University of Global Village (UGV), Barishal

Content of the Theory Course

University Student (UGV)

Course Title: Computer Fundamental

Course Code: CSE-1101

Program: Bachelor of Science in Computer Science & Engineering (CSE)

Course Code: CSE-1101
Name of Course Title: Computer Fundamental
Course Type: Core Course
Level: 1st Semester (Even)

Name(s) of Academic Course teacher(s):
Sohag Mollik
Lecturer,
CSE at UGV
Mobile: 01304142395
E-mail: sohag.cse.just@gmail.com

COMPUTER FUNDAMENTAL

Course Code: CSE-1101	Credits: 3
Exam hours: 3	CIE Marks: 90
	SEE Marks: 60

Course Learning Outcome (CLOs): After Completing this course successfully, the student will be able to…

CLO1	Understand the fundamental concepts of computer systems, including the components of a computer, computer organization, and how data is represented and processed by a computer.
CLO2	Identify and use common computer software applications, including operating systems, word processing, spreadsheets, and presentation software.
CLO3	Demonstrate proficiency in using computer hardware and peripherals, including input and output devices, storage devices, and networking equipment.
CLO4	Analyse and evaluate ethical and social issues related to computer usage, including privacy, security, intellectual property, and accessibility.
CLO5	Apply problem-solving and critical thinking skills to troubleshoot common computer issues, perform basic maintenance tasks, and effectively communicate technical information to a non-technical audience.

SUMMARY OF COURSE CONTENT:

Sl. No.	COURSE CONTENT	HRs	CLOs
1	Introduction to Computers: This section covers the basics of computing including a brief history of computers, hardware and software components, input/output devices, and the role of operating systems.	9	CLO1 CLO2
2	Computer Arithmetic: This section covers the fundamental concepts of computer arithmetic including binary and hexadecimal number systems, binary arithmetic, signed numbers, and floating-point arithmetic.	9	CLO3
3	Computer Programming: This section covers the basics of programming including algorithms, flowcharts, data types, variables, expressions, and control structures.	9	CLO4
4	Data Storage and Management: This section covers the basics of data storage and management including storage devices, data representation, file management, and database concepts.	9	CLO4 & CLO5
5	Computer Networks: This section covers the basics of computer networks including network architecture, network topologies, communication protocols, and internet basics. It also includes an overview of network security and management.	9	CLO5

RECOMMENDED BOOKS:

1. "Computer Fundamentals" by P.K. Sinha
2. "Computer Organization and Design" by David A. Patterson and John L. Hennessy
3. "Operating System Concepts" by Abraham Silberschatz, Greg Gagne, and Peter B. Galvin
4. "Introduction to Algorithms" by Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein
5. "Computer Networks" by Andrew S. Tanenbaum and David J. Wetherall

ASSESSMENT PATTERN

CIE- Continuous Internal Evaluation (90 Marks)

Bloom's Category Marks (out of 90)	Tests (45)	Assignments (15)	Quizzes (15)	Attendance (15)
Remember	5	03		
Understand	5	04	05	
Apply	15	05	05	
Analyze	10			
Evaluate	5	03	05	
Create	5			

SEE- Semester End Examination (60 Marks)

Bloom's Category	Test
Remember	7
Understand	7
Apply	20
Analyze	15
Evaluate	6
Create	5

COURSE PLAN

Week	Topics	Teaching Learning Strategy(s)	Assessment Strategy(s)	Alignment to CLO
1	Introduction to Computers and Their Components	Lecture, multimedia, discussions	Feedback, Q&A, assessment	CLO1 & CLO2
2	Computer Memory	Lecture, discussions	Q&A, assignments	CLO1
3	Input Devices	Lecture, multimedia	Quiz & assessments	CLO3
4	Output Devices	Lecture, multimedia	Q&A assessments	CLO3
5	Central Processing Unit (CPU)	Lecture, Practical implementation	Feedback, Q&A, assessment	CLO1 & CLO3
6 & 7	Number System	Lecture, Practical implementation	Q&A, assignments	CLO1
7 & 8	Boolean Algebra	Lectures, discussions	Midterm assessments	CLO1 & CLO2
9 & 10	Mid Examination	Mid-term exams	Mid-term assessment	CLO1 – CLO3
11	Logic Gates	Lecture, Practical implementation	Q&A, assignments	CLO1 & CLO3
12	Introduction to Basic Networking Concepts	Lecture, multimedia, discussions	Ethical analysis, Midterm assessments	CLO3, CLO5
13	Operating Systems: Functions, Booting, and Types	Interactive lectures, examples from real-world applications	Final term assessments	CLO5
14	Computer Security: Viruses, Infection Mechanisms, and Antivirus Protection	Lecture, multimedia, discussions	Final term assessments	CLO5

COURSE PLAN

15 & 16	Core Programming Concepts: Algorithms, Flowcharts, and Pseudocode	Interactive lectures, examples from real-world applications	Feedback, Q&A, assessment	CLO4
17	Final Topics Review and Discussion: Integration of Concepts	Revision through Q&A, group activities	Participation, group evaluation	CLO1 - CLO5

Week 1

Introduction to Computers and Their Components

Page
10-25

❖Computer

A Computer is a machine that can be programmed to accept data, process data into useful information and store it for later use.

A computer consists of Hardware and Software.

The machine is known as Hardware.

The programs are called Software.

Hardware & Software

- Hardware

Physical parts of the computer, including processor and memory chips, input/output devices, tapes, disks, modems, cable, etc.

- Software

Programs that tell the computer what to do. It provides instructions that the CPU will need to carry out.

❖ Components of a Computer System

- Input Devices
- Processing Device
- Output Devices
- Storage Devices

- Input Devices

The data that is given to the computer is called Input. Input devices are used to input data and instructions into the computer. These devices send this data to the Processing Unit.

Following are some examples of Input devices :-

- # PROCESSING DEVICE

The **Processor** is used to process data. It is also called Central Processing Unit (CPU). It is the brain of the computer. It consists of electronics circuit. CPU interprets and executes program instructions. All computers must have a Central Processing Unit.

Following are some Examples of CPU :-

- Output Devices

The data processed into useful information is called output. Output devices are used to display the result of processing.

Following are some examples of output devices :-

SPEAKER

MONITOR

HEADPHONE

Output Devices of Computer

PLOTTER

PROJECTOR

www.examplesof.net

PRINTER

• Storage Devices

Storage usually refers to the **Secondary storage**. The main memory stores data and programs temporary & is called **Primary Storage**. The **Secondary storage** is required to store Data , Information and Programs permanently.

Following are some examples of storage devices :-

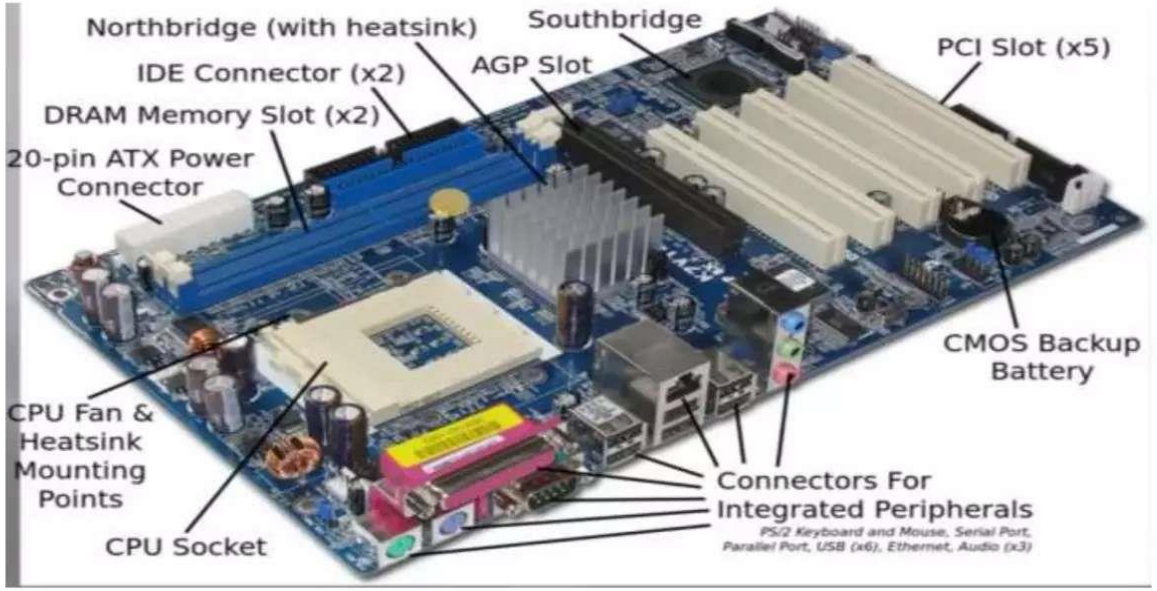
- Primary Storage Devices

RAM
(Random Access Memory)

ROM
(Read Only Memory)

- Secondary Storage Devices

Motherboard



A **Motherboard** is one of the most essential **parts** of a **computer system**. It holds together many of the crucial **components** of a **computer**, including the central processing unit (CPU), memory and connectors for input and output devices.

It is a large board with integrated circuits that connect the various parts of computer e.g CPU, RAM, Disk Drives (CD, DVD, Hard disk) etc.

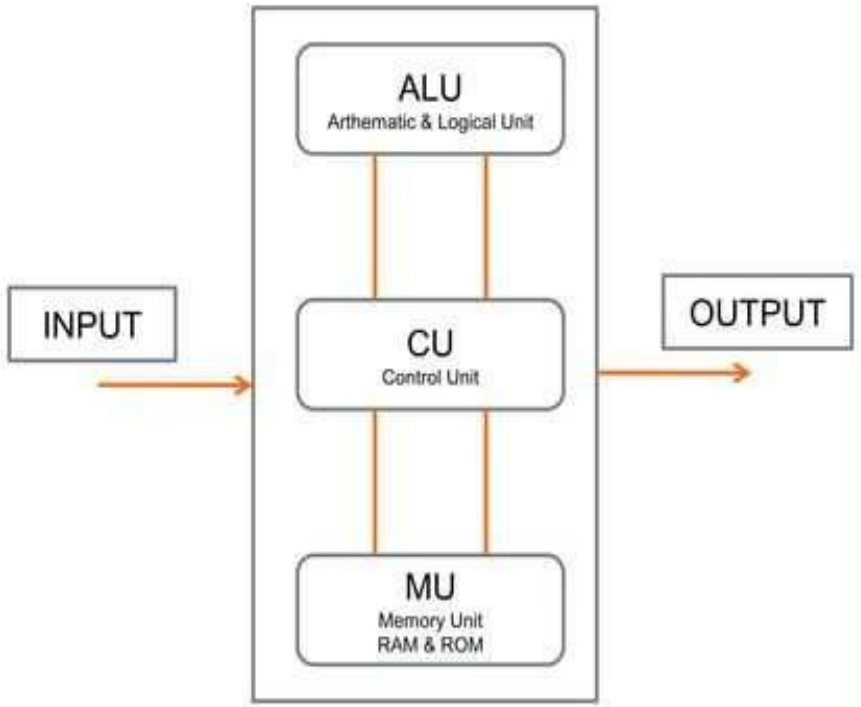
The Main Components which are directly attached to the Motherboard include :-

- CPU
- RAM
- ROM
- Connectors for Peripherals
- Internal bus

❑ **Note**

It is to be noted that all Components of Computer System are Linked with each other on a Motherboard . The Motherboard acts as a base for the communication or Interaction of Computer's different Components.

Parts of Computer (Block Diagram)



- Conclusion

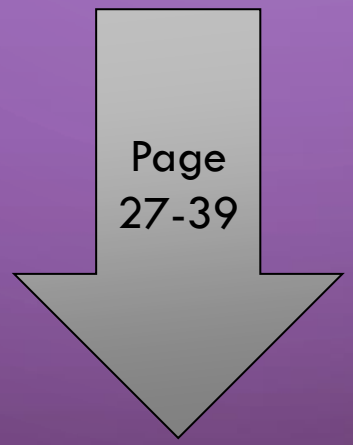
A computer system requires different components to perform the functions of Input, Processing, Output and Storage and these four components are necessary for a computer to work.

Self Study

Review & explore this topics

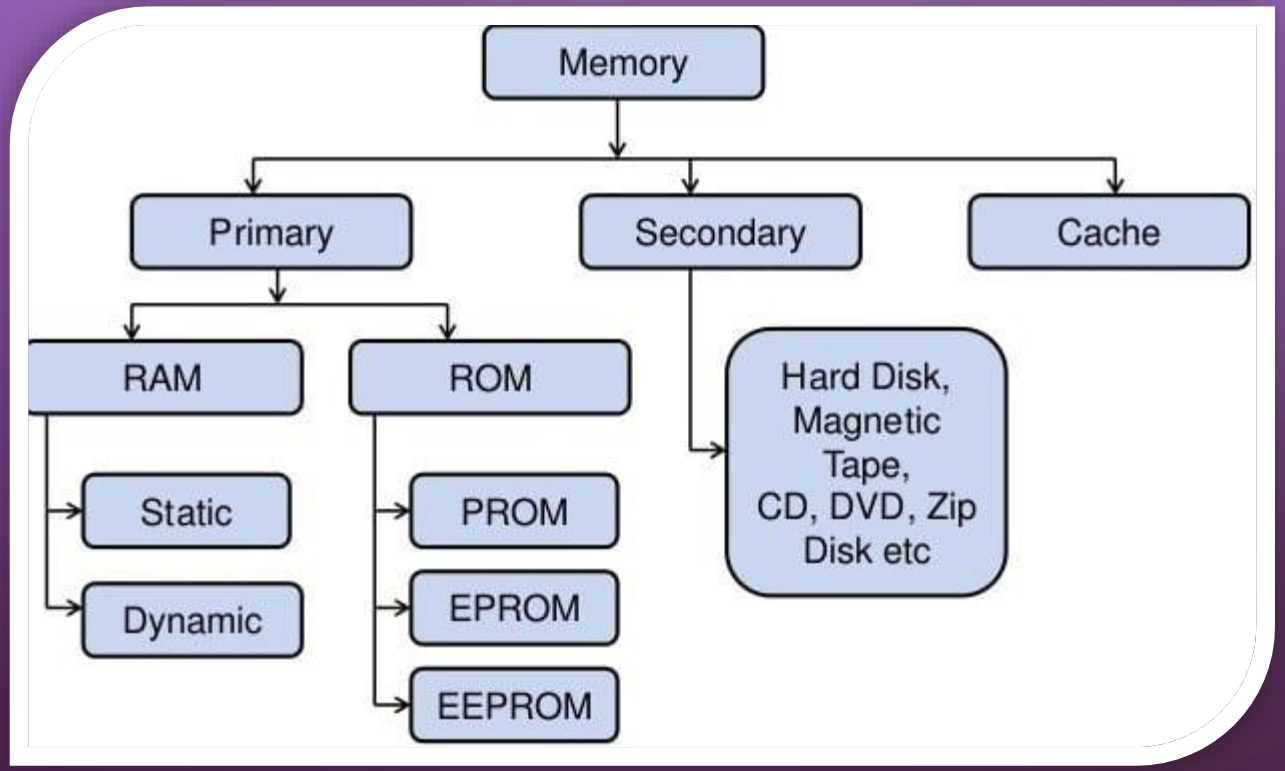
Week 2

Computer Memory



COMPUTER MEMORY

Computer memory, device that is used to store data or programs (sequences of instructions) on a temporary or permanent basis for use in an electronic digital computer. Computers represent information in binary code, written as sequences of 0s and 1s.



