**1. Define Cyber space. What is Cyber law? Write its advantages and disadvantages of Cyber law.**

## Definition of Cyberspace

Cyberspace refers to the virtual environment of computer networks, the internet, and digital communication systems where users interact, share information, and conduct various online activities. It encompasses websites, social media, online transactions, cloud computing, and all other forms of digital interactions.

## What is Cyber Law?

Cyber law, also known as internet law or IT law, is the legal framework that governs activities conducted online. It includes laws related to cybercrime, data protection, electronic commerce, intellectual property rights, privacy, and digital transactions. Cyber law ensures the security, privacy, and ethical use of technology.

## Advantages of Cyber Law

1. Prevention of Cybercrime – Helps protect individuals and organizations from hacking, identity theft, and fraud.
2. Data Protection – Ensures user data privacy and prevents unauthorized access to sensitive information.
3. Regulation of E-Commerce – Provides legal recognition to online businesses and transactions.
4. Intellectual Property Rights – Protects digital content from unauthorized use and piracy.
5. Improved National Security – Helps in monitoring and preventing cyber threats and terrorism.
6. Legal Framework for Digital Transactions – Supports secure online banking, digital contracts, and electronic signatures.

## Disadvantages of Cyber Law

1. Enforcement Challenges – Difficult to track and prosecute cybercriminals, especially across international borders.
2. Privacy Concerns – Excessive regulations may lead to government surveillance and reduced user privacy.
3. Constantly Changing Technology – Laws may become outdated quickly due to rapid advancements in technology.
4. Costly Compliance – Businesses may face high costs to comply with cybersecurity laws and regulations.
5. Limited Awareness – Many users are unaware of cyber laws, making them vulnerable to cyber threats.
6. Risk of Misuse – Cyber laws may be misused by authorities to suppress free speech and restrict internet freedom.

## Discuss the various Cybercrime related to online banking.

## Cybercrimes Related to Online Banking

Online banking makes money transfers and transactions easy, but it also comes with risks. Cybercriminals use different tricks to steal money and personal information. Here are some common cybercrimes related to online banking:

### 1. Phishing

Phishing is when criminals send fake emails, messages, or links that look real. These messages often ask for banking details like passwords or account numbers. If someone enters their details, hackers steal their money.

### 2. Identity Theft

In this crime, hackers steal a person's personal information, like their name, bank details, or passwords, and use it to make transactions or apply for loans without permission.

### 3. Hacking

Hackers break into bank accounts by guessing weak passwords or using special software. Once they get access, they can transfer money or change account details.

### 4. Card Skimming

Criminals attach a small device to ATMs or payment machines to copy card details when someone swipes their card. They use this stolen information to make fake transactions.

### 5. SIM Swap Fraud

Hackers trick mobile network providers into giving them a duplicate SIM card of a victim's number. Since many banks send OTPs (one-time passwords) to phones, hackers can receive them and access the victim's bank account.

### 6. Malware Attacks

Malware is harmful software that hackers install on devices. If someone downloads an infected app or file, hackers can steal banking information when they log in.

### 7. Fake Banking Apps

Cybercriminals create apps that look like real banking apps. If someone enters their details in these fake apps, hackers can steal their information and money.

### 8. Online Banking Fraud Calls

Criminals call people pretending to be bank employees. They ask for PINs, passwords, or OTPs and use that information to steal money.

**What is identity theft? Explain with example.**

## What is Identity Theft?

Identity theft is when a criminal steals someone's personal information, like their name, bank details, or passwords, and uses it without permission. They can use this stolen information to take money, apply for loans, or even commit crimes in the victim's name.

## Example of Identity Theft

Imagine that John gets an email that looks like it's from his bank. The email asks him to enter his bank username and password to "verify" his account. John believes the email is real and enters his details.

A hacker, who actually sent the fake email, now has John's banking information. The hacker logs into John's account, transfers money, and even applies for a loan in John's name. John only realizes what happened when he sees missing money from his account.

**Discuss various International conventions and Treaties on Cybercrime.**

## International Conventions and Treaties on Cybercrime

Cybercrime is a global problem, so different countries have come together to create rules and agreements to fight it. These international treaties help countries work together to catch cybercriminals and make the internet safer. Below are some important international conventions on cybercrime:

## 1. Budapest Convention on Cybercrime (2001)

- It is the first international treaty to fight cybercrime.
- Created by the Council of Europe with help from other countries.
- Helps countries work together to catch hackers, fraudsters, and cybercriminals.
- Covers crimes like hacking, identity theft, and spreading computer viruses.

**Example:** If a hacker from one country attacks a bank in another country, both countries can work together under this treaty to arrest and punish the hacker.

## 2. The African Union Convention on Cyber Security and Personal Data Protection (2014)

- Also known as the Malabo Convention.
- Focuses on protecting personal data and fighting cybercrime in African countries.
- Encourages African countries to create strong laws against cybercrime.

