Daffodil International University

Course Title: Computer Fundamentals

Course Code: COF101

Semester Final

Fall 2024

By: Aadil

Table of Contents

Computer Fundamentals

Introduction:

- The word "computer" comes from the Latin word"computare," which means "to calculate"

- According to the Old Oxford English Dictionary, a computer was originally a person who did mathematical calculations.
- Charles Babbage is often credited with inventing the computer in 1882.
- **ENIAC** was the first electronic general-purpose digital computer (1945).
- **The Micral N** was the world's first personal computer (1973).

What is a Computer?

A computer is an electronic machine that follows instructions stored in its memory. It can take in data, process it, and provide output as information. Computers are made up of various parts that work together.

History of Computers and Its Generations

First Generation (1940-1950)

- **Technology:** Vacuum tubes
- **Characteristics:** Large, expensive, and consumed a lot of power. Used **machine language** for programming.
- **Example:** ENIAC

Second Generation (1950-1960)

- **Technology:** Transistors
- **Characteristics:** Smaller, more efficient, and used less power. Used **assembly language** for programming.
- **Example:** IBM 1401

Third Generation (1960-1970)

- **Technology:** Integrated Circuits (IC)
- **Characteristics:** More powerful processing. Introduced high-level programming languages like **FORTRAN** and **COBOL**.
- **Example:** IBM 360

Fourth Generation (1970-1980)

- **Technology:** Microprocessors
- **Characteristics:** Smaller and more efficient. Introduced **Graphical User Interfaces (GUI)**, advanced operating systems, and applications.
- **Example:** Intel 4004, Apple Macintosh

Fifth Generation (1980-Present)

- **Technology:** AI, Quantum, and Nanotechnology
- **Characteristics:** Focused on **Artificial Intelligence (AI)** and **Machine Learning (ML)**. Increased interaction between humans and computers.
- **Example:** Siri, Alexa, ChatGPT

Computer Components

1. **Hardware:** Physical components (e.g., keyboard, mouse, screen).
2. **Software:** Instructions that tell hardware how to function (e.g., applications, programs).

Memory Types

RAM (Random Access Memory)

- **Functions:** Temporary storage for data currently being used or processed.
- **Types:**
    - **SRAM (Static RAM):** Faster but more expensive; doesn't require refreshing.
    - **DRAM (Dynamic RAM):** Slower and cheaper; requires periodic refreshing.

ROM (Read-Only Memory)

- **Functions:** Non-volatile memory used to store firmware (e.g., BIOS).
- **Types:**
    - **Mask ROM:** Pre-programmed data; cannot be changed.
    - **PROM (Programmable ROM):** Can be programmed once by the user.
    - **EPROM:** Can be erased and reprogrammed using UV light.
    - **EEPROM (Electrically Erasable Programmable ROM):** Can be erased and reprogrammed with electrical pulses.

Storage Devices

Hard Disk (HDD)

- **Features:** Non-volatile, stores large amounts of data, slower than RAM.
- **Functionality:** Magnetic storage, used for long-term storage.

Solid State Disk (SSD)

- **Features:** Faster, more reliable than HDDs, no moving parts, uses flash memory.
- **Functionality:** Faster data access, lower power consumption.

Optical Disk (CD/DVD/Blu-ray)

- **Features:** Data is stored using laser technology.
- **Functionality:** Used for data storage, but less commonly used now.

Flash Memory (USB Drives, SD Cards)

- **Features:** Portable, uses flash memory technology.
- **Functionality:** Temporary storage, used in small devices like USB drives and cameras.

Microprocessor

A microprocessor is a small electronic circuit containing the necessary components (arithmetic, logic, control units) to perform the functions of a computer’s central processing unit (CPU).

Functions of a Microprocessor

- Controls all parts of the computer system.
- Transfers data between memory and I/O devices.
- Executes instructions stored in memory.
- Performs arithmetic and logical operations.

Microprocessor Architecture

- **Components:**
  - **CPU (Central Processing Unit)**
  - **Memory modules**
  - **System Bus** (includes data bus, address bus, and control bus)

Types of Microprocessors

1. **CISC (Complex Instruction Set Computer)**
   - Large instruction set, used in personal computers.
2. **RISC (Reduced Instruction Set Computer)**
   - Small instruction set, used in workstations.
3. **EPIC (Explicitly Parallel Instruction Computing)**
   - Allows parallel operations, used in high-end servers.
4. **Multi-Core Processor**
   - Multiple cores for improved parallel processing, used in modern systems.