CHARACTERISTICS OF MEMORIES

1. Volatility

- Volatile {RAM}
- Non-volatile {ROM, Flash memory}

2. Mutability

- Read/Write {RAM, HDD, SSD, RAM, Cache, Registers…}
- Read Only {Optical ROM (CD/DVD…), Semiconductor ROM}

3. Accessibility

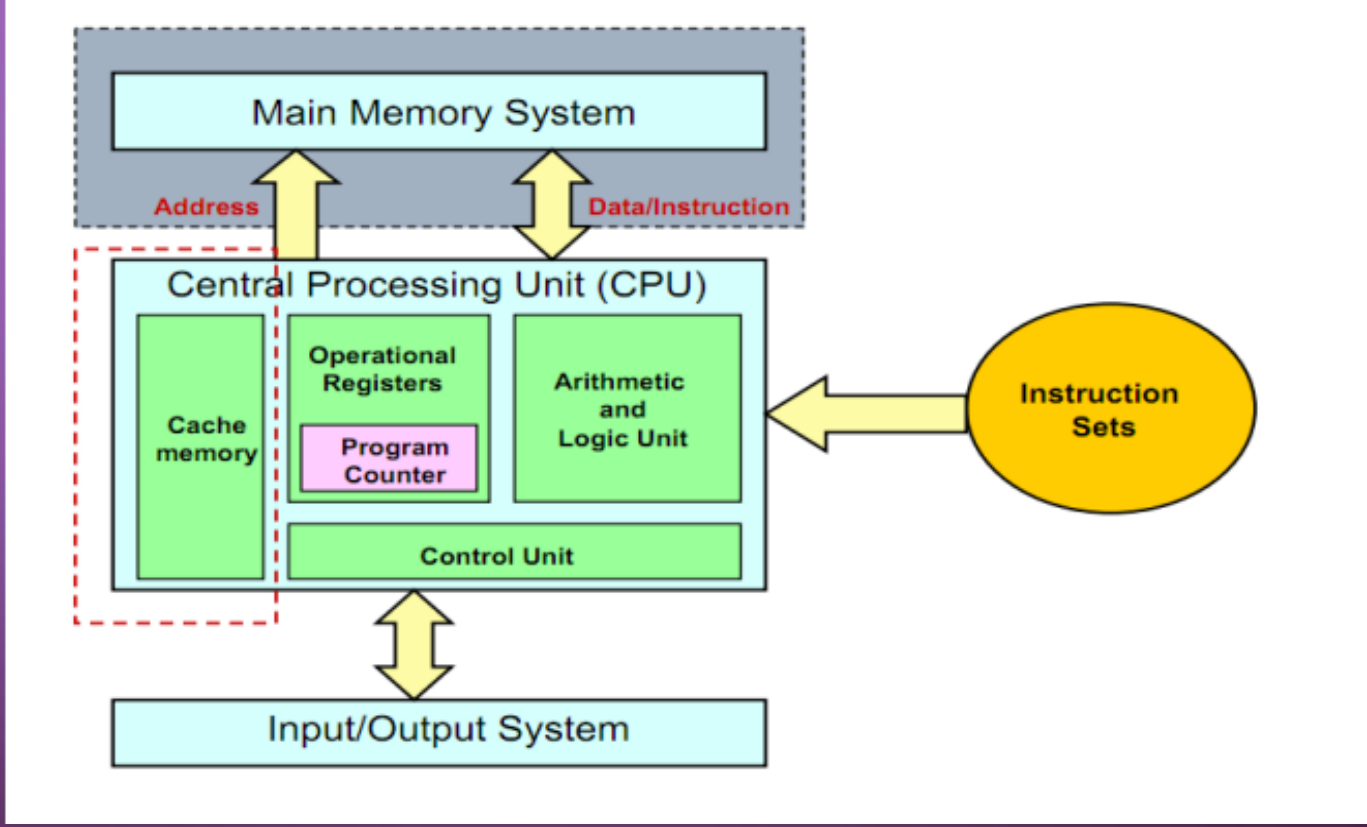
- Random Access {RAM, Cache}
- Direct Access {HDD, Optical Disks}
- Sequential Access {Magnetic Tapes}

TYPES

Computer memory is of three types:

- Primary memory
- Secondary memory
- Cache memory

RELATION


Main Memory System
Address
Data/Instruction
Central Processing Unit (CPU)
Cache memory
Operational Registers
Program Counter
Arithmetic and Logic Unit
Control Unit
Instruction Sets
Input/Output System

PRIMARY MEMORY

- It is also known as the main memory of the computer system.
- It is used to store data and programs or instructions during computer operations.
- Primary memory is of two types:

➢RAM

➢ROM

RAM

Definition:

RAM is a type of volatile memory used in computers to store data and machine code currently in use.

Key Characteristics:

- **Volatile**: Data is lost when power is turned off.
- **Fast**: Provides high-speed read and write access.
- **Temporary**: Used to store data needed for active processes and applications.

Types of RAM:

- **Dynamic RAM (DRAM)**: Requires periodic refreshing to maintain data.
- **Static RAM (SRAM)**: Faster and more expensive, used for cache memory.

Usage:

- Stores operating system, application programs, and active data.
- Enhances system performance by allowing faster data access compared to hard drives or SSDs.

Capacity:

Modern RAM capacities range from 4GB to 64GB or more, depending on system requirements.

ROM

Definition:

ROM is a type of non-volatile memory used to store permanent data and instructions that do not change over time.

Key Characteristics:

- **Non-volatile**: Retains data even when power is turned off.
- **Read-only**: Data is written during manufacturing and cannot be easily modified or erased.

Types of ROM:

- **PROM (Programmable ROM)**: Can be programmed once after manufacturing.
- **EPROM (Erasable PROM)**: Can be erased using UV light and reprogrammed.
- **EEPROM (Electrically Erasable PROM)**: Can be erased and reprogrammed electronically.
- **Flash Memory**: A modern type of EEPROM used in USB drives and SSDs.

Usage:

- Stores firmware, such as BIOS or UEFI.
- Used in embedded systems and devices to hold essential operating instructions.

Advantages:

- Reliable for storing critical system information.
- Resistant to accidental data loss or corruption.

DIFFERENCE BETWEEN RAM AND ROM

RAM	ROM
1. Temporary Storage.	1. Permanent storage.
2. Store data in MBs.	2. Store data in GBs.
3. Volatile.	3. Non-volatile.
4.Used in normal operations.	4. Used for startup process of computer.
5. Writing data is faster.	5. Writing data is slower.

CACHE MEMORY

Definition:
Cache memory is a small, high-speed memory located close to the CPU to store frequently accessed data and instructions, improving processing efficiency.

Key Characteristics:

- **Volatile**: Loses data when power is turned off.
- **Fast**: Faster than RAM and significantly enhances CPU performance.
- **Small Size**: Limited capacity compared to RAM, typically ranging from KB to a few MB.

Levels of Cache:

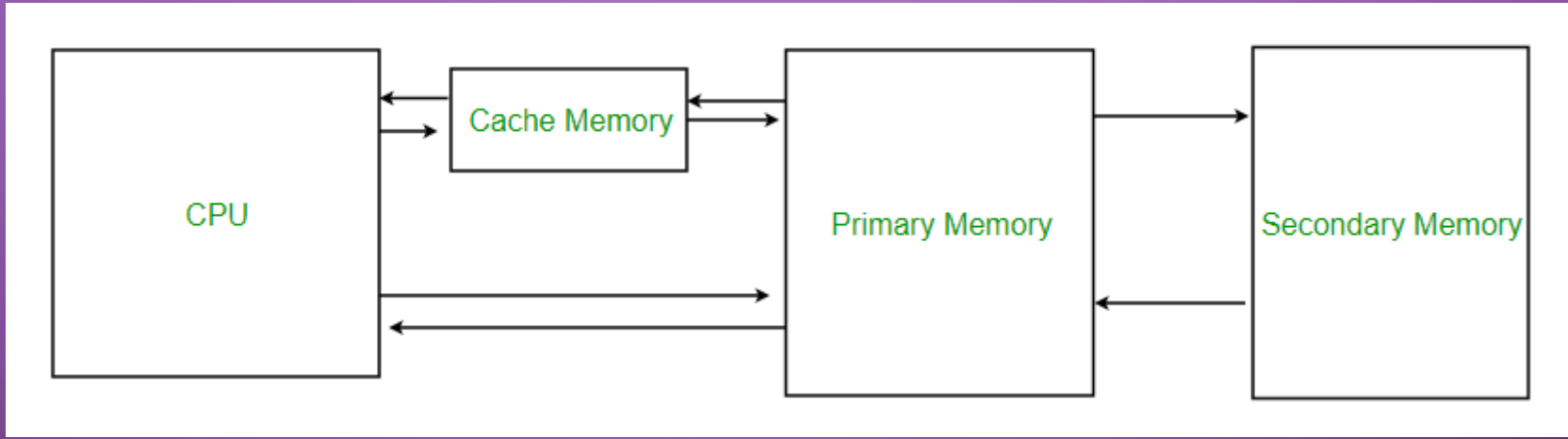
- **L1 (Level 1)**: Smallest and fastest, integrated within the CPU core.
- **L2 (Level 2)**: Larger but slightly slower, located on the CPU or nearby.
- **L3 (Level 3)**: Shared among multiple CPU cores, larger but slower than L1 and L2.

Usage:

- Stores frequently used data and instructions to reduce access time to main memory.
- Helps minimize bottlenecks in CPU processing.

Benefits:

- Accelerates data retrieval and program execution.
- Improves overall system performance.



Cache Memory

CACHE HIT & CACHE MISS

- **Cache Hit:** When the CPU finds the required data in the cache memory, allowing for quick access. On searching in the cache if data is found, a cache hit has occurred.
- **Cache Miss:** When the required data is not found in the cache, forcing the CPU to retrieve it from the slower main memory. On searching in the cache if data is not found, a cache miss has occurred.

EXERCISE

A memory capacity is a way of specifying how many bits can be stored in a particular memory device or complete memory system. The capacity of memory depends on **two** parameters, **the number of words**(m) and **the number of bits per word** (n).

Memory capacity = (number of word) × (number of bits per word)

= m (word) * n (bits)

= m*n bits

EX:- A certain memory chip is specified as 2K × 16

1. How many words can be stored on this chip?
2. What is the words size?
3. How many total bits can this chip store?

Solution:-

1. 2K = 2 × 1024 = 2048 words
2. The word size is 16-bits(2 byte).
3. Capacity = 2048 * 16 = 32,768 =23 KB.

How many 128 * 8 memory chips are required for a memory capacity of 4096*16?

➢Number of chips required = Required RAM size/ Available chip capacity

= (4096 * 16)/(128 * 8) = 64

Self Study

Review all the topics

&

Assignment on

Secondary memory

Week 3

Input Devices

Page
41-62

Input Devices

- In computing, an **input device** is a piece of computer hardware equipment used to provide data and control signals to an information processing system such as a computer or information appliance
- An **input device** is a hardware or peripheral **device** used to send data to a computer
- An **input device allows** users to communicate and feed instructions and data to computers for processing, display, storage and/or transmission.

Following are some of the important input devices which are used in a computer

- Keyboard
- Mouse
- Joy Stick
- Light pen
- Track Ball
- Scanner
- Microphone
- Optical Character Reader(OCR)
- Bar Code Reader
- VRC(voice recognition chip)

Keyboard

- Keyboard is the most common and very popular input device which helps to input data to the computer. The layout of the keyboard is like that of traditional typewriter, although there are some additional keys provided for performing additional functions.
- Keyboards are of two sizes 84 keys or 101/102 keys, but now keyboards with 104 keys or 108 keys are also available for Windows and Internet.
- The traditional QWERTY. First six letters on top row

The keys on the keyboard are as follows –

S. No	Keys & Description
1	**Typing Keys** These keys include the letter keys (A-Z) and digit keys (09) which generally give the same layout as that of typewriters.
2	**Numeric Keypad** It is used to enter the numeric data or cursor movement. Generally, it consists of a set of 17 keys that are laid out in the same configuration used by most adding machines and calculators.
3	**Function Keys** The twelve function keys are present on the keyboard which are arranged in a row at the top of the keyboard. Each function key has a unique meaning and is used for some specific purpose.
4	**Control keys** These keys provide cursor and screen control. It includes four directional arrow keys. Control keys also include Home, End, Insert, Delete, Page Up, Page Down, Control(Ctrl), Alternate(Alt), Escape(Esc).
5	**Special Purpose Keys** Keyboard also contains some special purpose keys such as Enter, Shift, Caps Lock, Num Lock, Space bar, Tab, and Print Screen, control).

Mouse

- Mouse is the most popular pointing device.
- It is a very famous cursor-control device having a small palm size box with a round ball at its base
- which senses the movement of the mouse and sends corresponding signals to the CPU when the mouse buttons are pressed.

- Generally, it has two buttons called the left and the right button and a wheel is present between the buttons.
- A mouse can be used to control the position of the cursor on the screen
- but it cannot be used to enter text into the computer.

Advantages

- Easy to use
- Not very expensive
- Moves the cursor faster than the arrow keys of the keyboard.

Joystick

- Joystick is also a pointing device, which is used to move the cursor position on a monitor screen.
- It is a stick having a spherical ball at its both lower and upper ends.
- The lower spherical ball moves in a socket. The joystick can be moved in all four directions.

