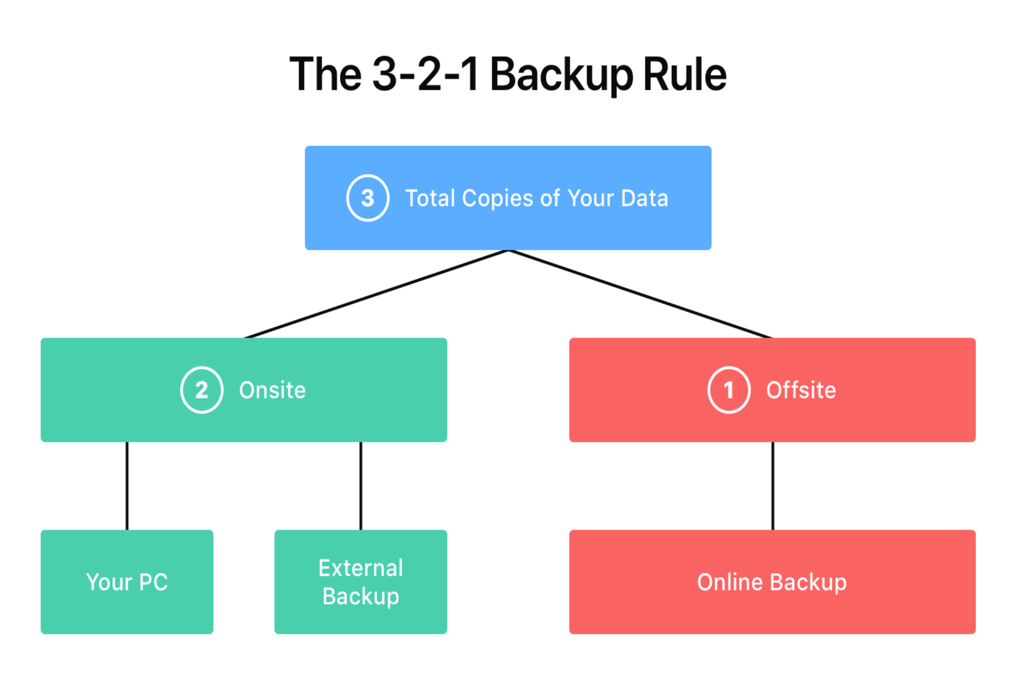
- https://recoverit.wondershare.com/file-system/fat16-file-system.html
- FAT https://www.youtube.com/watch?v=pUUP45WsYFw
- https://study.com/academy/lesson/files-systems-fat-ntfs-hfs-and-ffs.html

Basics of Data Backup and Restore

- Backup and recovery is the process of duplicating data and storing it in a secure place in case of loss or damage, and then restoring that data to a location — the original one or a safe alternative — so it can be again used in operations.

The 3-2-1 backup rule

- The 3-2-1 backup rule is a popular backup practice.
- It involves creating and maintaining:
  1. Three total copies of your data
  2. Two local copies — your original files and a backup stored on an **external hard drive**
  3. One offsite copy — such as a **cloud-based** backup
-

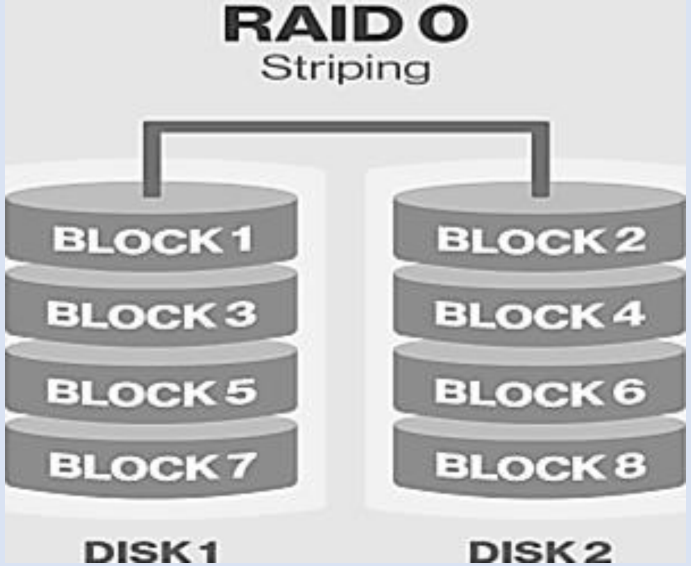


RAID

- Redundant Array of Independent Disk
- RAID is a set of physical disk devices viewed by the operating system as the single drive.
- RAID is a data storage virtualization technology that combines multiple physical disk drive components into a single logical unit for purpose of data redundancy, performance improvement, or both.