Microprocessor Architecture

A microprocessor typically includes the following units:

- **Control Unit (CU)**: Manages data flow and operations.
- **Arithmetic Logic Unit (ALU)**: Performs mathematical and logical operations.
- **Registers**: Small storage areas for immediate data processing.
- **Cache Memory**: High-speed memory for storing frequently accessed data.
- **System Bus**: A collection of data paths for communication between CPU, memory, and peripherals.

POSSIBLE QUESTIONS

Write Intel Core i-series vs Intel Pentium Series (Old vs New Architecture Differences).

Ans:

Performance: i-series is faster, more powerful; Pentium is slower.

Cores & Threads: i-series has 2-8+ cores; Pentium has 2 cores.

Clock Speed: i-series has higher clock speeds; Pentium has lower.

Graphics: i-series has better graphics (UHD/Iris Plus); Pentium has basic HD graphics.

Cache: i-series has larger cache (4-16MB); Pentium has smaller cache (1-2MB).

Power Efficiency: i-series is more efficient; Pentium consumes more power.

Tech Support: i-series supports DDR4/DDR5, PCIe 4.0; Pentium supports older tech.

Multitasking: i-series excels in multitasking; Pentium is for basic tasks.

Price: i-series is more expensive; Pentium is cheaper.

Target Audience: i-series for gamers, professionals; Pentium for casual/basic users.

Why RAM and Cache Memory are Responsible for Faster Performance?

Ans:

Both RAM and cache memory are responsible for faster computer performance. **RAM** allows fast access to active data and supports multitasking, while **cache memory** speeds up processing by storing frequently used data close to the CPU. Together, they minimize delays and ensure quicker data retrieval, enhancing overall system efficiency.

Faster Data Access:
Both **RAM** and **cache memory** improve performance by allowing the CPU to quickly access data. **RAM** stores data that is actively being used by the system, enabling the CPU to retrieve it much faster than from storage devices like HDDs or SSDs.

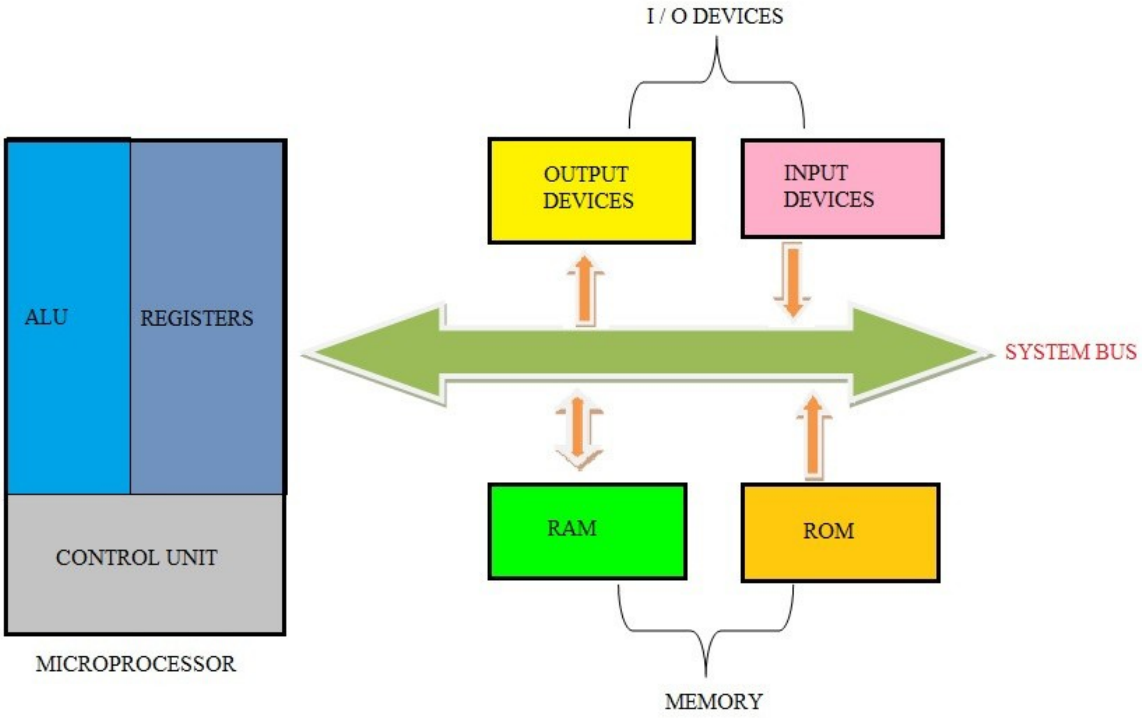
Reduced Latency:
Cache memory plays a crucial role in reducing latency by storing frequently used instructions and data close to the CPU. This proximity allows the CPU to access this data almost instantaneously, minimizing the time spent waiting for data retrieval. As a result, tasks are processed faster, and the overall system runs more smoothly. Without cache, the CPU would need to access data from slower memory (like RAM or disk storage), leading to noticeable delays in performance.