- The function of the joystick is similar to that of a mouse.
- It is mainly used in Computer Aided Designing (CAD) and playing computer games.

Light Pen

- Light pen is a pointing device similar to a pen.
- It is used to select a displayed menu item or draw pictures on the monitor screen.
- It consists of a photocell and an optical system placed in a small tube.

- When the tip of a light pen is moved over the monitor screen and the pen button is pressed, its photocell sensing element detects the screen location and sends the corresponding signal to the CPU.

Track Ball

- Track ball is an input device that is mostly used in notebook or laptop computer
- instead of a mouse. This is a ball which is half inserted and by moving fingers on the ball, the pointer can be moved.

- Since the whole device is not moved, a track ball requires less space than a mouse. A track ball comes in various shapes like a ball, a button, or a square.

Scanner

- Scanner is an input device, which works more like a photocopy machine. It is used when some information is available on paper and it is to be transferred to the hard disk of the computer for further manipulation.

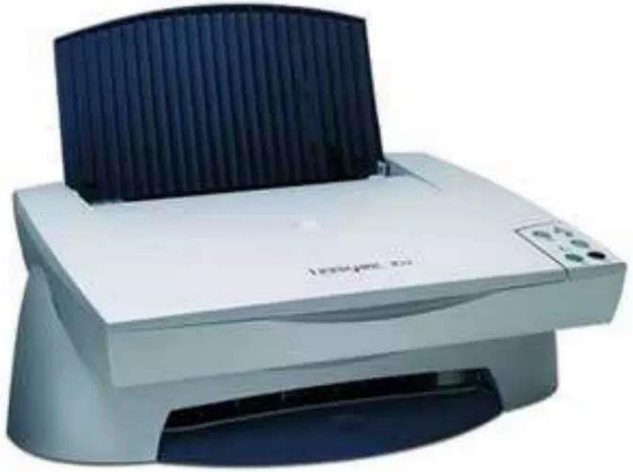
- Scanner captures images from the source which are then converted into a digital form that can be stored on the disk. These images can be edited before they are printed.

Microphone

- Microphone is an input device to input sound that is then stored in a digital form.
- The microphone is used for various applications such as adding sound to a multimedia presentation or for mixing music.
- 

Optical Character Reader (OCR)

- OCR is an input device used to read a printed text.
- OCR scans the text optically, character by character, converts them into a machine readable code, and stores the text on the system memory.



Bar Code Readers

- Bar Code Reader is a device used for reading bar coded data (data in the form of light and dark lines).
- Bar coded data is generally used in labelling goods, numbering the books, etc.
- It may be a handheld scanner or may be embedded in a stationary scanner.
- Bar Code Reader scans a bar code image, converts it into an alphanumeric value, which is then fed to the computer that the bar code reader is connected to.


1 234567 890128

VRC(voice recognition chip)

- Alternatively referred to as **speech recognition**, **voice recognition** is a computer software program or hardware device with the ability to decode the human voice.

- Voice recognition is commonly used to operate a device, perform commands, or write without having to use a keyboard, mouse, or press any buttons.
- Today, this is done on a computer with **automatic speech recognition** (**ASR**) software programs.


Speech Recognition Active
SIEMENS VDO


Speak now
Cancel

SELF STUDY

PRACTICE

WEEK 4

OUTPUT DEVICE

Page
64-80

Output devices: Definition

- An output device is computer hardware that uses received data and commands from a computer in order to perform a task.
- Any peripheral that receives data from a computer, usually for display, projection, or physical reproduction.
- Computer hardware equipment used to communicate the results of data processing carried out by a computer to the outside world.

difference between an input and output device

Input devices	Output device
An input device sends information for processing	output device would reproduce or display the results of the processing.
An **input** device can send data to another device.	An output device can receive data from another device.
It cannot receive data from another device	It cannot send data to another device
Examples : Keyboard,Mouse etc.	Examples:Monitor,Speakers etc

Output devices:Function

They perform the following functions:

- ✓ Receive results from memory.
- ✓ Convert data into human readable form.
- ✓ Display results to the user.

Output devices: Types

Some types of output are

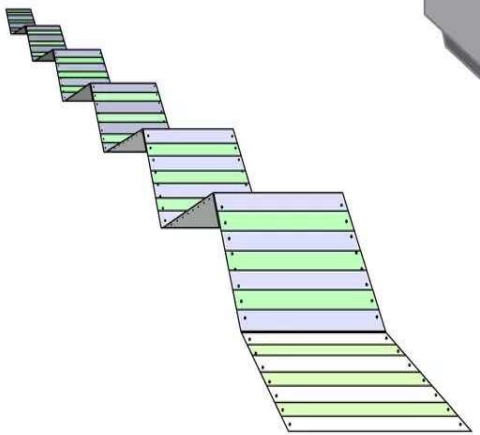
- ✓ Text
- ✓ Graphics
- ✓ Tactile
- ✓ Audio
- ✓ Video

Most output can be divided into two categories:

- ✓ Soft Copy
- ✓ Hard Copy

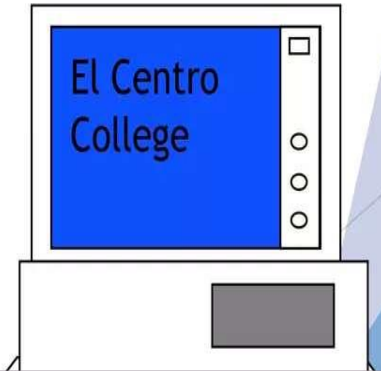
Hard Copy vs. Soft Copy Output

- Hard Copy (Paper Output)



- Soft Copy

  (Monitor Display)



Output devices: Examples

Some output devices are:

- ✓ Speaker
- ✓ Headphones
- ✓ Screen (Monitor)
- ✓ Printer
- ✓ Projector
- ✓ Plotters

Output devices: Printers

- ✓Output devices that produces text and graphics on a physical medium
- ✓Printing mechanism strikes paper, ribbon and character together
- ✓Results in hard copy or printout
- ✓Two orientations: portrait and landscape

Fig: Printers

Output devices: printer (con..)

- ✓A printer is a device that produces output on paper
- ✓Most printers today can produce both text and graphics
- ✓Two types of printer
  - 1) Impact printers
  - 2)Non-impact printers

Output devices: printer (Con..)

1)Impact Printers

- ✓ There is some physical contact with the paper to produce the image i.e.physically striking the paper
- ✓ Types
  - Line printers
  - Dot matrix printers

2)Non-Impact Printers

Types

- Laser Printers
- Ink-jet printer

Output devices: speaker

- ✓ Computer speakers, or multimedia speakers, are speakers external to a computer, that disable the lower fidelity built-in speaker
- ✓ They often have a low-power internal amplifier.
- ✓ Computer speakers range widely in quality and in price.
- ✓ The computer speakers typically packaged with computer systems are small, plastic, and have mediocre sound quality. Some computer speakers have equalization features

Fig:speaker

Output devices: Headphones

- ✓ Headphones are a pair of small loudspeakers, or less commonly a single speaker, with a way of holding them close to a user's ears and a means of connecting them to a signal source such as an audio amplifier, radio or CD player.
- ✓ They are also known as stereo phones, headsets.
- ✓ The in-ear versions are known as earphones or ear buds.
- ✓ In the context of telecommunication, the term headset is used to describe a combination of headphone and microphone used for two-way

Fig: Headphones

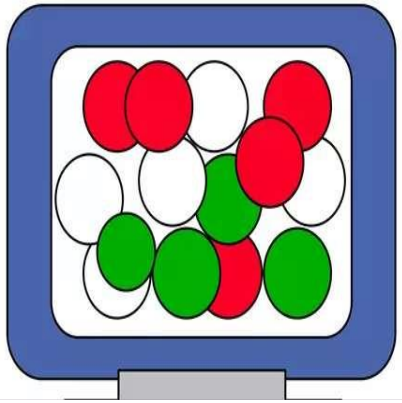
Output devices: Screen(Monitor)

- ✓ A Monitor or Display (sometimes called a visual display unit) is an electronic visual display for computers.
- ✓ The monitor comprises the display device, circuitry, and an enclosure.
- ✓ The display device in modern monitors is typically a thin film transistor liquid crystal display (TFT-LCD) thin panel, while older monitors use a cathode ray tube about as deep as the screen size.

Fig: Monitors

Output devices: Monitor (con..)

- Types
  - CRT
  - LCD
  - LED
- Resolution
  - Pixels
  - SVGA or VGA
  - Monochrome or color



Output devices: Monitor (con..)

- cathode ray tube (CRT)
- liquid crystal display (LCD)

Desktop

Laptop color LCD display

Output devices: projector

- ✓A projector is an output device that can take images generated by a computer or Blu-ray player and reproduce them onto a screen, wall, or other surface.
- ✓ Typically, the surface projected onto is large, flat, and lightly colored.
- ✓ The most common type of projector used today is called a

Fig: projector

Output devices: Plotters

- ✓Used by graphic designers/architects
- ✓Image transferred to paper with ink pens
- ✓Very high resolution
- ✓Excellent for scientific and engineering applications

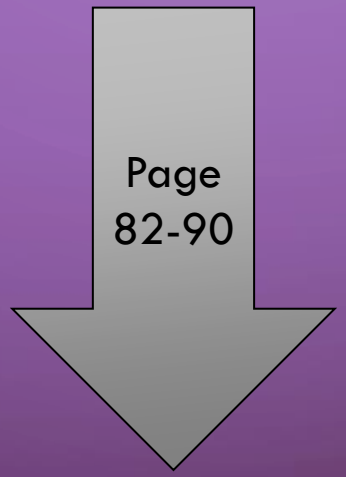
Fig: Plotters

SELF STUDY

PRACTICE

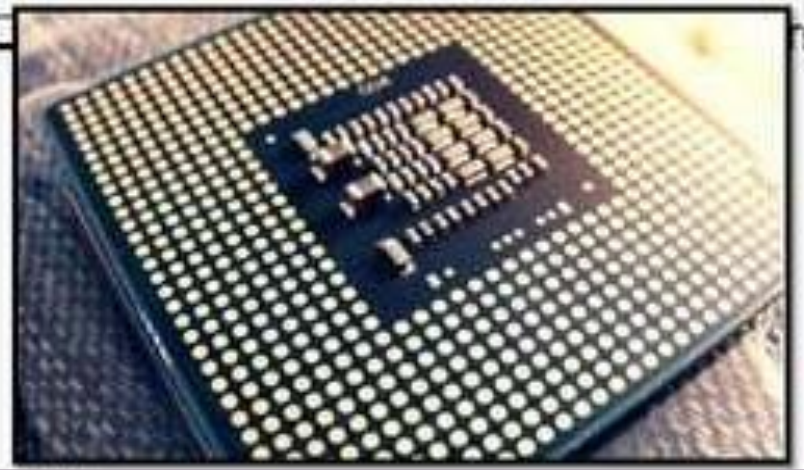
WEEK 5

CENTRAL PROCESSING UNIT (CPU)



INTRODUCTION

- It is a multipurpose, programmable, clock-driven, register based semiconductor device
- CPU interprets instructions to the computer, performs the logical and arithmetic processing operations, and causes the input and output operations
- First CPU was made in the 1940s and was ran with the first computer the EDVAC
- rm



FUNCTION OF CPU

- To carry out processing.
- To perform arithmetic calculation such as addition, subtraction.
- To read instruction & data from memory.
- To communicate with peripherals using system bus.
- To give commands to all parts of the computer system.
- To control the timing of information flow.
- To control the storage of data or instruction.

COMPONENTS OF CPU

1. ALU (Arithmetic Logic Unit)
2. CU (Control Unit)
3. Register Array

ALU (ARITHMETIC LOGIC UNIT)

- ALU performs arithmetic and logic operations such as addition, subtraction, multiplication, division, shifting operations and logic instructions
- ALU includes a group of register-high speed memory locations built directly into the CPU that holds the data currently being processed which is known as Accumulator
- ALU also perform operation like increment, decrement etc.

CU (CONTROL UNIT)

- CU directs the moment of electronic signals between main memory and ALU
- It acts as the **nerve center** of the computer system
- It provides the necessary timing and control signals to all the operations in the computer

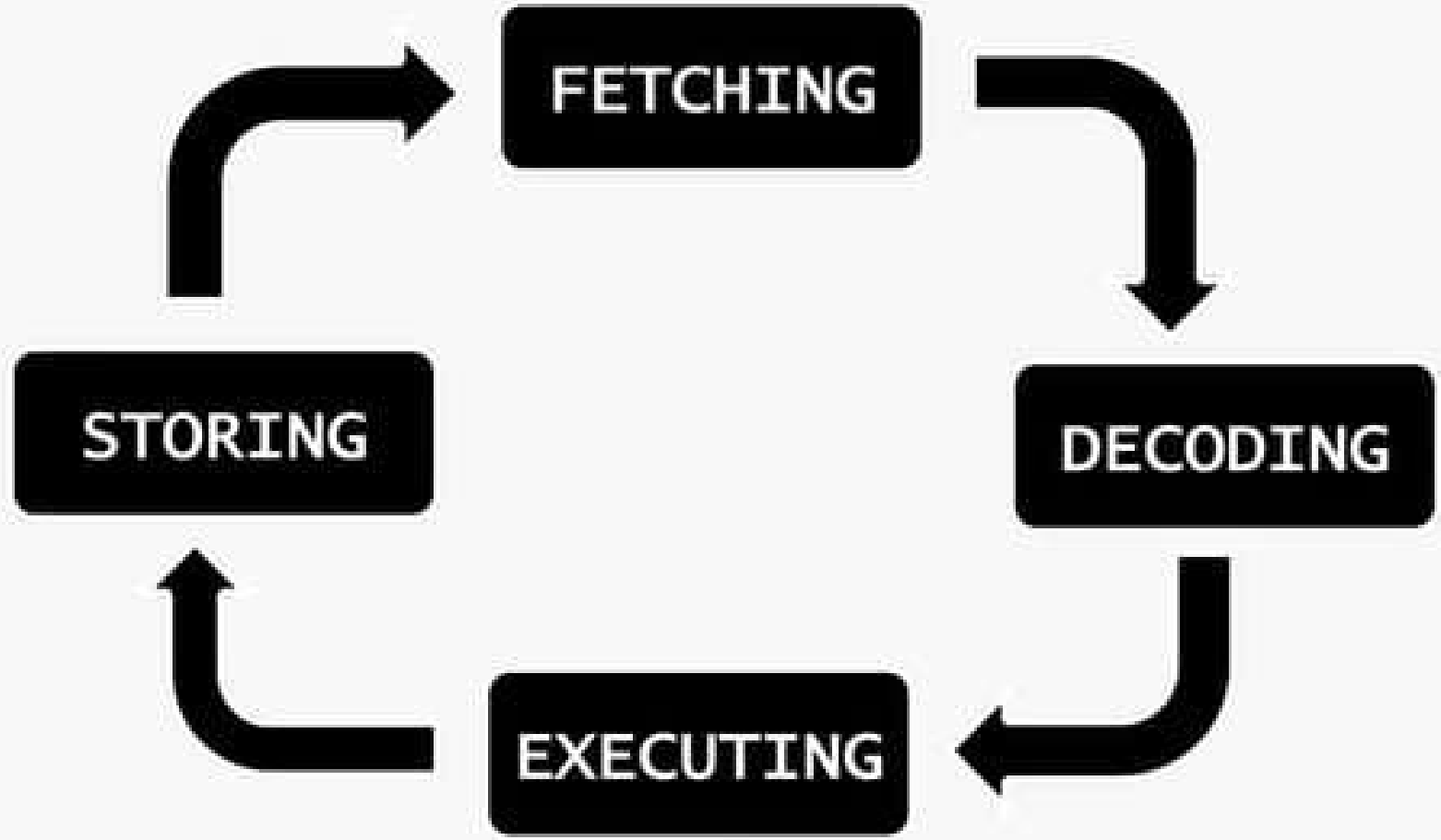
REGISTER ARRAY

- Register is the special purpose temporary storage locations inside the CPU that holds data that is being processed
- It generally occupy the top-most position in the memory hierarchy, providing **high-speed** and **fast access**
- It is normally made of static or dynamic random access memory (RAM) cells
- E.g.
  - Accumulator
  - Address Register
  - Instruction register
  - Sequence register