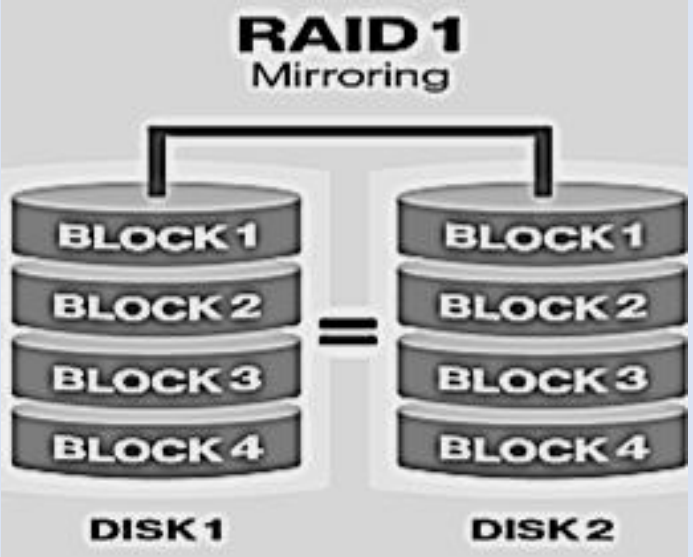
RAID 0 : Stripping

- Often called **striping** which is breaking of file into block of data
- Strips the block across disks in system
- Provide no redundancy or error detection



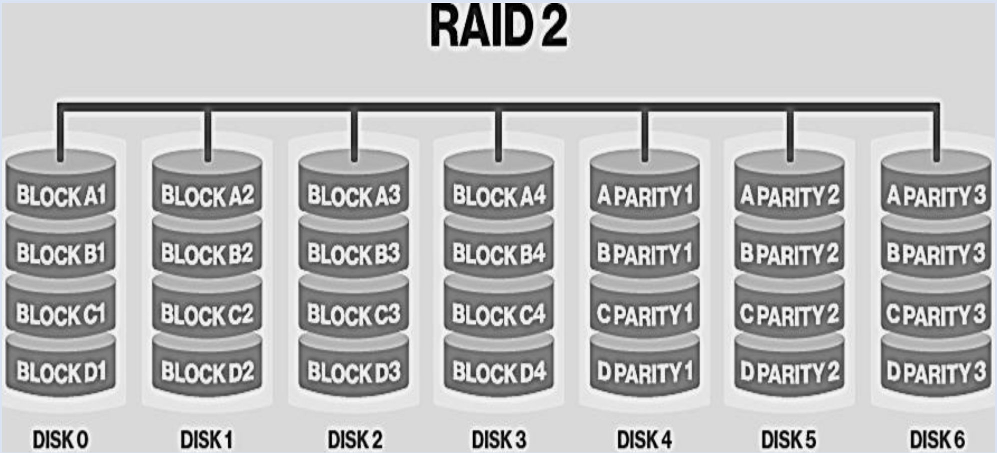
RAID 1: Mirroring

- A complete file is stored on a single disk
- Second disk contents the exact copy of file
- Provides complete redundancy of data



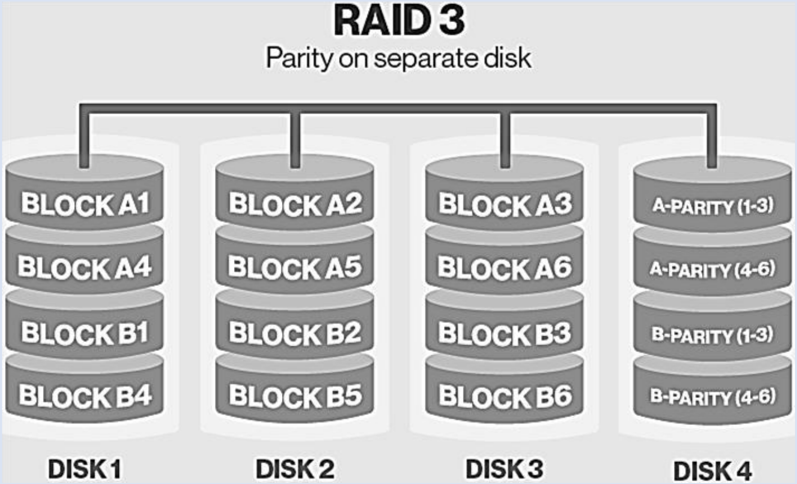
RAID 2 (Stripping and bit interleave)