**Example:** If a company in Africa misuses customer data, this treaty helps governments take legal action.

**Explain the power of Cyber Appellate Tribunal of Cyber.**

## Power of Cyber Appellate Tribunal

The Cyber Appellate Tribunal is a special court that handles cases related to cybercrime and online disputes. It listens to appeals when people or businesses are unhappy with decisions made by lower cyber courts.

## Main Powers of Cyber Appellate Tribunal

1. **Hear Appeals** – If someone is not satisfied with the decision of a lower cyber court, they can appeal to the tribunal. The tribunal will review the case and give a fair judgment.
2. **Punish Cybercriminals** – The tribunal can give punishments to hackers, fraudsters, and other cybercriminals based on the law.
3. **Give Compensation** – If someone loses money or faces harm due to cybercrime, the tribunal can order the criminal to pay compensation.
4. **Enforce Cyber Laws** – It ensures that all online activities follow cyber laws and regulations.
5. **Oversee Digital Transactions** – The tribunal can handle cases related to online banking fraud, digital contracts, and electronic payments.
6. **Protect Personal Data** – If a company or person misuses someone's private data, the tribunal can take legal action against them.
7. **Issue Orders to Government & Police** – The tribunal can direct authorities to investigate cybercrimes, arrest criminals, and take necessary legal actions.

**Is there any protection for digital signature in Bangladesh? What method has the Act adopted? Explain.**

## Protection for Digital Signature in Bangladesh

Yes, Bangladesh has legal protection for digital signatures under the Information and Communication Technology (ICT) Act, 2006. This law recognizes digital signatures as legally valid and secure for online transactions, electronic documents, and official communications.

## Method Adopted by the ICT Act for Digital Signature Protection

The ICT Act, 2006 of Bangladesh follows the Public Key Infrastructure (PKI) method for digital signature protection. PKI is a secure system that uses encryption to protect digital signatures. The main features of this system are:

1. **Use of Cryptography –** Digital signatures use encryption and decryption to ensure security.
2. **Public and Private Keys –** A private key is used to sign a document, and a public key is used to verify its authenticity.

3. **Legal Validity –** Digital signatures are legally accepted in online contracts, financial transactions, and e-governance.
4. **Certifying Authority (CA) –** The government approves certain organizations as "Certifying Authorities" to issue and verify digital signatures.
5. **Protection Against Fraud –** Digital signatures ensure that a document is not changed, forged, or misused after signing.

## Example of Digital Signature Use in Bangladesh

If a business in Bangladesh signs an online contract using a digital signature, it is legally valid. If someone tries to tamper with the signed document, the digital signature will become invalid, proving the fraud.

**Classify Cybercrime with example and categorize Cyber criminals.**

## Classification of Cybercrime with Examples

Cybercrime is any illegal activity that happens online using computers, the internet, or digital devices. Cybercrimes can be classified into different types based on their nature.

1. Cybercrimes Against Individuals
2. Cybercrimes Against Organizations
3. Cybercrimes Against Government and National Security
4. Financial Cybercrimes

## Categories of Cybercriminals

A **cybercriminal** is a person or group who uses computers, the internet, or digital technology to commit illegal activities. Their goal is often to steal data, cause harm, or make money through fraud, hacking, or other online crimes.

1. Hackers

2. Crackers

3. Cyber Terrorists

4. Cyber Stalkers

5. Fraudsters

6. Script Kiddies

7. Insider Threats

Write the strategies can be used to prevent Cybercrime.

Strategies to Prevent Cybercrime:

## 1. Use Strong Passwords

- Create long, complex passwords using a mix of letters, numbers, and symbols.
- **Example:** Instead of using “password123,” use something like “T!m3$trong$987!”
- Avoid using the same password for multiple accounts.

## 2. Keep Software Updated

- Always update your computer, phone, and app software to the latest version.
- Updates often fix security problems and make your devices safer.

## 3. Install Antivirus Software

- Install and regularly update antivirus software to protect your devices from malware, viruses, and hackers.

## 4. Be Careful with Emails and Links

- Be careful of **phishing emails** (fake emails that try to trick you).
- Don’t click on links or open attachments from unknown senders.
- Check if the email address is real and if the link looks safe.

## 5. Enable Two-Factor Authentication (2FA)

- Use **2FA** when available. This means you’ll need to verify your identity with a second method, like a text message or an app, when logging into your account.
- This extra step makes it harder for hackers to access your accounts.

## 6. Avoid Public Wi-Fi for Sensitive Transactions

- Do not log into your bank account or make online payments while using **public Wi-Fi** (like in coffee shops or airports).
- Use a **VPN (Virtual Private Network)** to secure your internet connection if you need to use public Wi-Fi.

