COMPUTER: A computer is an electronic device that accepts data/inputs from its user and processes it into useful information as per the processing instructions to generate the output.

Generations	**Period**	**Technology Used**
First Generation	1946-1959	Vacuum tube-based
Second Generation	1959-1965	Transistor-based
Third Generation	1965-1971	Integrated Circuit based
Fourth Generation	1971-1980	VLSI microprocessor-based
Fifth Generation	1980-onwards	ULSI microprocessor-based

First Generation : 1946-1959

Vacuum Tubes

In first stage of computer development we used vacuum tubes. These vacuum tubes are slower in processing speed and used machine language which was hard to understand as instruction was in 0 and 1.These first generation computer was bigger in size even occupied entire room , generates lot of heat and was very expensive So these cant be used continuously for longer duration of time

Second Generation : 1959-1965

Transistor

In second generation of computer we used transistors. In Second generation vacuum tubes was replaced with transistor. Second generation saw the improvement in speed and size but heat produced was still damaging to the system

Language used was assembly language , which means it was easy to understand as instructions consist of words.

Third Generation : 1964-1971

Integrated Circuits

Third generation saw the used to integrated circuits. Transistor were miniaturized and put on chip to foam integrated circuit .Which was faster in processing speed, store instruction in memory and reduced in size. These extremely small electronics can perform calculations and store data using either digital or analog technology.

Fourth Generation :1972-2010

Microprocessor

Crucial stage in the development of computer was microprocessor . Intel was first to develop microprocessor. In microprocessor ten of millions of transistor fabricated on single chip which is very small in size and also have very high processing capabilities

Microprocessor support multiple task This generation saw the development of computer for home use developed by IBM.

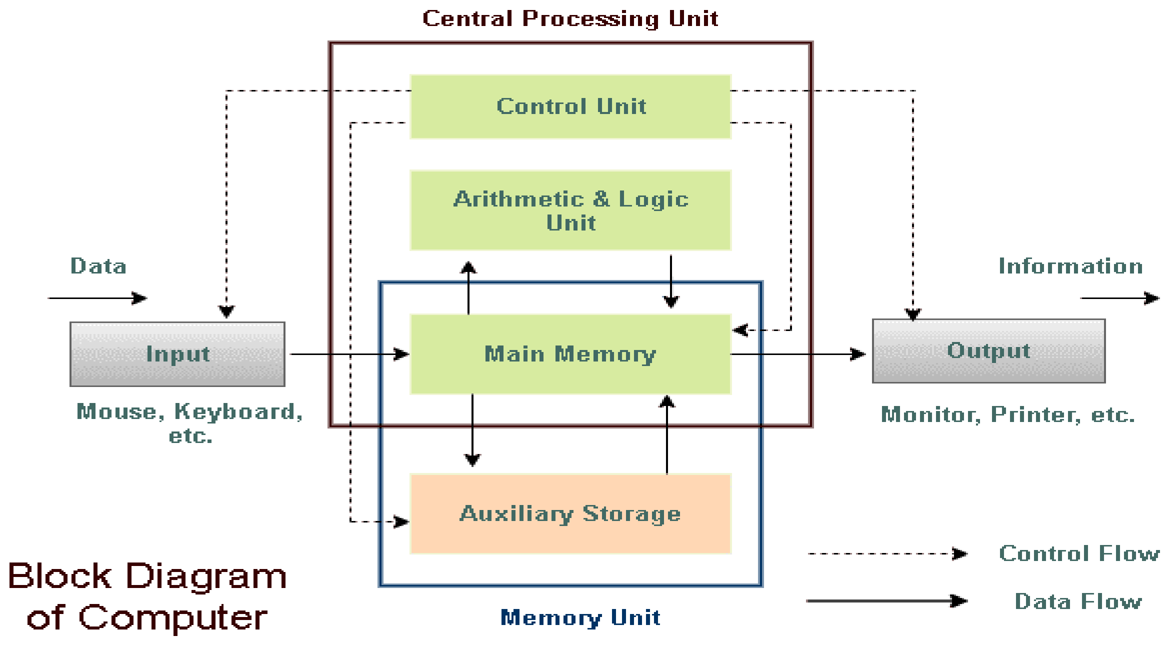
Fifth Generation : 2010- Onwards

Artificial Intelligence

Fifth generation saw the advent of artificial intelligence, features like voice recognition are made possible with artificial intelligence as machine able to respond in natural language and have capability to learn and organize themselves.

Fifth generation is still in development stage

BLOCK DIAGRAM OF COMPUTER



Central Processing Unit (CPU)

The CPU can be called the brain of a computer system.

The central processing unit (CPU) is where the majority of the important calculations and comparisons are performed. In addition, the CPU is in charge of turning on and controlling the operation of the other units.