- Strips data across disk similar to level 0, difference is data is bit interleaved instead of block interleaved
- Uses error control to monitor correctness of information on disk
- A parity disk is used to reconstruct corrupted or lost data



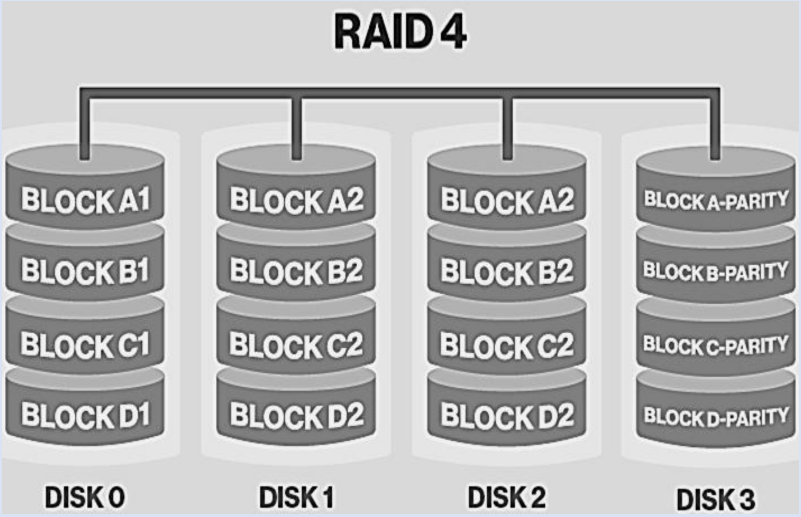
RAID 3: (Stripping and bit interleave & parity checking)

- One big problem with level 2 is the disk needed to detect which disk had an error
- Modern disk already determines if there is an error if sector is bad, the disk itself tell us and use the parity disk to correct it



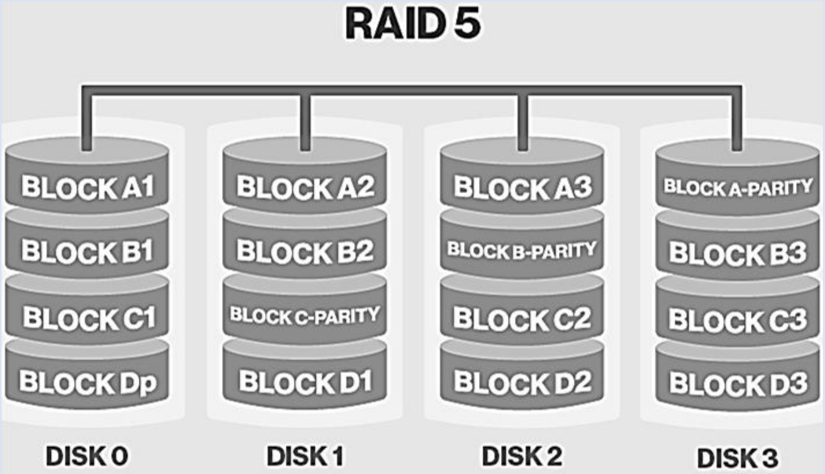
RAID 4: (Striping with block interleave &parity checking)

- It consists of a block level stripping with detected parity
- It allows multiple small I/O operations to be done at once.