FACTORS AFFECTING PROCESSING SPEED

- Clock rate of the CPU
- Computer word size
- Bus speed
- Main memory size
- Cache memory size
- Instruction set complexity
- Number of processing units

CPU CYCLE



CONCLUSION

- Thus CPU is the main part (**brain**) of the computer system
- It controls the operation of all other components such as memory, input and output device
- It interprets instructions to the computer, performs the logical and arithmetic operations

SELF STUDY

PRACTICE

WEEK 6 & 7

NUMBER SYSTEM

Page
93-104

What is Number System

- A number system is a system representing numbers. It is also called the system of numeration and it defines a set of values to represent a quantity. These numbers are used as digits and the most common ones are 0 and 1, that are used to represent binary numbers. Digits from 0 to 9 are used to represent other types of number systems.

Types of Number Systems

- There are different types of number systems in which the four main types are:

Binary number system

(Base - 2) like that $(110101)_2$

Octal number system

(Base - 8) like that $(826)_8$

Hexadecimal number system

(Base - 16) like that $(27FBE)_{16}$

Decimal number system

(Base - 10) like that $(102345)_{10}$

Binary Number System

- The binary number system uses only two digits: 0 and 1. The numbers in this system have a base of 2. The binary system is applied internally by almost all latest computers and computer-based devices because of its direct implementation in electronic circuits using logic gates. Every digit is referred to as a bit. binary number, the rightmost digit is called least significant bit (LSB) and leftmost digit is called most significant bit (MSB). The binary number are represent like $(110101)_2$

1	1	0	0	1	1
MSB					LSB

Binary Number System

- Binary number system conversion into decimal And decimal equivalent of this number is sum of product of each digit with its positional value.
- Binary to Decimal conversation

$$
\begin{aligned}
110010_2 &= 1\times2^5 + 1\times2^4 + 0\times2^3 + 0\times2^2 + 1\times2^1 + 0\times2^0 \\
&= 32+16 + 0 + 0 + 2 + 0 \\
&= 50_{10}
\end{aligned}
$$

Decimal to Binary Conversion

- To convert Decimal to binary numbers, the following steps should be followed:-
- 1. Take any decimal number and divide it by "2". After dividing, you will get some results along with the remainder.
- 2. If the decimal number chosen by you is even, then the result will be in a whole number and it will give the remainder 0.
- 3. If the decimal number chosen by you is odd, then the number will not be divided fully and you will get the remainder "1".
- 4. Continue dividing the number till you get the quotient 0
- 5. Now place all the remainders in the series of Least Significant Bit (LSB) at the top and the Most Significant bit (MSB) at the bottom.

Decimal to Binary Conversion Example

- **Let us Convert the Decimal Number 75 into a Binary Number.**

Division of Decimal Number by 2	Quotient	Remainder	Binary
75/2	37	1	(LSB) 1
37/2	18	1	1
18/2	9	0	0
9/2	4	1	1
4/2	2	0	0
2/2	1	0	0
1/2	0	1	(LSB) 1

Octal Number System

- **Octal number system** has eight digits – 0, 1, 2, 3, 4, 5, 6 and 7. Octal number system is also a positional value system with where each digit has its value expressed in powers of 8, For example: 45_8, 53_8, 241_8 are some examples of numbers in the octal number system. as shown here – (Octal to Decimal)

$$326_8 = 3\times8^2 + 2\times8^1 + 6\times8^0$$

$$= 192 + 16 + 6$$

$$= 214_{10}$$

Decimal to Octal Conversion

1. Take the decimal number as dividend.
2. Divide the number by 8 (as 8 is the base of octal so divisor here).
3. Preserve the remainder in an array (and it will be: 0, 1, 2, 3, 4, 5, 6 or 7 because of the divisor 8).
4. Repeat the above two steps until the amount is bigger than zero.
5. Print the mentioned array in the reverse order.

Let us Convert the Decimal Number 210 into a Octal Number. (Therefore, $210_{10} = 322_{16}$)

Division	Remainder (R)
210 / 8 = 26	2
26 / 8 = 3	2
3 / 8 = 0	3

Hexadecimal Number System

- The hexadecimal number system uses sixteen digits/alphabets: 0,1,2,3,4,5,6,7,8,9 and A,B,C,D,E,F with the base number as 16. Here, A-F of the hexadecimal system means the numbers 10-15 of the decimal number system respectively. This system is used in computers to reduce the large-sized strings of the binary system. For example: $7A3_{16}$, $6E_{16}$, $4C2A_{16}$ are some examples of numbers in the hexadecimal number system.

(Hexadecimal to Decimal)

$17FB_{16} = 1\times16^3 + 7\times16^2 + 15\times16^1 + 10\times16^0$

$= 4096 + 1792 + 240 + 10$

$= 6138_{10}$

Decimal to Hexadecimal Conversion

1. Take the decimal number as dividend.
2. Divide the number by 16 (as 16 is the base of octal so divisor here).
3. Preserve the remainder in an array

(and it will be: 0, 1, 2, 3, 4, 5, 6 , 7, 8, 9, A, B, C, D, E, F because of the divisor 16).

1. Repeat the above two steps until the amount is bigger than zero.
2. Print the mentioned array in the reverse order.

Let us Convert the Decimal Number 210 into a Octal Number. (Therefore, $600_{10} = 258_{16}$)

Divide by 16	Quotient	Remainder	Hex Value
600/ 16	37	8	8
37/ 16	2	5	5
2/ 16	0	2	2

Decimal Number System

- Decimal number system is a **base 10** number system having 10 digits from 0 to 9. This means that any numerical quantity can be represented using these 10 digits. Decimal number system is also a **positional value system**. This means that the value of digits will depend on its position. Let us take an example to understand this.

$$1234_{10} = 1\times10^3 + 2\times10^2 + 3\times10^1 + 4\times10^0$$

$$= 1000 + 200 + 30 + 4$$

$$= 1234_{10}$$

SELF STUDY

PRACTICE PROBLEM

WEEK 7 & 8

BOOLEAN ALGEBRA

Page
106-127

Boolean Algebra Summary

- We can interpret high or low voltage as representing true or false.
- A variable whose value can be either 1 or 0 is called a Boolean variable.
- AND, OR, and NOT are the basic Boolean operations.
- We can express Boolean functions with either an expression or a truth table.
- Every Boolean expression can be converted to a circuit.
- Now, we' ll look at how Boolean algebra can help simplify expressions, which in turn will lead to simpler circuits.

Boolean Algebra Summary

- Recall that the two binary values have different names:
  - True/False
  - On/Off
  - Yes/No
  - 1/0
- We use 1 and 0 to denote the two values.
- The three basic logical operations are:
  - AND
  - OR
  - NOT
- AND is denoted by a dot (·).
- OR is denoted by a plus (+).
- NOT is denoted by an overbar ($\overline{\ }$), a single quote mark (') after, or (~) before the variable

Boolean Algebra Summary

- Examples:
  - is read "Y is equal to A AND B."
  - is read "z is equal to x OR y."
  - is read "X is equal to NOT A."

Tabular listing of the values of a function for all possible combinations of values on its arguments
Example: Truth tables for the basic logic operations:

AND		
X	Y	$Z = X \cdot Y$
0	0	0
0	1	0
1	0	0
1	1	1

OR		
X	Y	$Z = X+Y$
0	0	0
0	1	1
1	0	1
1	1	1

NOT	
X	$Z=\overline{X}$
0	1
1	0

Boolean Operator Precedence

- **The order of evaluation is:**
  1. Parentheses
  2. NOT
  3. AND
  4. OR
- **Consequence: Parentheses appear around OR expressions**
- **Example:** F = A(B + C)(C + D)

Boolean Algebra Postulates

- Commutative Law

$$x \cdot y = y \cdot x \qquad x + y = y + x$$

- Identity Element

$$x \cdot 1 = x \qquad x + 0 = x$$
$$x' \cdot 1 = x' \qquad x' + 0 = x'$$

- Complement

$$x \cdot x' = 0 \qquad x + x' = 1$$

Boolean Algebra Theorems

Theorem 1

- $x \cdot x = x$ $\qquad$ $x + x = x$

- Theorem 2
  - $x \cdot 0 = 0$ $\qquad$ $x + 1 = 1$

- Theorem 3: *Involution*
  - $(x')' = x$ $\qquad$ $(\overline{x}) = x$

Boolean Algebra Theorems

- Theorem 4:
  - *Associative:* $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
    $(x + y) + z = x + (y + z)$
  - *Distributive* :
    $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
    $x + (y \cdot z) = (x + y) \cdot (x + z)$

- Theorem 5: *DeMorgan*
  - $(x \cdot y)' = x' + y'$ $\quad (x + y)' = x' \cdot y'$
  - $\overline{x \cdot y} = \overline{x} + \overline{y}$ $\quad \overline{(x + y)} = \overline{x} \cdot \overline{y}$

- Theorem 6: *Absorption*
  - $x \cdot (x + y) = x$ $\quad x + (x \cdot y) = x$

Truth Table to Verify DeMorgan's

$$\overline{X + Y} = \overline{X} \cdot \overline{Y} \qquad \overline{X \cdot Y} = \overline{X} + \overline{Y}$$

X	Y	X·Y	X+Y	$\overline{X}$	$\overline{Y}$	$\overline{X+Y}$	$\overline{X} \cdot \overline{Y}$	$\overline{X \cdot Y}$	$\overline{X}+\overline{Y}$
0	0	0	0	1	1	1	1	1	1
0	1	0	1	1	0	0	0	1	1
1	0	0	1	0	1	0	0	1	1
1	1	1	1	0	0	0	0	0	0

- Generalized DeMorgan's Theorem:

$$\overline{X_1 + X_2 + \ldots + X_n} = \overline{X_1} \cdot \overline{X_2} \cdot \ldots \cdot \overline{X_n}$$

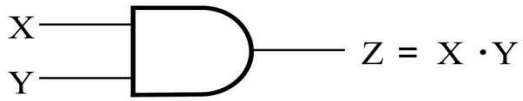
$$\overline{X_1 \cdot X_2 \cdot \ldots \cdot X_n} = \overline{X_1} + \overline{X_2} + \ldots + \overline{X_n}$$

Logic Gates

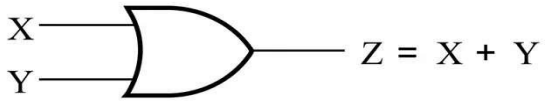
- In the earliest computers, switches were opened and closed by magnetic fields produced by energizing coils in *relays*. The switches in turn opened and closed the current paths.
- Later, *vacuum tubes* that open and close current paths electronically replaced relays.
- Today, *transistors* are used as electronic switches that open and close current paths.

Logic Gate Symbols

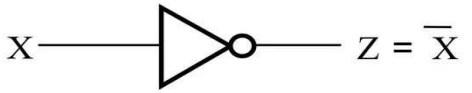
- **Logic gates have special symbols:**



AND gate



OR gate

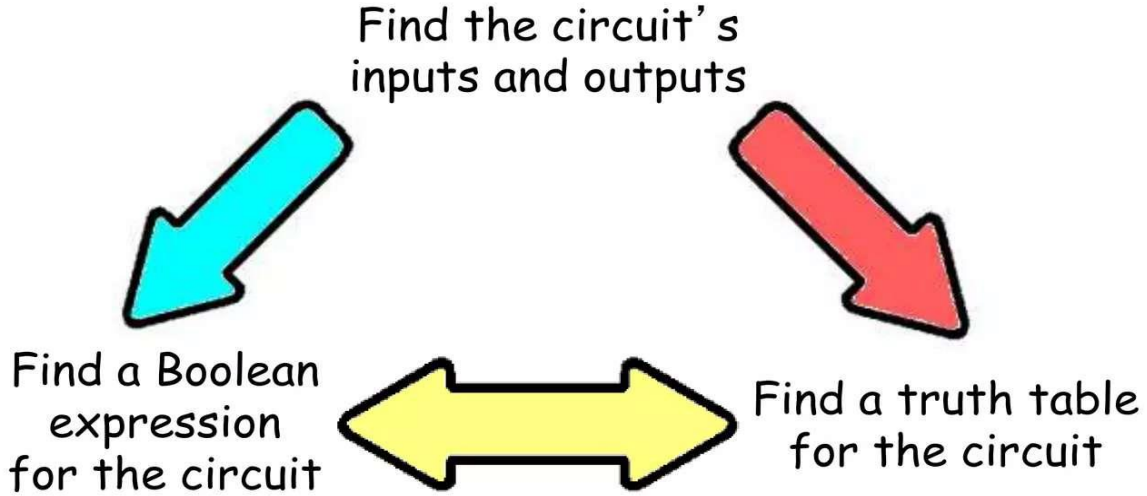


NOT gate or inverter

Boolean Functions

- *A **Boolean function*** is a function whose arguments, as well as the function itself, assume values from a two-element set ({0, 1}).
- ***Example***: $F(x, y) = x'y' + xyz + x'y$

- After finding the circuit inputs and outputs, you can come up with either an expression or a truth table to describe what the circuit does.
- You can easily convert between expressions and truth tables.