Why is a Microprocessor Called Versatile?

Ans:

- **Multiple Functions:** Can handle a variety of tasks, from basic calculations to complex system control.
- **Programmable**: Can be configured to execute different operations based on software instructions.
- **Adaptable**: Used in a wide range of devices (computers, smartphones, cars, home appliances, etc.).
- **Compact**: Despite being small, integrates multiple functions (arithmetic, logic, control) into one chip, enabling diverse applications.

Draw the block diagram of a microprocessor and explain the function of each component



Explanation of the Diagram:

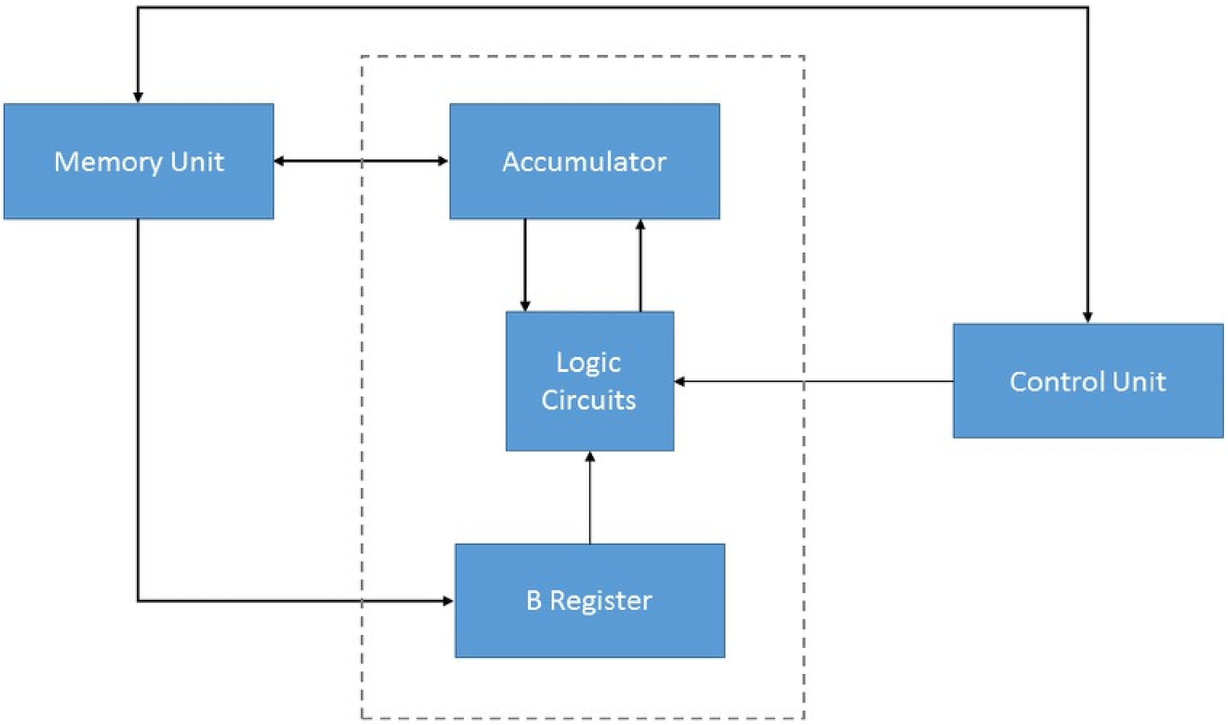
1. **Control Unit (CU)** directs all activities within the microprocessor, instructing other units like the ALU, registers, and BIU.
2. **ALU (Arithmetic Logic Unit)** performs all calculations and logical operations.
3. **Registers** store data temporarily and hold intermediate values for computation.
4. The **Bus Interface Unit (BIU)** manages the communication between the microprocessor and external memory or I/O devices.
5. **Memory Unit** holds the data and instructions required for processing.