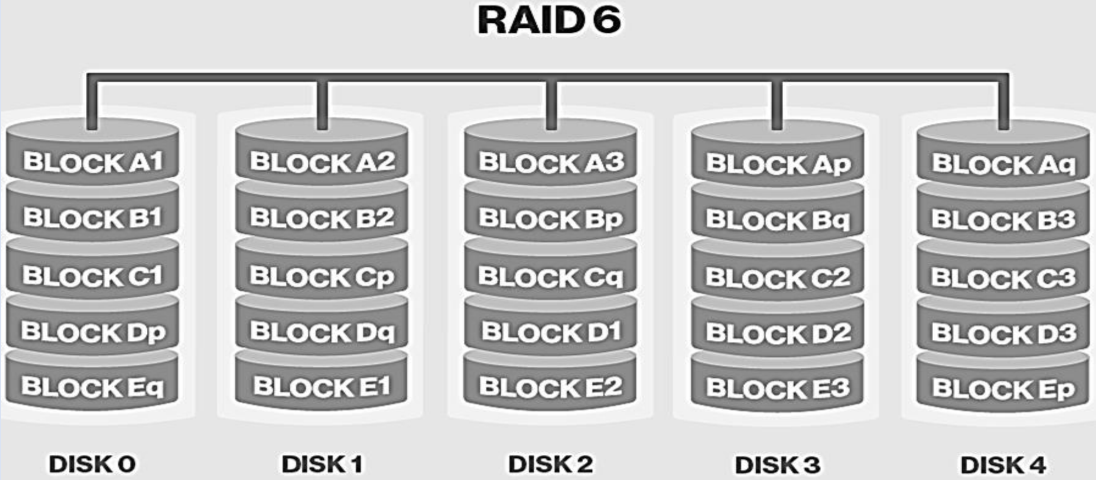
RAID 5: (Striping with block interleave & distributed parity checking)

- It consists of block level striping distributed parity
- Unlike in RAID 4 parity information is distributed among the drives
- It required at least three disks



RAID 6: (Striping with double parity checking)

- Consists of block level striping with double distributed parity
- Double parity provides fault tolerance up to 2 failed drives
- Requires minimum of four disks



Other RAID

- There are also other modification of RAID.
- **Refererence:** *https://www.youtube.com/watch?v=U-OCdTeZLac*

High Availability

- High availability (HA) is a system’s ability to operate continuously without experiencing failure for a predefined period.
- High Availability is about eliminating single points of failure, so it implies redundancy.
- There are basically 3 kinds of redundancy that are implemented in most systems: hardware, software, and environmental.
    - **Hardware Redundancy:** RAID, multiple power supplies, redundant networking, etc.
    - **Software Redundancy:** Clustering technologies such as database clusters
    - **Environmental redundancy:** Data center at different geographic region.

Disaster Recovery

- IT disaster recovery is a portfolio of policies, tools, and processes used to recover or continue operations of critical IT infrastructure, software, and systems after a natural or human-made disaster.
- A disaster recovery plan must address:
  - **Man-made disasters**—including cyber attacks, terrorism, and human error.
  - **Natural disasters**—including earthquakes, landslides, lightning, volcanic eruptions, wildfires, tornadoes, floods, hurricanes, and extreme weather conditions.
- An effective DR plan addresses three different elements for recovery:
  1. **Preventive:** Ensuring your systems are as secure and reliable as possible, using tools and techniques to prevent a disaster from occurring in the first place. This may include backing up critical data or continuously monitoring environments for configuration errors and compliance violations.
  2. **Detective:** For rapid recovery, you'll need to know when a response is necessary. These measures focus on detecting or discovering unwanted events as they happen in real time.
  3. **Corrective:** These measures are aimed at planning for potential DR scenarios, ensuring backup operations to reduce impact, and putting recovery procedures into action to restore data and systems quickly when the time comes.

Open-source Systems

- Open source software is computer software whose source code is available openly on the internet and programmers can modify it to add new features and capabilities without any cost.
- Here the software is developed and tested through open collaboration. This software is managed by an open-source community of developers.
- It provides community support, as well as commercial support, which is available for maintenance.
- We can get it for free of cost. This software also sometimes comes with a license and sometimes does not.
- This license provides some rights to users.
    - The software can be used for any purpose
    - Allows to study how the software works
    - Freedom to modify and improve the program
    - No restrictions on redistribution
- Some **examples of Open source software** include Android, Ubuntu, Firefox, Open Office, etc.

Proprietary Softwares

- Proprietary software is computer software where the source codes are publicly not available only the company that has created them can modify it.
- Here the software is developed and tested by the individual or organization by which it is owned not by the public.
- This software is managed by a closed team of individuals or groups that developed it. We have to pay to get this software and its commercial support is available for maintenance.
- The company gives a valid and authenticated license to the users to use this software.
- But this license puts some restrictions on users also like.
    - Number of installations of this software into computers
    - Restrictions on sharing of software illegally
    - Time period up to which software will operate
    - Number of features allowed to use
- Some **examples of Proprietary software** include Windows, macOS, Internet Explorer, Google Earth, Microsoft Office, etc.