Boolean Functions

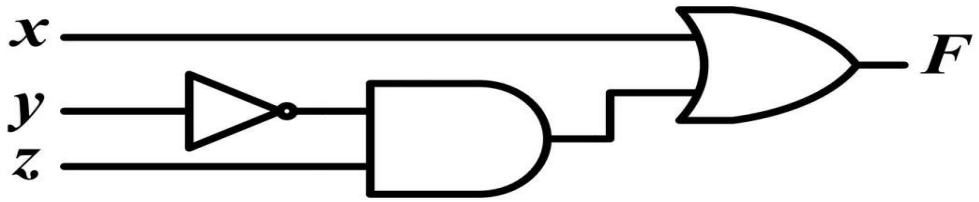
- **Boolean Expression/Function**

  Example: $F(x, y) = x + y' z$

- **Truth Table**

  All possible combinations of input variables

- **Logic Circuit**



x	y	z	F
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

Logic Diagrams and Expressions

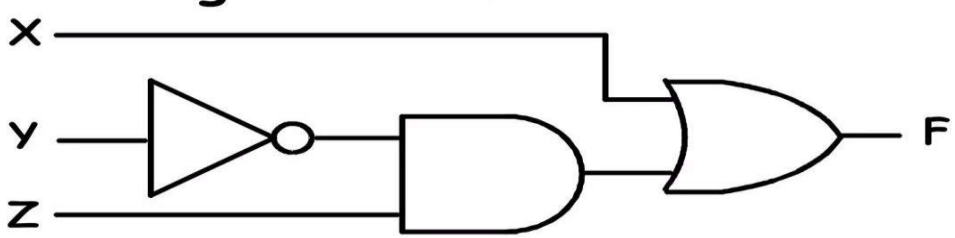
Truth Table

X Y Z	F = X + $\overline{Y}$ XZ
0 0 0	0
0 0 1	1
0 1 0	0
0 1 1	0
1 0 0	1
1 0 1	1
1 1 0	1
1 1 1	1

Logic Equation/Boolean Function

$$F = X + \overline{Y}\,Z$$

Logic Circuit



- Boolean equations, truth tables and logic diagrams describe the same function!
- Truth tables are unique, but expressions and logic diagrams are not. This gives flexibility in implementing functions.

Boolean Functions Exercise

- The truth table for the function:

$$F(X, Y, Z) = XY + \overline{Y}Z \quad \textit{is:}$$

X	Y	Z	XY	$\overline{Y}$	$\overline{Y}Z$	$F = XY + \overline{Y}Z$
0	0	0	0	1	0	0
0	0	1	0	1	1	1
0	1	0	0	0	0	0
0	1	1	0	0	0	0
1	0	0	0	1	0	0
1	0	1	0	1	1	1
1	1	0	1	0	0	1
1	1	1	1	0	0	1

Draw the logic circuit for the boolean function above.

Converting from Truth Table to Boolean Function

- In designing digital circuits, the designer often begins with a truth table describing what the circuit should do.
- The design task is largely to determine what type of circuit will perform the function described in the truth table.
- While some people seem to have a natural ability to look at a truth table and immediately envision the necessary logic gate or relay logic circuitry for the task, there are procedural techniques available for the rest of us.
- Here, Boolean algebra proves its utility in a most dramatic way!

Converting from Truth Table to Boolean Function

- This problem will be solved by showing that any Boolean function can be represented by a Boolean sum of Boolean products of the variables and their complements or the product of sums.

- There are two ways to convert from truth tables to Boolean functions:
  1. Using Sum of Products /Minterms
  2. Using Product of Sums /Maxterms

Converting from Truth Table to Boolean Function

- **Minterm**
  - Product (*AND* function)
  - Contains all variables
  - Evaluates to '1' for a specific combination

Example

$A = 0$
$B = 0$
$C = 0$

$\overline{A} \quad \overline{B} \quad \overline{C}$

$(\overline{0}) \cdot (\overline{0}) \cdot (\overline{0})$

$1 \cdot 1 \cdot 1 = 1$

	A	B	C	Minterm	
0	0	0	0	m_0	$\overline{A}\,\overline{B}\,\overline{C}$
1	0	0	1	m_1	$\overline{A}\,\overline{B}\,C$
2	0	1	0	m_2	$\overline{A}\,B\,\overline{C}$
3	0	1	1	m_3	$\overline{A}\,B\,C$
4	1	0	0	m_4	$A\,\overline{B}\,\overline{C}$
5	1	0	1	m_5	$A\,\overline{B}\,C$
6	1	1	0	m_6	$A\,B\,\overline{C}$
7	1	1	1	m_7	$A\,B\,C$

Converting from Truth Table to Boolean Function

- **Maxterm**
  - Sum (*OR* function)
  - Contains all variables
  - Evaluates to '0' for a specific combination

Example

$A = 1$
$B = 1$
$C = 1$

$$\overline{A} \quad \overline{B} \quad \overline{C}$$
$$(\overline{1}) \cdot (\overline{1}) \cdot (\overline{1})$$
$$0 \cdot 0 \cdot 0 = 0$$

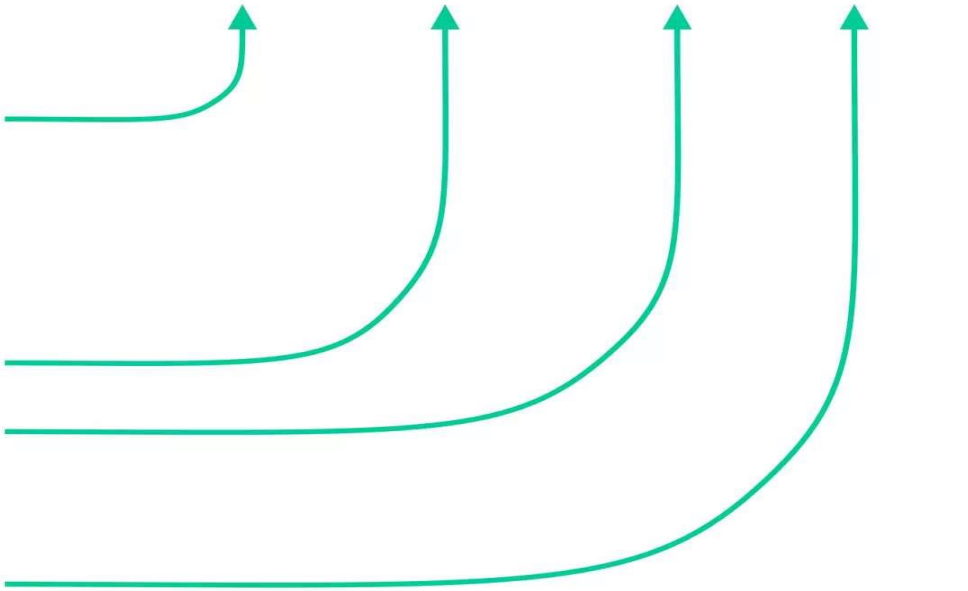
	A	B	C	Maxterm	
0	0	0	0	M_0	$A+B+C$
1	0	0	1	M_1	$A+B+\overline{C}$
2	0	1	0	M_2	$A+\overline{B}+C$
3	0	1	1	M_3	$A+\overline{B}+\overline{C}$
4	1	0	0	M_4	$\overline{A}+B+C$
5	1	0	1	M_5	$\overline{A}+B+\overline{C}$
6	1	1	0	M_6	$\overline{A}+\overline{B}+C$
7	1	1	1	M_7	$\overline{A}+\overline{B}+\overline{C}$

Converting from Truth Table to Boolean Function

- Truth Table *to* Boolean Function

A	B	C	F
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

$$F = \overline{A}\overline{B}C + A\overline{B}\overline{C} + A\overline{B}C + ABC$$



Using Minterms

Converting from Truth Table to Boolean Function

- Truth Table to Boolean Function

$$F = (A + B + C)(A + \overline{B} + C)(A + \overline{B} + \overline{C})(\overline{A} + \overline{B} + C)$$

A	B	C	$\overline{F}$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

Using Maxterms

Converting from Truth Table to Boolean Function

- Sum of *Minterms*

$$F = \overline{A}\overline{B}C + A\overline{B}\overline{C} + A\overline{B}C + ABC$$

$$F = m_1 + m_4 + m_5 + m_7$$

$$F = \sum(1,4,5,7)$$

- *Product of Maxterms*

$$\overline{F} = \overline{A}\overline{B}\overline{C} + \overline{A}B\overline{C} + \overline{A}BC + AB\overline{C}$$

$$\overline{\overline{F}} = \overline{\overline{A}\overline{B}\overline{C} + \overline{A}B\overline{C} + \overline{A}BC + AB\overline{C}}$$

$$F = \overline{\overline{A}\overline{B}\overline{C}} \cdot \overline{\overline{A}B\overline{C}} \cdot \overline{\overline{A}BC} \cdot \overline{AB\overline{C}}$$

$$F = (A + B + C)(A + \overline{B} + C)(A + \overline{B} + \overline{C})(\overline{A} + \overline{B} + C)$$

$$F = M_0 \quad M_2 \quad M_3 \quad M_6$$

$$F = \prod(0,2,3,6)$$

	A	B	C	F	$\overline{F}$
0	0	0	0	0	1
1	0	0	1	1	0
2	0	1	0	0	1
3	0	1	1	0	1
4	1	0	0	1	0
5	1	0	1	1	0
6	1	1	0	0	1
7	1	1	1	1	0

SELF STUDY

PRACTICE PROBLEM

Week 9 & 10

Mid Exam

Overview all the topics before mid exam.

Week 11

Logic Gates

What is a gate?

- The building blocks used to create digital circuits are logic gates
- Combination of transistors that performs binary logic
- There are three elementary logic gates and a range of other simple gates
- Each gate has its own logic symbol which allows complex functions to be represented by a logic diagram
- The function of each gate can be represented by a truth table or using Boolean notation

LOGIC GATES

- Types of gates
  - NOT
  - AND
  - OR
  - NAND
  - NOR
  - EX-OR
  - EX-NOR
  - BUFFER GATE

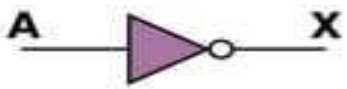
NOT Gate

- A NOT gate accepts one input value and produces one output value
- By definition, if the input value for a NOT gate is 0, the output value is 1, and if the input value is 1, the output is 0
- A NOT gate is sometimes referred to as an *inverter* because it inverts the input value

Boolean Expression

$X = A'$

Logic Diagram Symbol



Truth Table

A	X
0	1
1	0

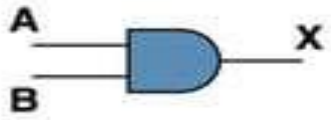
AND Gate

- An AND gate accepts two input signals
- If the two input values for an AND gate are both 1, the output is 1; otherwise, the output is 0

Boolean Expression

$X = A \cdot B$

Logic Diagram Symbol



Truth Table

A	B	X
0	0	0
0	1	0
1	0	0
1	1	1

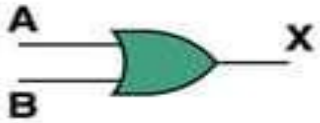
OR Gate

- If the two input values are both 0, the output value is 0; otherwise, the output is 1

Boolean Expression

$$X = A + B$$

Logic Diagram Symbol

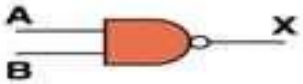


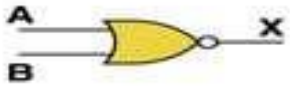
Truth Table

A	B	X
0	0	0
0	1	1
1	0	1
1	1	1

NAND and NOR Gates

- The NAND and NOR gates are essentially the opposite of the AND and OR gates, respectively.
- They are also called universal gates.