The arithmetic logic unit, also known as the ALU, and the control unit (CU) are the two primary elements that make up this unit. First, let's take a moment to briefly define these two different units of CPU.

Arithmetic Logic Unit (ALU)

The arithmetic logic unit is responsible for carrying out all of the mathematical operations, including addition, subtraction, multiplication, and division. In addition to that, a logical operation is used for the comparison.

Control Unit (CU)

In addition, the control unit of a central processing unit is responsible for directing the overall operation of a computer. In addition to this, it exercises control over all devices connected to the CPU, including memory and input/output devices.

The CU is responsible for retrieving instructions from memory, decoding those instructions, interpreting those instructions to determine what tasks are to be carried out, and then sending appropriate control signals to the other components so that they can carry out the steps necessary to execute the instruction.

Input/Output Unit

The input/output unit is made up of different devices that are responsible for transmitting and receiving information between the memory of the computer and the outside world.

The information that is entered into the computer via the input unit is saved in the memory of the device for later processing. The completed processing can then be saved in the memory and either recorded or displayed on the output medium.

Memory Unit

Memory units are an integral part of any modern digital computer. It is the repository for all of the results, both intermediate and final.

The data that are read from the primary storage or an input unit are moved to the memory of the computer so that they can be processed. These data can come from either the main storage or an input unit.

The data that needs to be processed and the instructions that need to be carried out are both stored in this memory unit so they can be accessed quickly.

Disk Storage Unit

Before a computer can begin the process of actually using the data and instructions that it has received from an input device, the data and instructions must first be stored inside the computer.

Primary and secondary storage units are the two categories that can be found in a storage facility. Now let's briefly define these two storage units one by one, starting with the "primary storage unit."

Primary Storage Unit

Primary memory is connected to the input unit as well as the output unit in a straightforward manner. It stores both the data that was input and the result of the calculation.

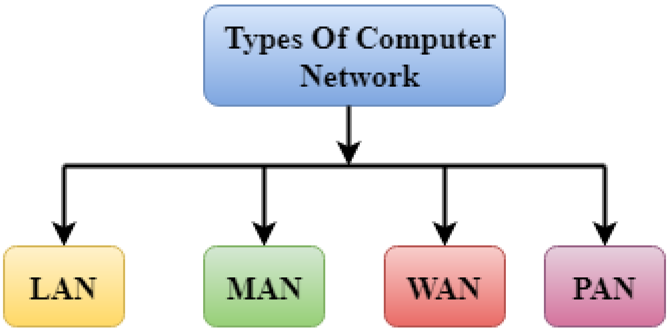
Secondary Storage Unit

It is not possible to store data permanently on the primary storage for use at a later time. Because of this, additional forms of data storage technology, also known as secondary or auxiliary storage, are required in order to store the data in a manner that is both permanent and accessible over an extended period of time.

Computer Network Types

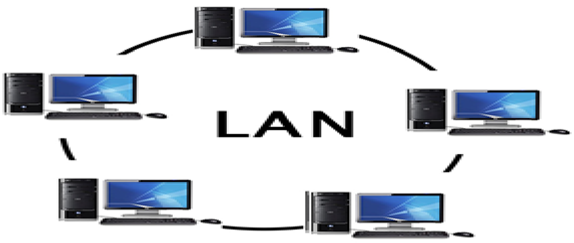
A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size. A computer network is mainly of four types:



LAN(Local Area Network)

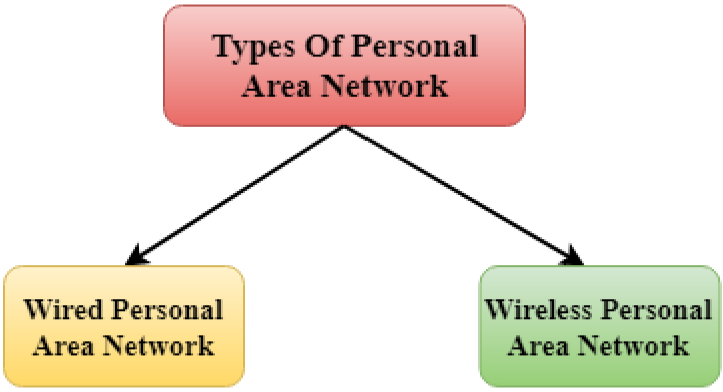
- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.