Assignment:

- Differentiate between Proprietary and Open source software.

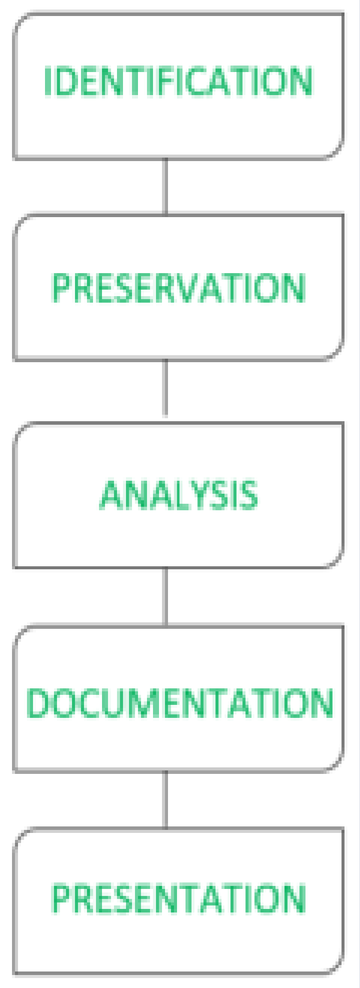
- Reference: https://www.shiksha.com/online-courses/articles/difference-between-open-source-software-and-proprietary-software-blogId-153109

Introduction to Digital Forensic

- Digital forensics is the process of **storing**, **analyzing**, **retrieving**, and **preserving electronic data** that may be useful in an investigation.
- It includes data from hard drives in computers, mobile phones, smart appliances, vehicle navigation systems, electronic door locks, and other digital devices.
- The process's goal of digital forensics is **to collect, analyze, and preserve evidence.**
- It is a method of discovering proofs from digital media like a PC, mobile or cellular devices, servers, or networks.
- It gives the forensic department group the elite procedures and equipment to resolve difficult digital cases of crimes.

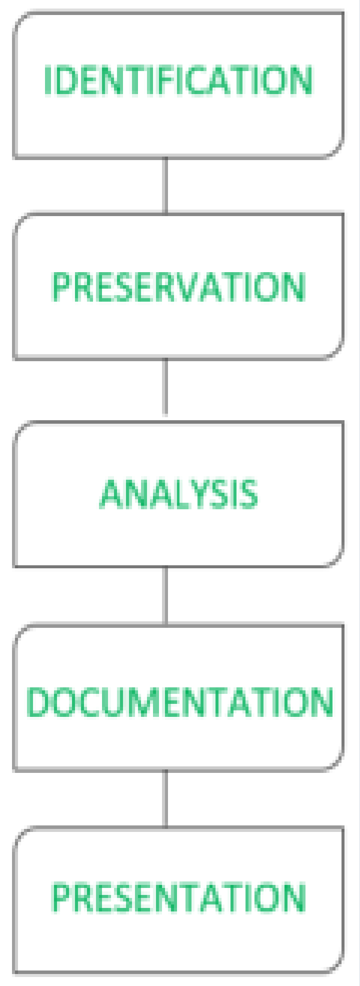
- Reference:
  - https://www.youtube.com/playlist?list=PLa2xctTiNSCiTGuejkc05zsr-G5t9AuH8
  - https://www.geeksforgeeks.org/introduction-of-computer-forensics/
  - https://www.simplilearn.com/what-is-digital-forensics-article

Steps of Digital Forensic



1. **Identification**
   - This is the initial stage in which the individuals or **devices to be analyzed are identified** as likely sources of significant evidence.
   - It is the first and fore more step in the process, including the forensic process, like where the evidence is found, where it is preserved, and how it is stored.
2. **Preservation**
   - It **focuses on safeguarding relevant electronically stored information (ESI)** by capturing and preserving the crime scene, documenting relevant information such as visual images, and how it was obtained.
   - An isolating place **stores the evidence to secure and preserve it from theft**. People are prevented from buying digital devices to ensure no proof is meddled with.

Steps of Digital Forensic



3. Analysis

- It is a **methodical examination of the evidence of the information gathered**. This examination produces data objects, including system and user-generated files, and seeks specific answers and points of departure for conclusions.
- In this phase, the inspection group will reform the chunks of evidence and determine the outcome based on the resulting proofs or evidence. But it may sometimes take several iterations to discover the support on a criminal case.