6. **Input/output** use for taking instruction and output results.

What is the Arithmetic Logic Unit (ALU)? Draw its block diagram and explain how it works.

Ans:

The Arithmetic Logic Unit (ALU) is a part of the CPU responsible for performing arithmetic (addition, subtraction, etc.) and logical (AND, OR, NOT) operations. It processes data and returns results that are used in executing instructions.



Organization of Arithmetic and Logic Unit

- **Inputs**: Takes two data inputs, usually numbers or data to be processed.
- **Processing**: Executes arithmetic (addition, subtraction, multiplication, division) and logical (AND, OR, NOT, XOR) operations.
- **Control Signals**: The ALU receives control signals from the Control Unit to determine the operation to be performed.
- **Output**: Sends results to an accumulator or memory, depending on the system's architecture.

Write The Common Features of an Operating System (OS).

Ans:

Program Execution: The OS loads and executes programs, managing the CPU's scheduling to ensure smooth operation.

Providing User Interface: The OS provides interfaces (e.g., graphical or command-line) for users to interact with the system and run programs.

Handling Input/Output Operations: The OS manages communication between the hardware (e.g., keyboard, mouse, display) and software applications, ensuring data is received and displayed correctly.

Error Handling: The OS detects and manages errors, alerting users or taking corrective actions to keep the system running.

Memory Management: The OS controls and allocates memory, ensuring programs have the necessary resources and preventing conflicts.

Process Management: The OS manages running programs (processes), schedules their execution, and ensures efficient multitasking without conflicts.

Write The Common Functionality of Operating System.

Ans:

Process Management:

Manages the execution of programs (processes).

Controls starting, stopping, and switching between processes.

Example: Opening, saving, and printing files.

Memory Management:

Manages and allocates memory (RAM) for programs.

Keeps track of memory usage and ensures efficient allocation.

Example: Deciding which program gets how much memory.

Device Management:

Manages input/output devices like printers, keyboards, and USBs.

Allocates devices to processes and tracks their usage.

Example: Deciding which process uses which device.

What is deadlock, how can it be prevented, and what can the operating system do to resolve deadlock?

Ans:

Deadlock is when two or more tasks (processes) are stuck because they are each waiting for the other to release something they need, like memory or a device. Because they keep waiting for each other, none of the tasks can finish. This causes the system to freeze.

Example of Deadlock:

Imagine two tabs in Google Chrome:

Tab 1 is downloading a file and needs the internet connection.

Tab 2 is uploading a file and also needs the internet connection.

Tab 1 is holding the internet connection and waiting for Tab 2 to finish.

Tab 2 is holding part of the internet connection and waiting for Tab 1 to finish.

Now, both tabs are stuck and can't do anything, because they are waiting for the other to finish. This is a deadlock.

To stop deadlock from happening, we need to stop these four conditions from happening:

Mutual Exclusion: Only one process can use a resource at a time. If multiple processes share resources, deadlock chances decrease.

Hold and Wait: This happens when a task holds one resource and waits for another. To prevent this, processes should ask for all the resources they need at once, so they don't hold one and wait for more.

No Preemption: In deadlock, no process can take back a resource from another. The OS can take resources away from a task and give them to another, if needed.

Circular Wait: Deadlock happens when tasks are waiting in a circle. The OS can prevent this by setting a rule where resources must be requested in a certain order, stopping the circle of waiting.

When deadlock happens, the operating system can fix it in two ways:

Ending Processes: The OS can stop one or more processes that are causing the deadlock. It can either stop all processes involved or just one to free up resources.

Taking Resources: The OS can take resources from one process and give them to another process. This breaks the deadlock and allows tasks to continue.

What is Pagging and How it works and What is advantage of pagging?

Ans:

Paging is a method that computers use to manage memory. The computer has RAM (Random Access Memory), which it uses to store data that is being actively used. However, RAM has a limited size, so sometimes the computer cannot fit all the data it needs into RAM at once. To handle this, paging allows the computer to move some data to a larger storage area, like an SSD (Solid State Drive), while keeping the most important data in RAM.

How Paging Works:

The first step in paging is that the computer divides data into small, fixed-size blocks called pages. Each page is a piece of the program or data that the computer is working with. These pages are kept in RAM while they are needed, and when RAM fills up, the computer can move some of the pages to the SSD.

If the computer needs a page that is stored on the SSD, it loads that page back into RAM and makes space for it by moving another page to the SSD. This process ensures that the computer can continue working on tasks, even when there is not enough RAM for everything.