Boolean Expression	Logic Diagram Symbol	Truth Table
$X = (A \cdot B)'$		A B X 0 0 1 0 1 1 1 0 1 1 1 0

Boolean Expression	Logic Diagram Symbol	Truth Table
$X = (A + B)'$		A B X 0 0 1 0 1 0 1 0 0 1 1 0

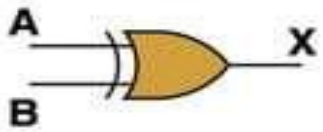
XOR Gate

- XOR, or *exclusive* OR, gate
  - An XOR gate produces 0 if its two inputs are the same, and a 1 otherwise

Boolean Expression

$X = A \oplus B$

Logic Diagram Symbol



Truth Table

A	B	X
0	0	0
0	1	1
1	0	1
1	1	0

XNOR Gate

The exclusive-nor gate or xnor is logically equivalent to an xor gate followed by an inverter

Exclusive-NOR gate

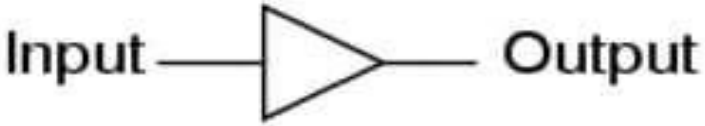
A	B	Output
0	0	1
0	1	0
1	0	0
1	1	1

Equivalent gate circuit

BUFFER GATE

The buffer gates returns the same output as same as that of input

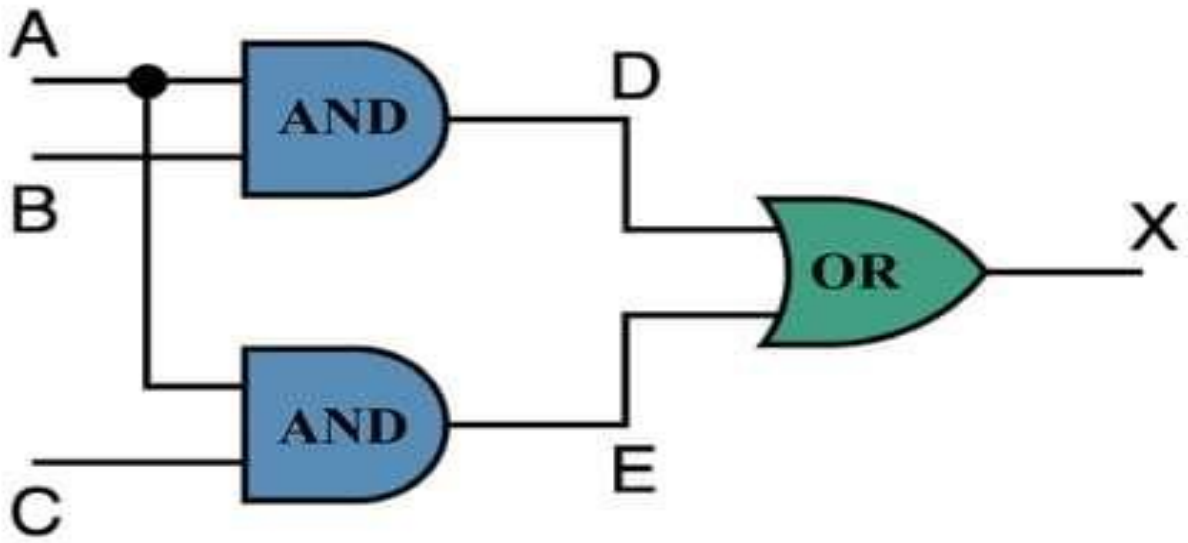
"Buffer" gate



Input	Output
0	0
1	1

Combinational Circuits

- The digital logic circuits whose outputs can be determined using the logic function of current state input are combinational logic circuits



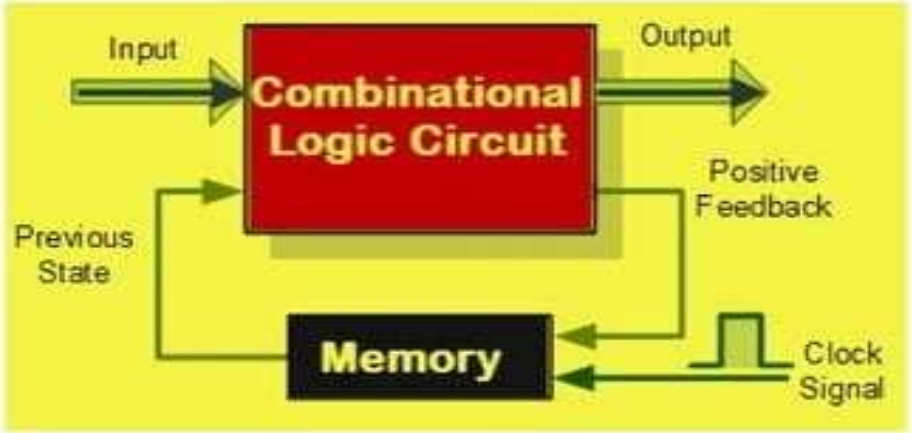
As soon as inputs are changed, the information about the previous inputs is lost, that is, combinational logic circuits have no memory.

Some examples of combinational circuits are-:

- Adder
- Subtractor
- Decoder
- Encoder
- Multiplexer
- Demultiplexer

Sequential Circuits

The digital logic circuits whose outputs can be determined using the logic function of current state inputs and past state inputs and also can store information are called as sequential logic circuits.



It is a combination of memory elements and combinational gates.

Types of sequential circuits

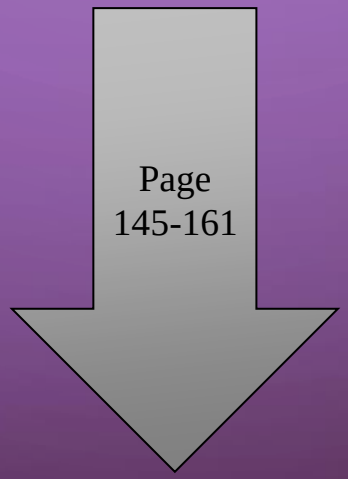
- **Flip flops**
- **Registers**
- **Counters**

SELF STUDY

PRACTICE LECTURE NOTES

WEEK 12

INTRODUCTION TO BASIC NETWORKING CONCEPTS



Networks and Standalone Computers

- Network
  - Group of computers and other devices connected by some type of transmission media
  - Networks enable users to share devices and data, collectively called a network's **resources**
- Standalone computer
  - Uses programs and data only from its local disks and is not connected to a network

Communication before Network

- Method of sharing data by copying it to a disk and carrying the disk from computer to computer

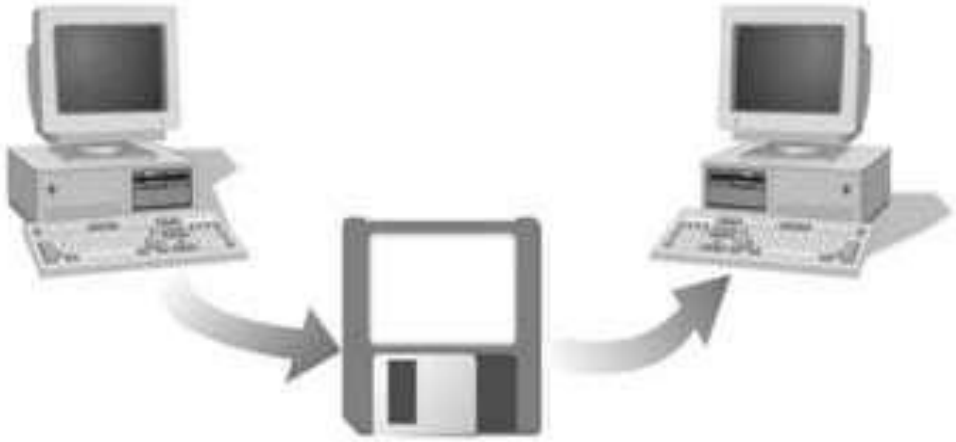


Figure 1-1: Data sharing before the advent of networks

Local and Remote Computers

- Local computer
  - Computer on which user is working
- Remote computer
  - Computer that user controls or works on via network connection

Types of Network

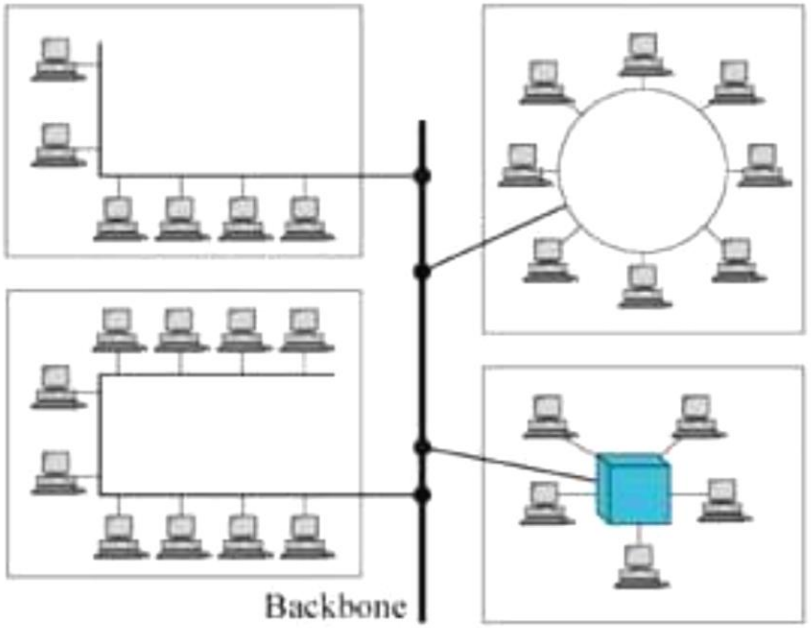
- Local Area Network [LAN]
- Metropolitan Area Network [MAN]
- Wide Area Network [WAN]
- Intranet
- Internet

Local Area Network (LAN)

- Network of computers and other devices confined to relatively small space
- LANs involving many computers are usually server-based
  - On a **server-based network**, special computers (known as **servers**) process data for and facilitate communication between other computers on the network (known as **clients**)

LAN

a. Single-building LAN

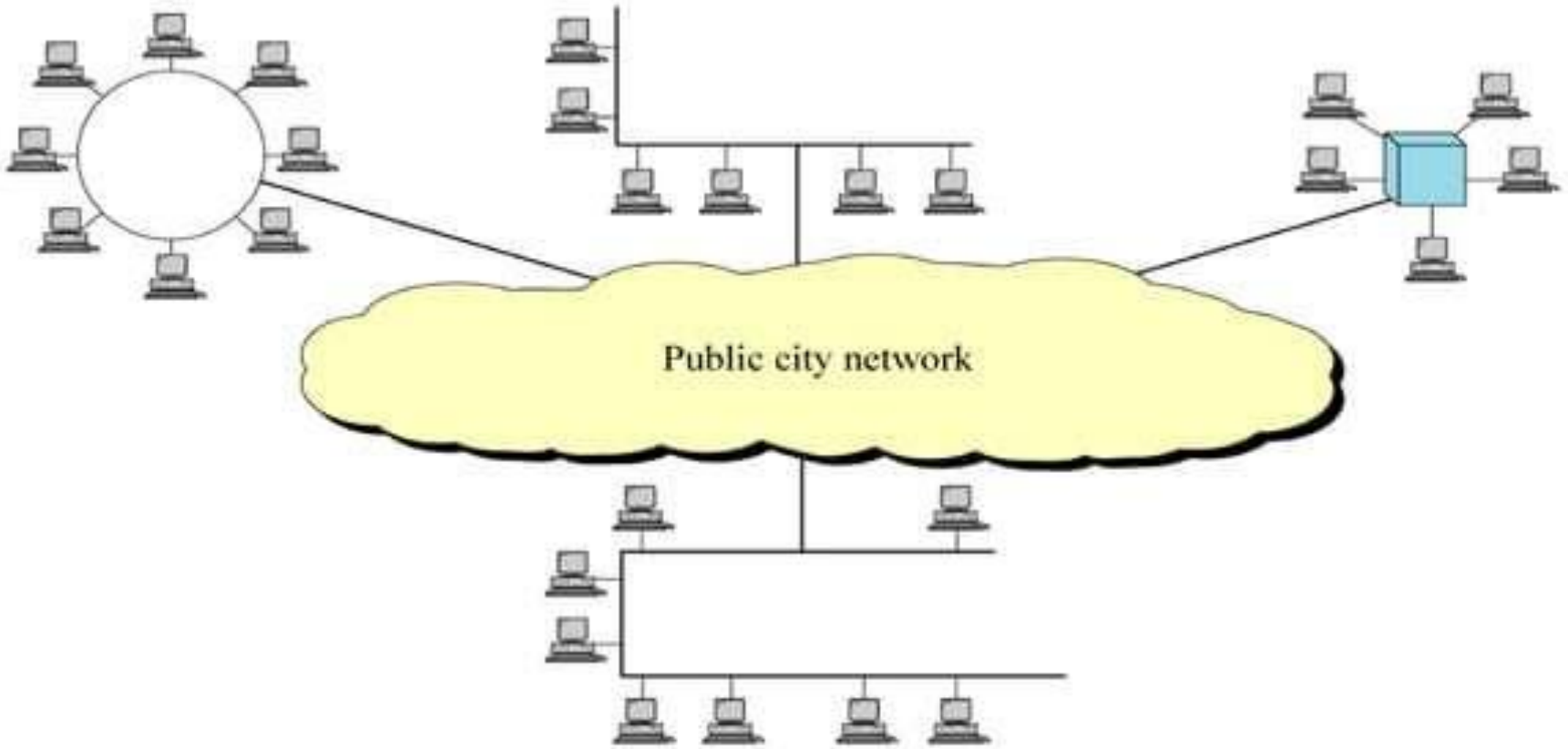


b. Multiple-building LAN

MANs and WANs

- Metropolitan area network (MAN)
  - Network connecting clients and servers in multiple buildings within limited geographic area
- Wide area network (WAN)
  - Network that spans large distance and connects two or more LANs
  - The **Internet** is an example of a very intricate and extensive WAN that spans the globe

MAN



WAN

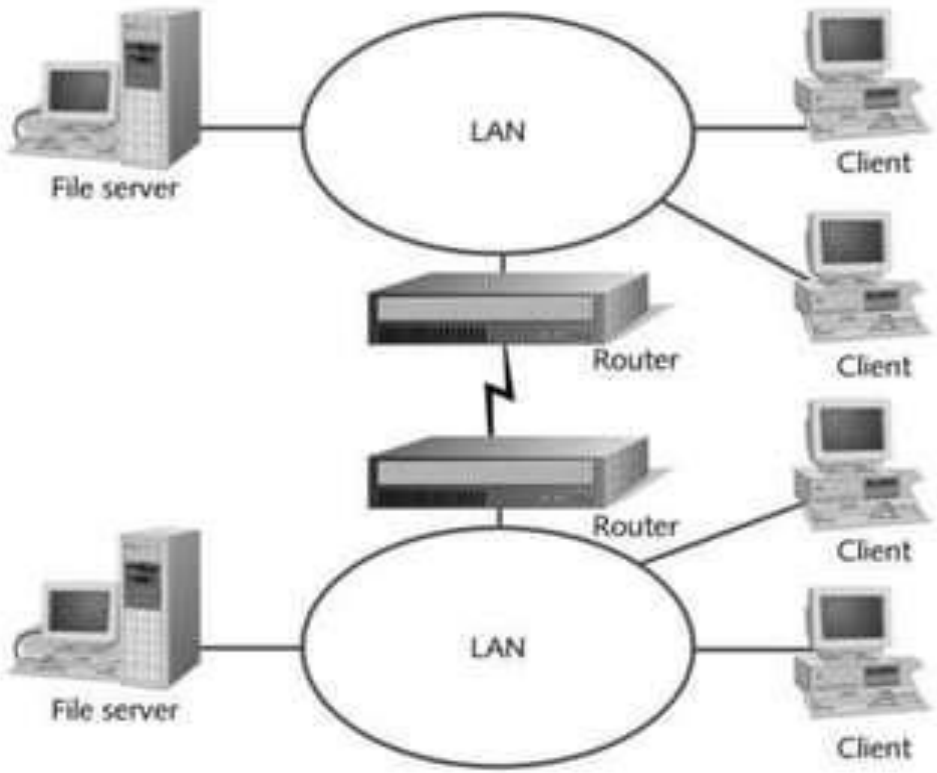


Figure 1-5:
A simple
WAN

11

Types of Network model

- Peer-to-Peer Network
- Client/Server Network

Peer-to-Peer Network

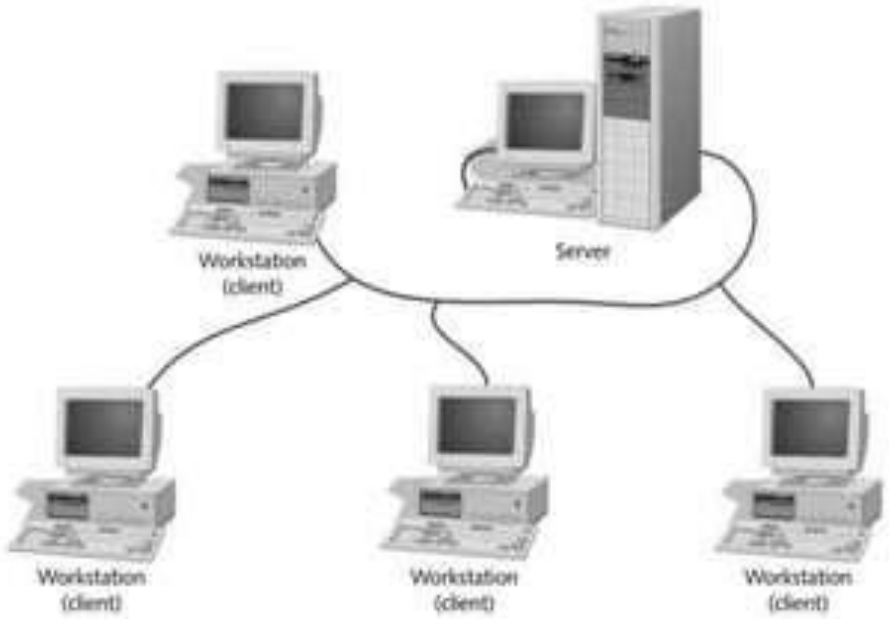
- Computers communicate on single segment of cable and share each other's data and devices
- Simple example of a local area network (LAN)
- Also know as Workgroup Model