PAN(Personal Area Network)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- Thomas Zimmerman was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of 30 feet.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

There are two types of Personal Area Network:


Types Of Personal Area Network
Wired Personal Area Network
Wireless Personal Area Network

- Wired Personal Area Network
- Wireless Personal Area Network

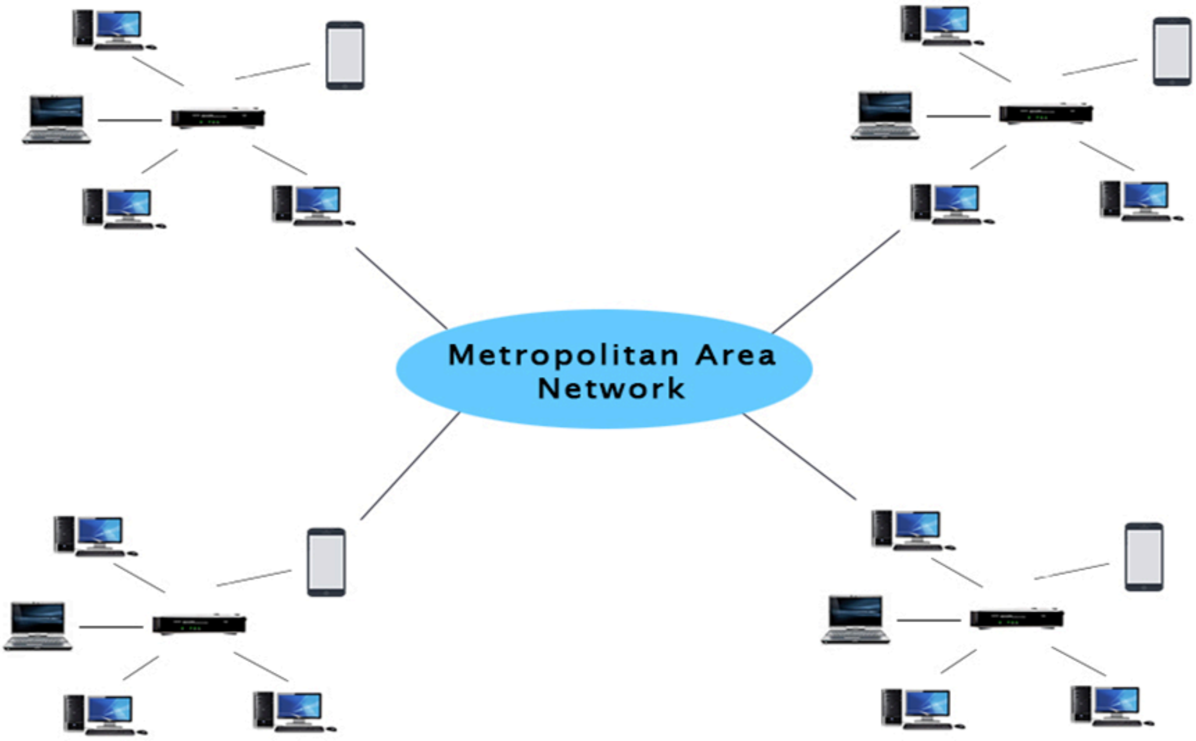
Wireless Personal Area Network: Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.

Wired Personal Area Network: Wired Personal Area Network is created by using the USB.

MAN(Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.

- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network(LAN).



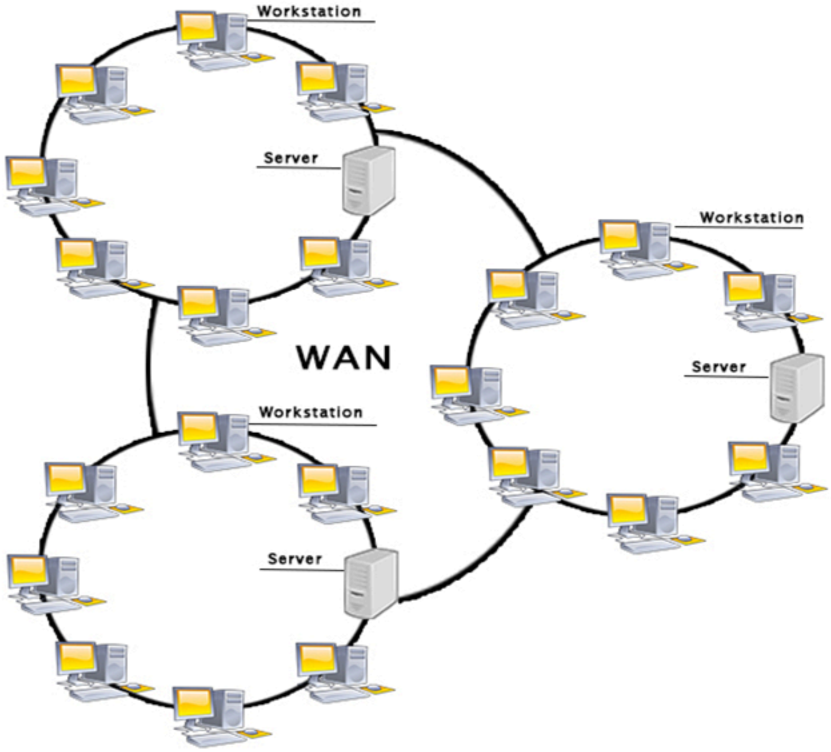
Uses Of Metropolitan Area Network:

- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

WAN(Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.

- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.



Examples Of Wide Area Network:

- Mobile Broadband: A 4G network is widely used across a region or country.
- Last mile: A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
- Private network: A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

Advantages Of Wide Area Network:

- **Geographical area**: A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.
- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files**: Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global business**: We can do the business over the internet globally.
- **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages of Wide Area Network:

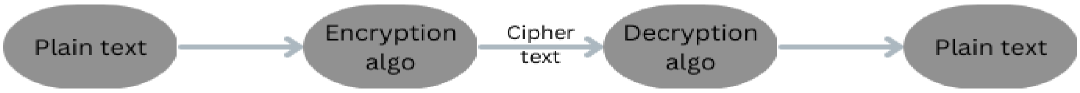
- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

Cryptography and its Types

The prefix “crypt” means “hidden” and suffix “graphy” means “writing”. In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it.

Encryption: The process of changing the plaintext into the ciphertext is referred to as encryption.

Decryption: The process of changing the ciphertext to the plaintext that process is known as decryption.



Features Of Cryptography are as follows:

1. **Confidentiality**: Information can only be accessed by the person for whom it is intended and no other person except him can access it.
2. **Integrity:** Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. **Non-repudiation:** The creator/sender of information cannot deny his intention to send information at later stage.
4. **Authentication**: The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types Of Cryptography:

1. **Symmetric Key Cryptography:** It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system are Data Encryption System(DES) and Advanced Encryption System(AES).

2. **Hash Functions**: There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
3. **Asymmetric Key Cryptography**: Under this system a pair of keys is used to encrypt and decrypt information. A receiver’s public key is used for encryption and a receiver’s private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone know his private key. The most popular asymmetric key cryptography algorithm is RSA algorithm.

Applications Of Cryptography:

Computer passwords: Cryptography is widely utilized in computer security, particularly when creating and maintaining passwords. When a user logs in, their password is hashed and compared to the hash that was previously stored. Passwords are hashed and encrypted before being stored. In this technique, the passwords are encrypted so that even if a hacker gains access to the password database, they cannot read the passwords.

Digital Currencies: To safeguard transactions and prevent fraud, digital currencies like Bitcoin also use cryptography. Complex algorithms and cryptographic keys are used to safeguard transactions, making it nearly hard to tamper with or forge the transactions.

Secure web browsing: Online browsing security is provided by the use of cryptography, which shields users from eavesdropping and man-in-the-middle assaults. Public key cryptography is used by the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols to encrypt data sent between the web server and the client, establishing a secure channel for communication.

Electronic signatures: Electronic signatures serve as the digital equivalent of a handwritten signature and are used to sign documents. Digital signatures are created using cryptography and can be validated using public key cryptography. In many nations, electronic signatures are enforceable by law, and their use is expanding quickly.

Authentication: Cryptography is used for authentication in many different situations, such as when accessing a bank account, logging into a computer, or using a secure network. Cryptographic methods are employed by authentication protocols to confirm the user's identity and confirm that they have the required access rights to the resource.

Cryptocurrencies: Cryptography is heavily used by cryptocurrencies like Bitcoin and Ethereum to safeguard transactions, thwart fraud, and maintain the network's integrity. Complex algorithms and cryptographic keys are used to safeguard transactions, making it nearly hard to tamper with or forge the transactions.

End-to-End Encryption: End-to-end encryption is used to protect two-way communications like video conversations, instant messages, and email. Even if the message is encrypted, it assures that only the intended receivers can read the message. End-to-end encryption is widely used in communication apps like WhatsApp and Signal, and it provides a high level of security and privacy for users.

Advantages

1. **Access Control:** Cryptography can be used for access control to ensure that only parties with the proper permissions have access to a resource. Only those with the correct decryption key can access the resource thanks to encryption.
2. **Secure Communication:** For secure online communication, cryptography is crucial. It offers secure mechanisms for transmitting private information like passwords, bank account numbers, and other sensitive data over the internet.
3. **Protection against attacks:** Cryptography aids in the defence against various types of assaults, including replay and man-in-the-middle attacks. It offers strategies for spotting and stopping these assaults.
4. **Compliance with legal requirements:** Cryptography can assist firms in meeting a variety of legal requirements, including data protection and privacy legislation.