Example:

A program needs 8 GB of memory, but the computer only has 4 GB of RAM available.The computer loads some parts of the program into RAM. When RAM becomes full, some pages are moved to the SSD.

Later, when the program needs data that is stored on the SSD, the computer loads that data back into RAM.

his process happens automatically, so the program can continue running even though not all of its data is stored in RAM.

Advantages :

Since paging divides data into small, fixed-size pieces (pages), the computer doesn’t waste any space. It can always store the pages in the most efficient way.

Paging makes it possible to run more programs than would otherwise be possible. If a program needs more memory than RAM can provide, the computer can move some data to the SSD to make room.

What is Cryptography and How Does It Help?

Ans:

Cryptography is the practice of securing information by converting it into a secure format through encryption. This makes the information unreadable to unauthorized users. Only those with the correct decryption key can access the original data, ensuring confidentiality.

How Cryptography Helps:

Ensures Data Privacy: Encrypts sensitive information to protect it from unauthorized access.

Verifies Identity: Uses authentication methods (like digital signatures) to confirm the identity of users or systems.

Protects Data Integrity: Ensures that data has not been altered during transmission.

Secure Communication: Protects messages, emails, and transactions from eavesdropping or tampering.

Prevents Fraud and Identity Theft: Safeguards personal and financial information, especially in online transactions and banking.

What are Active and Passive Attacks, and How Can They Cause Financial Damage?

Ans:

Active Attack:

An active attack happens when someone tries to change, damage, or steal your data or system. The attacker actively does something to harm the system, often causing financial damage.

Examples:

Denial of Service (DoS): The attacker sends too much traffic to a website, making it crash or stop working.

A business could lose revenue due to the website being down, as customers cannot access products or services.

Phishing: The attacker tricks people into giving away their personal information, like passwords, by pretending to be a trusted source (like a fake email from a bank).

Victims might lose money directly from their bank accounts or credit cards after giving out their login details.

Real-life Example:

WannaCry Ransomware (2017): This attack locked people's files on their computers and demanded money to unlock them.

The ransomware caused billions of dollars in damages, affecting businesses, hospitals, and government organizations, leading to lost productivity, ransom payments, and system repair costs.

Passive Attack:

A passive attack happens when someone watches or listens to your data without changing anything. The attacker is just gathering information quietly, with the potential to cause financial damage later.

Examples:

Man-in-the-Middle (MITM): The attacker secretly listens to or changes the communication between two people without them knowing.

If an attacker intercepts financial data, they could steal sensitive information like bank details, causing financial loss to the victims.

Footprinting: The attacker collects information about a system or network (like IP addresses) without directly interacting with the system.

By gathering information, attackers can later plan targeted attacks, potentially stealing money or causing damage to a company's infrastructure.

Real-life Example:

Wi-Fi Intercepting (2018): In 2018, researchers demonstrated how attackers can use public, unsecured Wi-Fi networks to intercept sensitive data, like login credentials or personal information, from unsuspecting users.

Victims may face financial loss if their credit card details or personal information are stolen and used for fraudulent purchases.

What Are the Three Key Security Objectives in Cybersecurity and Information Protection?

Ans:

In cybersecurity, there are three important goals to protect data and systems. These goals are called the CIA Triad: Confidentiality, Integrity, and Availability. They are the basic rules to keep information safe and secure.

1. Confidentiality

Confidentiality means keeping information private. Only authorized people should be able to see sensitive data. This helps protect personal or business information from being exposed.

Confidentiality helps keep your private information safe, like your passwords, bank details, or personal messages. If someone who is not allowed sees your information, it could cause harm.

When you send a secret email, encryption (changing the message into unreadable code) helps make sure only the person you send it to can read it.

2. Integrity

Integrity means making sure that data stays correct and unchanged. When data is sent or stored, it should not be altered without permission.

If data is changed by someone who shouldn't, it can cause mistakes, confusion, or fraud. Integrity ensures that information is trustworthy.

When you make an online payment, integrity ensures that the amount of money you pay is not changed or tampered with during the process.

3. Availability

Availability means making sure that systems and data are available and working when needed. People should be able to access the information or use services without any problems.

If a website, app, or system is not available, users cannot get the information or services they need. Availability ensures that everything works when it’s needed.

When you visit an online store to buy something, availability makes sure the website is working and you can make a purchase.

What is Ciphertext, and What is the Difference Between Plaintext and Ciphertext?