Figure 1-2: Simple peer-to-peer network

13

Client/Server Network

Figure 1-3:
LAN with a file
server



14

Intranet

- It is a worldwide system which has the following characteristics:
- Internet is a world-wide / global system of interconnected computer networks.
- Internet uses the standard Internet Protocol (TCP/IP)
- Every computer in internet is identified by a unique IP address.
- IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer's location.
- A special computer DNS (Domain Name Server) is used to give name to the IP Address so that user can locate a computer by a name.
- Internet is accessible to every user all over the world.

Intranet

- Intranet is system in which multiple PCs are connected to each other.
- PCs in intranet are not available to the world outside the intranet.
- Usually each company or organization has their own Intranet network and members/employees of that company can access the computers in their intranet.
- Each computer in Intranet is also identified by an IP Address which is unique among the computers in that Intranet.

Intranet fig.

Similarities in Internet and Intranet

- Intranet uses the internet protocols such as TCP/IP and FTP.
- Intranet sites are accessible via web browser in similar way as websites in internet. But only members of Intranet network can access intranet hosted sites.
- In Intranet, own instant messengers can be used as similar to yahoo messenger/ gtalk over the internet.

Differences in Internet and Intranet

- Internet is general to PCs all over the world whereas Intranet is specific to few PCs.
- Internet has wider access and provides a better access to websites to large population whereas Intranet is restricted.
- Internet is not as safe as Intranet as Intranet can be safely privatized as per the need.

SELF STUDY

PRACTICE LECTURE NOTES

Week - 13

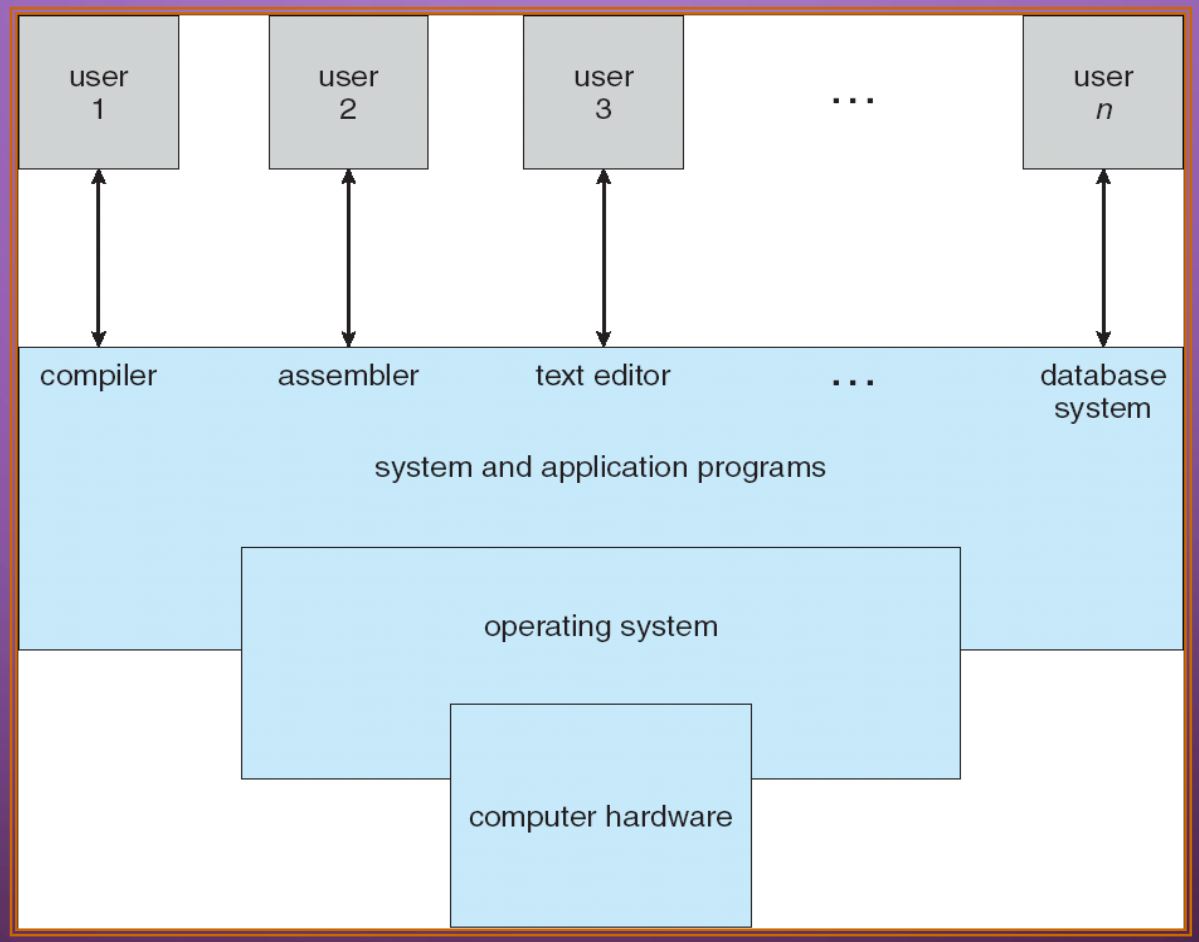
Operating Systems

Page
164-169

WHAT IS AN OPERATING SYSTEM?

- A program that acts as an intermediary between a user of a computer and the computer hardware.
- Operating system goals:
  - Execute user programs and make solving user problems easier.
  - Make the computer system convenient to use.
- Use the computer hardware in an efficient manner.

Four Components of a Computer System



Operating Systems

Windows

Linux

FreeBSD

Mac OS

redhat.

solaris

Sun Cobalt

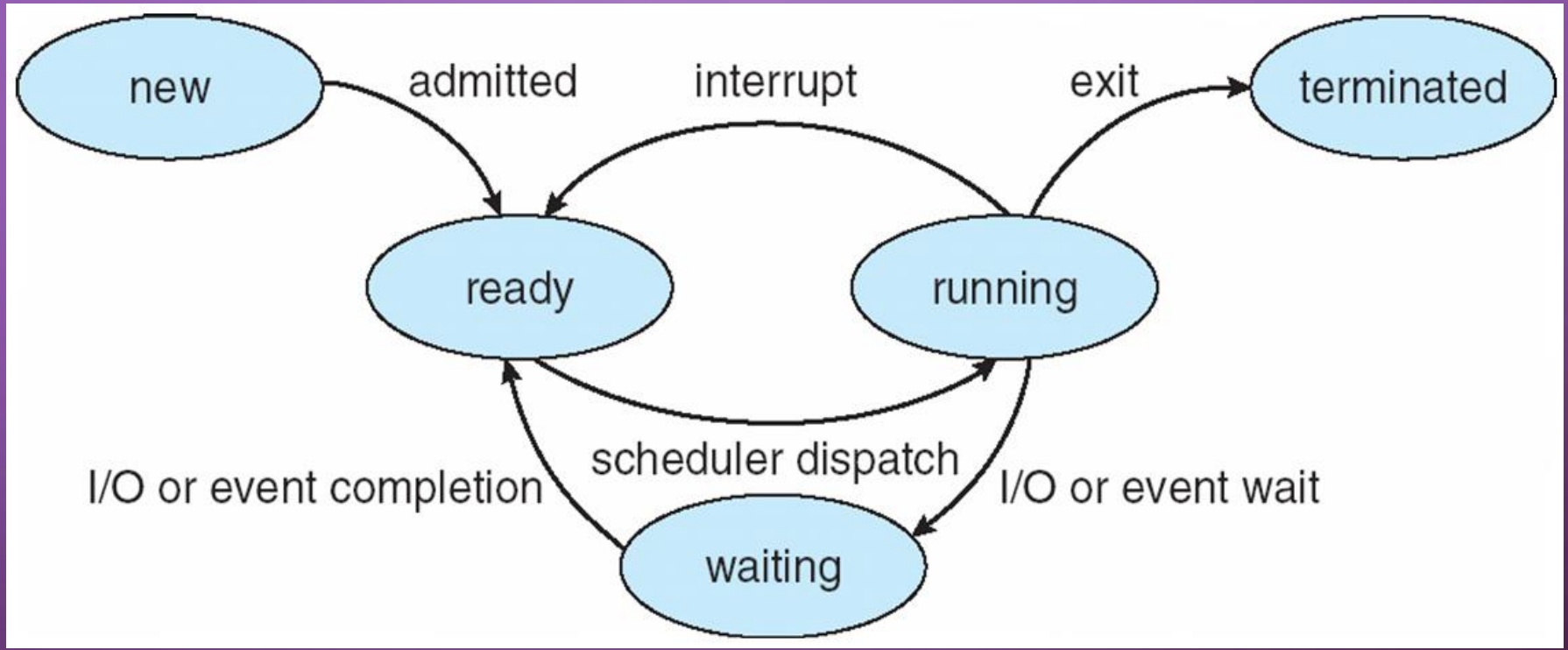
MAIN FUNCTIONS OF AN OS

- Process management
- Memory management
- File management
- Security
- Command interpretation

Process State

- As a process executes, it changes **state**
  - **new:** The process is being created
  - **running:** Instructions are being executed
  - **waiting:** The process is waiting for some event to occur
  - **ready:** The process is waiting to be assigned to a processor
  - **terminated:** The process has finished execution

Diagram of Process State



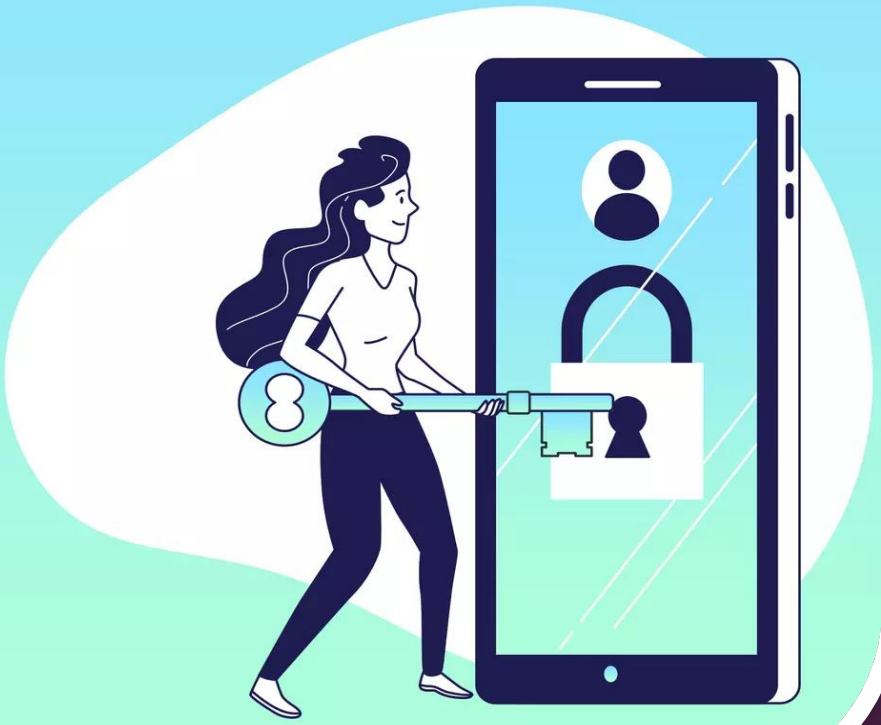
Week - 14

Computer Security

Page
171-181

Introduction to Computer Security

- Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use.
- It is the process of preventing and detecting unauthorized use of your computer system.
- Computer Security mainly focuses on three factors:
  I. Security Attacks
  II. Security Services
  III. Security Mechanisms



Why is Computer Security Important?

- Cyber Crime is on the rise
- Damage is Significant
- Cyber Security builds trust
- Our identities protect our data
- Every organization has vulnerabilities.

QUICK FACTS

- 95% of Computer Security breaches are due to human error.
- There is a hacker attack every 39 seconds
- Share prices fall 7.27% on average after a breach
- Approximately $6 trillion is expected to be spent globally on cybersecurity by 2021
- Unfilled cybersecurity jobs worldwide is already over 4 million

SECURITY MECHANISMS

Security mechanisms are technical tools and techniques that are used to implement security services.

A mechanism might operate by itself, or with others, to provide a particular service.

Security mechanisms deal with prevention, detection, and recovery from a security attack.