4. Documentation

- These are **tried-and-true procedures for documenting** the analysis's conclusions, and they must allow other competent examiners to read through and duplicate the results.
- In this stage, **all possible evidence of data is drawn from the given inputs**.
- It will help in rebuilding the crime scene and analyzing it.
- The investigators document the correct documentation of the crime scenes by mapping the crime scene, sketching it, and then relating its photographs with the documents.

5. Presentation

- we summarize and explain the documents.

Types of Digital Forensics

As digital data forensics evolves, several sub-disciplines emerge, some of which are listed below:

1. **Computer Forensics**
   - It **analyzes digital evidence obtained from laptops, computers, and storage media** to support ongoing investigations and legal proceedings.
2. **Mobile Device Forensics**
   - It entails **obtaining evidence from small electronic devices such as personal digital assistants, mobile phones, tablets, sim cards, and gaming consoles.**
3. **Network Forensics**
   - Network or cyber forensics depends on the **data obtained from monitoring and analyzing cyber network activities** such as attacks, breaches, or system collapse caused by malicious software and abnormal network traffic.

3. **Digital Image Forensics**
   - This sub-specialty **focuses on the extraction and analysis of digital images to verify authenticity** and metadata and determine the history and information surrounding them.
4. **Digital Video/Audio Forensics**
   - This field **examines audio-visual evidence to determine its authenticity** or any additional information you can extract, such as location and time intervals.
5. **Memory Forensics**
   - It refers to the **recovery of information from a running computer's RAM** and is also known as live acquisition.
   - **collects the data from the computer’s cache memory or RAM** dump and then gathers the evidence.

Challenges in Digital Forensics

- **Extracting data from locked, or destroyed computing devices** is one of the challenges that digital forensic investigators face
- **Finding specific data** entries within massive amounts of data stored locally or in the cloud
- **Keeping track of the digital chain** of custody
- **Ensuring data integrity** throughout an investigation

Exercise:

1. Define Computer Network. Mention its advantages and disadvantages.
2. How Client-server Architecture is different from Peer2Peer Architecture?
3. Mention the types of network on the basis of geographic coverage.
4. Explain the functionality of each layer in the OSI stack protocol.
5. Explain the layers in TCP/IP model.
6. Differentiate between TCP and UDP protocol.
7. What is IP address? How IPV4 differs from IPV6?
8. What is the reason for introducing IPV6 in spite of IPV4?
9. Explain class A, class B and class C IP address.
10. What is a subnet? What are the benefits of subnetting a network?
11. What is the significance of understanding basic concepts in cybersecurity and networking?

12. Define the term: Encryption and Decryption.
13. Define cryptography. Explain its types.
14. Provide an example of Vigenère Cipher cryptography and explain it.
15. Provide an example of Rail-fence Cipher cryptography and explain it.
16. What are public and private key in cryptography?
17. What do you mean by hash function? How hash function is used in cryptography?
18. How End-to-End encryption (E2EE) secures digital communication? Explain.
19. How SHA is different from Message Digest (MD) ?
20. Explain the CIA triad with suitable example.
21. Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system. In each case, indicate the degree of importance of the requirement.

22. Introduce steganography with its types.
23. How does steganography differ from cryptography?
24. What is cryptocurrency? Provide some examples.
25. What are storage devices?
26. Explain the FAT file system.
27. What are FAT 16, FAT 32 , VFAT and EXT4 file system?
28. Why modern technology uses NTFS system?
29. What are the advantages of using NTFS over FAT32?
30. Why is the necessity of Backup? Explain.
31. Why is data backup critical for businesses and individuals?
32. How often should data backups be performed?
33. What are the different types of data backup (full, incremental, differential)?

34. Explain the 3-2-1 backup rule. How does it provide compliance with CIA triad?
35. What is RAID technology? Explain mirroring and stripping in RAID.
36. What is disaster recovery? Mention three elements for recovery for an effective Data recovery plan.
37. What is disaster recovery and how does it differ from regular data backup?
38. Differentiate between proprietary and open-source softwares with suitable examples.
39. How do high availability systems ensure continuous operation?
40. Introduce digital forensic. Also mention the challenges in it.
41. Explain the steps involved in digital forensic.
42. Explain different types of digital forensic.
43. When renaming a file, does its hash value change? Explain.
44. Explain the various types of File Systems.

End of Chapter