Ans:

Ciphertext is text that has been changed so it’s not readable. This happens through a process called encryption. Encryption makes the original text look like a mix of random letters and numbers. Only someone with the correct key can turn it back into normal, readable text.

Difference Between Plaintext and Ciphertext

Plaintext is normal text that anyone can read.

Example: "Hello, how are you?"

Ciphertext is text that has been encrypted and looks unreadable.

Example: "Uifsq, jpx bsf zpv?" (This is the encrypted version of "Hello, how are you?")

What is Malware? Explain Different Types of Malware with One-Line Descriptions and Provide a Real-Life Example of One of the Types.

Ans:

Malware is harmful software designed to damage, steal, or gain unauthorized access to data on a computer or network.

Types of Malware:

Virus: A program that attaches itself to a file and spreads when that file is shared.

Worm: Malware that spreads automatically over networks without needing a file to attach to.

Trojan Horse: Malware disguised as a legitimate program that secretly harms your system.

Ransomware: Malware that locks or encrypts your files and demands payment to unlock them.

Spyware: Software that secretly monitors and collects information from your computer.

Real-life Example:

WannaCry was a ransomware attack that affected thousands of computers in 2017. It encrypted files on infected computers and demanded a ransom (payment in Bitcoin) to decrypt them.

The attack spread quickly through a security hole in Windows.It locked important files on businesses, hospitals, and governments worldwide, causing major disruptions.Affected organizations like the National Health Service (NHS) in the UK, forcing them to cancel appointments and surgeries.Billions of dollars in damages.

How to Handle Cyber Threats Before and After They Happen?

Ans:

Cyber threats can be prevented or minimized with proper planning and response. Here's how to handle them before (proactively) and after (reactively) they occur:

Before a Cyber Threat Happens: Proactive Measures

Proactive measures focus on preventing cyberattacks before they happen.

Regular Software Updates: Keep your operating system and applications up-to-date to fix security vulnerabilities.

Strong Passwords & MFA: Use strong, unique passwords and enable Multi-Factor Authentication (MFA) for extra security.

Antivirus & Firewall: Install and regularly update antivirus software and use firewalls to block unauthorized access.

Employee Training: Educate employees about phishing, malware, and safe online practices.

Encryption: Encrypt sensitive data to protect it from unauthorized access.

Backups: Regularly back up important files to secure locations, like the cloud or an external drive.

After a Cyber Threat Happens: Reactive Measures

Reactive measures are taken after an attack occurs to minimize damage and recover quickly.

Incident Response Plan: Follow a predefined plan to detect, contain, and recover from the attack.

Isolate Affected Systems: Disconnect infected systems to stop malware from spreading.

Data Recovery: Restore lost or corrupted data from backups.

Forensic Investigation: Investigate the attack to understand how it happened and prevent future attacks.

Communication: Notify affected parties (employees, customers, etc.) and regulatory authorities if needed.

What is the Impact of Cyber Crime in Real Life?

Ans:

Cybercrime refers to illegal activities that are carried out using computers, the internet, or other digital technologies. It has become a major concern in the digital age, affecting individuals, businesses, governments, and society as a whole.

Real-Life Impacts of Cyber Crime

Financial Losses: Victims of cybercrime can lose significant amounts of money, either through direct theft (e.g., bank account hacking) or fraud (e.g., online scams or credit card fraud).

Identity Theft: Victims face financial losses and damage to their credit score. It can take years to fully recover from the effects of identity theft.

Data Breaches: Data breaches affect the privacy of individuals and can lead to the exposure of sensitive personal information, causing financial loss, reputation damage, and legal consequences.

Reputation Damage: For businesses, cybercrime can lead to a loss of customer trust, decline in sales, and harm to their reputation. For individuals, social media hacking or defamation can cause emotional distress.

Ransomware Attacks: Ransomware can disrupt business operations, healthcare services, and critical infrastructure. Victims may face hefty ransom demands, loss of data, or operational downtime.

Cyberbullying and Harassment: Cyberbullying and online harassment can lead to severe emotional and psychological harm, especially for young people. In extreme cases, it can result in self-harm or suicide.

Disruption of Critical Infrastructure: Cyberattacks on critical infrastructure (e.g., electricity, water supply, transportation) can disrupt entire cities or countries, causing economic damage, public safety risks, and national security threats.

Convert the hexadecimal number 9AD to decimal and binary.

Convert the octal number 765 to decimal and binary.

Note: Maybe I skipped some important things, so further investigate your slides