SECURITY MECHANISMS

1. CRYPTOGRAPHY

Secret Key Cryptography
Public Key Cryptography
Hash Functions

2. DIGITAL SIGNATURE

Introduction

3. FIREWALL

Functions
Types

4. USER IDENTIFICATION AND AUTHENTICATION

Username and Password
Smart Card
Biometrics

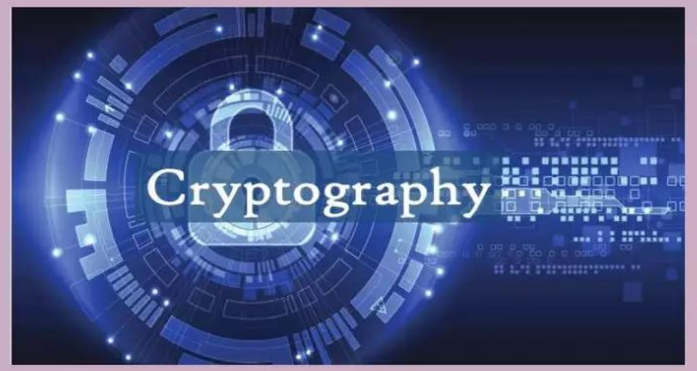
5. INTRUSION DETECTION SYSTEM

Intoduction

6. OTHER MECHANISMS

Virus Protection Software
Data and Information Backups
Secure Socket Layer(SSL)
IP Security Protocol

CRYPTOGRAPHY



- The prefix “crypt” means “hidden” and suffix “graphy” means “writing”. So Cryptography is the science of writing information in “hidden” or “secret” form.
- Cryptography is necessary when communicating data over any network, particularly the Internet.
- It protects the data in transit and also the data stored on the disk.

COMMON TERMS USED IN CRYPTOGRAPHY

Plaintext — Plaintext is ordinary readable text i.e. unencrypted data

Cipher and Code — Cipher is an algorithm for performing encryption or decryption. A cipher converts the original message, called plaintext, into cipher text using a key.

Cipher Text — It is the coded message or the encrypted data.

Encryption — **Encryption** is the process of converting normal message (plaintext) into meaningless message (Cipher text).

Decryption — **Decryption** is the process of converting meaningless message (Cipher text) into its original form (Plaintext).

ALICE

HARRY

BOB

Plain Text → Encryption → Cipher Text → Decryption → Plain Text

Readable format
Non- encrypted data

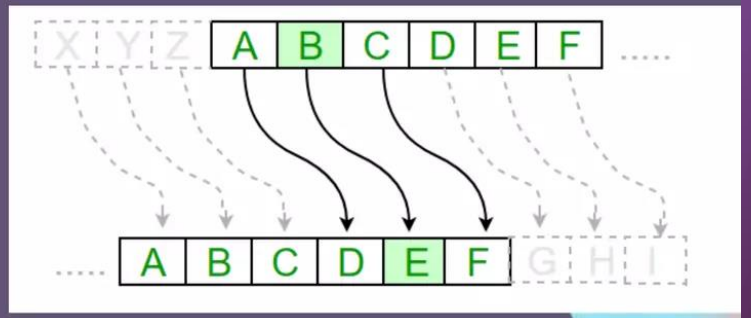
Non- Readable format
Encrypted data

Readable format
Non- encrypted data

CRYPTOGRAPHIC KEY

"Hello" + 🔑 = "KZ0KVey8l1c="

- A cryptographic key is a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa.
- Like a physical key, it locks (encrypts) data so that only someone with the right key can unlock (decrypt) it.
- The size of key is also important. The larger the key, the harder it is to crack a block of encrypted data.
- The three cryptographic schemes are as follows:
  - Secret Key Cryptography (SKC)
  - Public Key Cryptography (PKC)
  - Hash Functions



Attack

Shift by 3

Dwwdfn

STREAM CIPHER AND BLOCK CIPHER

Stream Cipher

- Stream ciphers convert one symbol of plaintext directly into a symbol of cipher text.
- It converts one byte of plain text at a time.
- Uses 8 bits at a time.
- It is easier to reverse the encrypted text to plain text.
- Stream cipher is fast in comparison to block cipher.

Block Cipher

- Block Cipher encrypt a group of plaintext symbols as one block.
- It converts plaintext block wise at a time.
- Uses 64 bits or more at a time.
- It is difficult to reverse the encrypted text to plain text
- Block cipher is slow as compared to stream cipher.

SECURITY AWARENESS

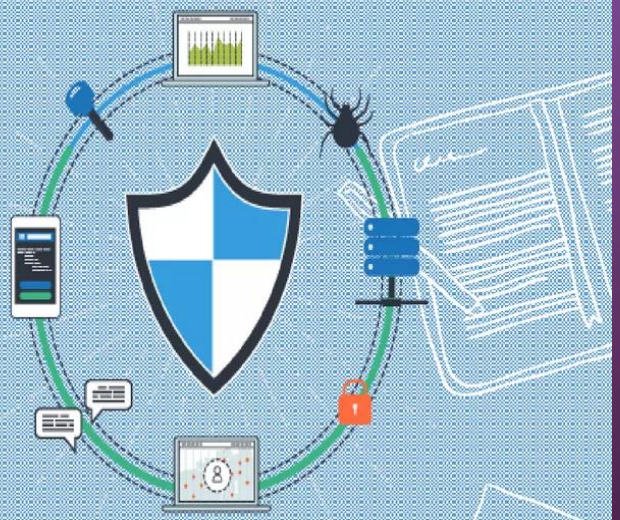
The aim of security awareness is to enhance security of the organization's resources by improving the awareness of the need to secure system resources

Security awareness teaches users to spot phishing, avoid risks online, and use good cyber-hygiene practices at work and at home.

In order to make the users and people in an organization aware of the security practices to be followed, frequent training programs should be conducted in organizations.

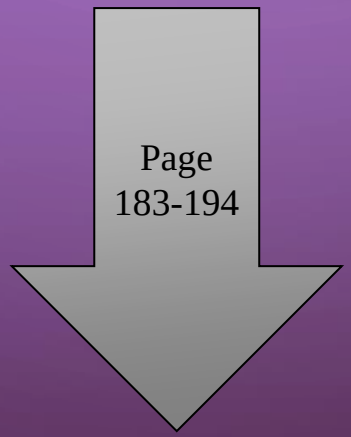
Security Policies

- A security policy is a written document in an organization outlining how to protect the organization from threats, including computer security threats, and how to handle situations when they do occur.
- To be practical and implementable, policies must be defined by standards, guidelines, and procedures.
- The security policy states what is, and what is not allowed. A security policy must be comprehensive, up-to-date, complete, delivered effectively, and available to all staff.
- Generally, security policies are included within a security plan. A security plan details how the rules put forward by the security policy will be implemented
- The security policy also includes physical security of the computers.



Week – 15 & 16

Core Programming Concepts:
Algorithms, Flowcharts, and Pseudocode



ALGORITHM

- A finite set of steps that specify a sequence of operations to be carried out in order to solve a specific problem.
- It consists a set of explicit and clearly defined finite steps to carry out for a given set of initial conditions, produce the corresponding output and terminate after a fixed amount of time.
- Tells the computer to solve the problem in a systematic way to get the desired output.

CHARACTERISTICS OR PROPERTIES OF ALGORITHMS

- **Finiteness**- must terminate in finite number of steps.
- **Simplicity**- Should be simple and easy to read.
- **Absence of Ambiguity**- each step must be clear and unambiguous.
- **Feasibility**- each step must be simple enough that it can be easily translated into the required language.
- **Completeness and correctness**- must be complete and correct.
- **Input**-These are zero or more values which are externally supplied to the algorithm.
- **Output**-At least one value is produced.

STEPS TO WRITE ALGORITHM

- Start the algorithm.
- Take input from user.
- Process the input data.
- Produce one or more results after processing.
- Show the result.
- Exit the algorithm.

EXAMPLE FOR AN ALGORITHM

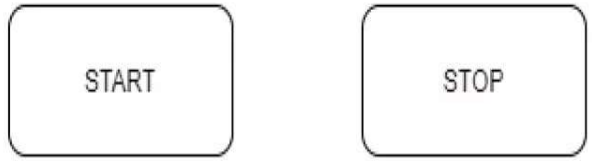
- Add two numbers.
  - Step 1: Start algorithm.
  - Step 2: Enter two numbers a, b.
  - Step 3: Compute c = a + b.
  - Step 4: Print c.
  - Step 5: Exit.

FLOW CHART

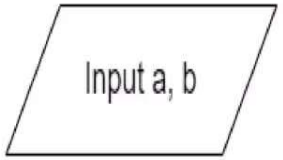
- A pictorial representation of problem and algorithms to its solution that uses the symbols connected by flow lines.
- Called flow chart because it charts the flow of program.
- Used in expressing and understanding algorithms.
- Useful for the programmer and system analyst.

SYMBOLS USED FOR FLOW CHART

- The terminator symbol:
  - represented by rectangle by rounded ends.
  - Indicates the start and stop of the flow chart.

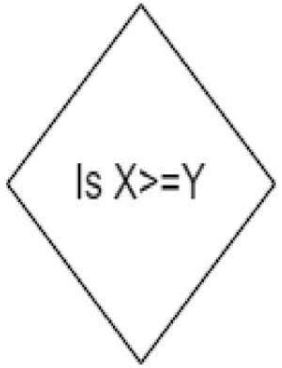


- Input output symbol:
  - Represented by parallelogram.
  - Indicates input output operation.

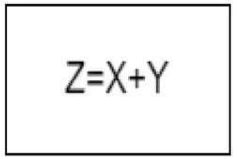


SYMBOLS USED FOR FLOW CHART

- Decision symbol:
  - Represented by diamond.
  - Used to check the conditions whether true or false.
  - Depending upon the condition, the program branches into direction.

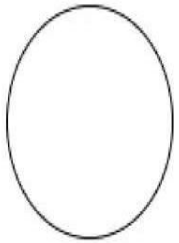


- Process symbol:
  - Represented by rectangle.
  - Indicates any processing, operation, calculation etc.

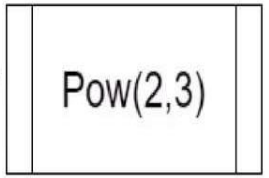


SYMBOLS USED FOR FLOW CHART

- Connector symbol:
  - Represented using a circle.
  - Brings together two branches of a program.
  - Connects various pages of long flow charts.

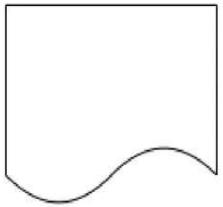


- Predefined Process symbol:
  - Represented using process symbol (rectangle with two lines one on left and one on right side).
  - Indicates a module of a program already defined by another flow chart.



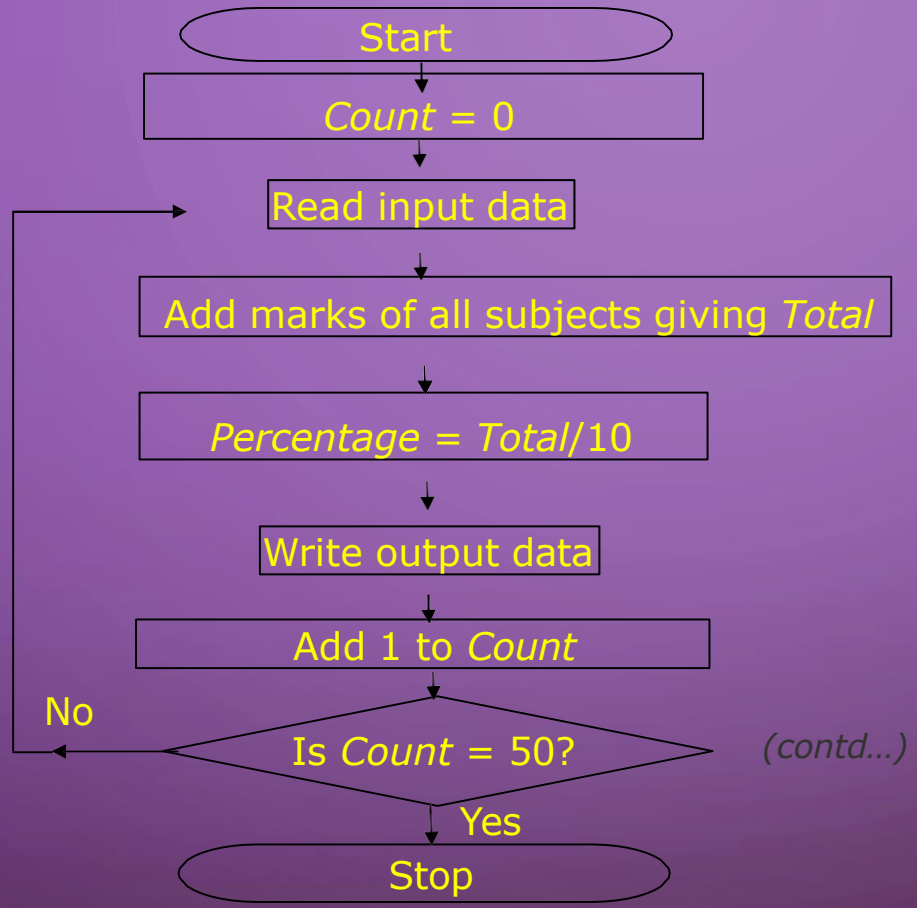
SYMBOLS USED FOR FLOW CHART

- Document symbol:
  - Represented by document symbol.
  - Used to represent any document on paper.



- Data flow symbol:
  - Represented by arrows.
  - Indicates the flow of operation.
  - Also connects other symbols to one another.

SAMPLE FLOWCHART



(contd…)

PSEUDOCODE

- Consists of short, English phrases used to explain specific tasks within a program.
- Is an informal high level description of the operating principle of a program or an algorithm.
- Should not include keywords in any specific computer language.
- Should be written as a list of consecutive phrases.
- allows the designer to focus on the logic of the algorithm without being distracted by details of language syntax.
- describe the entire logic of the algorithm.

EXAMPLE OF PSEUDOCODE

- **Write a pseudocode to find sum and average of given two numbers.**
  - *Begin*
  - *WRITE "Please enter two numbers to add"*
  - *READ num1*
  - *READ num2*
  - *Sum = num1+num2*
  - *Avg = Sum/2*
  - *WRITE Sum, Avg*
  - *End*

WEEK 17

FINAL TOPICS REVIEW AND DISCUSSION: INTEGRATION OF CONCEPTS

FINAL EXAM

THANK YOU