## 7. Protect Personal Information

- Be cautious about sharing personal details online (like your address, phone number, or credit card number).
- Check privacy settings on social media to control who can see your information.

## 8. Backup Your Data

- Regularly back up your important data (photos, documents, etc.) to an external hard drive or cloud storage.
- This way, if you lose data due to a cyberattack, you can restore it.

## 9. Educate Yourself and Others

- Learn about common online threats like phishing, ransomware, and identity theft.
- Share this knowledge with friends and family so they can stay safe too.

## 10. Report Suspicious Activity

- If you notice anything suspicious online (like strange emails or unauthorized transactions), report it to your bank, the website, or law enforcement.

**What is phishing? Explain with example.**

## What is Phishing?

Phishing is a type of online scam where criminals **pretend to be a trusted company** to trick people into sharing their **personal information, passwords, or bank details**. They usually do this through **fake emails, messages, or websites**.

## How Does Phishing Work?

1. A scammer sends a **fake email or message** that looks real (from a bank, social media, or government office).
2. The message asks you to **click a link** and enter your **password, credit card details, or personal information**.
3. If you enter your details, the scammer **steals your information** and may use it to hack your account or steal money.

## Example of Phishing

📧 **Fake Bank Email**
You get an email that looks like it's from your bank:

*"Your account has been locked due to security issues. Click the link below to verify your account."*

- The **link is fake** and leads to a **fraud website** that looks like your bank's website.
- If you **enter your username and password**, the scammer steals your bank details.

**What is digital forensic analysis? Discuss shortly about digital forensic lab.**

## What is Digital Forensic Analysis?

**Digital forensic analysis** is the process of **collecting, investigating, and analyzing** digital data from computers, mobile phones, or other electronic devices to find evidence of a crime. It helps police, government agencies, and cybersecurity experts solve cybercrimes.

## Uses of Digital Forensic Analysis:

✓ **Finding evidence** of hacking, fraud, or cybercrime.
✓ **Recovering deleted files** from computers or phones.
✓ **Tracking online criminals** and their activities.
✓ **Helping in court cases** with digital proof.

## What is a Digital Forensic Lab?

A **Digital Forensic Lab** is a special place where experts **examine electronic devices** to find proof of illegal activities. These labs use advanced tools and software to recover lost data, trace hackers, and analyze cybercrimes.

## Functions of a Digital Forensic Lab:

- **Data Recovery** – Restoring deleted or hidden files.
- **Cybercrime Investigation** – Finding proof of hacking, fraud, or illegal activities.
- **Network Analysis** – Checking online activities to find criminals.
- **Evidence Collection** – Gathering legal proof for court cases.

**What is meant by insider threat? How does it affect organization?**

## What is Insider Threat?

An insider threat is a security risk that comes from within an organization. It happens when an employee, contractor, or business partner misuses their access to harm the company. This could be intentional (fraud, data theft) or accidental (carelessness, mistakes).

## Types of Insider Threats:

- **Malicious Insider –** An employee steals company data or leaks confidential information.
- **Negligent Insider –** Someone accidentally shares sensitive information.
- **Compromised Insider –** A hacker tricks an employee into giving access (e.g., phishing attack).

---

## How Does Insider Threat Affect an Organization?

- **Data Theft –** Employees may steal customer data, trade secrets, or financial information.
- **Financial Loss –** Cyberattacks from insiders can cause huge financial damage to the company.
- **Reputation Damage –** Leaking confidential data can make customers lose trust in the company.
- **Legal Issues –** Companies may face lawsuits if personal or financial data is leaked.
- **Cybersecurity Risks –** Weak internal security can help hackers get into the company system.

**What is difference between DOS and DDOS?**

## Difference Between DoS and DDoS

Both DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks are cyberattacks that try to overload a system and make it unavailable to users. However, there are key differences between them.

| Feature | DoS Attack | DDoS Attack |
|---|---|---|
| **Full Form** | Denial of Service | Distributed Denial of Service |
| **Number of Attackers** | One attacker | Multiple attackers (botnet) |
| **How It Works** | A single computer sends excessive requests to crash a server. | Many computers (infected with malware) attack a server at the same time. |
| **Speed of Attack** | Slower attack, easier to stop. | Faster and more powerful, harder to stop. |
| **Detection** | Easier to detect and block. | Harder to detect because it comes from multiple sources. |
| **Example** | A hacker floods a website with fake traffic from one system. | A hacker infects thousands of devices worldwide and uses them to attack a website. |

---

## What is DoS Attack?

A DoS (Denial of Service) attack is when a hacker sends too many requests to a website or server to crash it and make it unavailable for real users.

- Example: A hacker sends thousands of fake login requests to a bank's website, making it too slow for real customers to use.

## What is DDoS Attack?

A DDoS (Distributed Denial of Service) attack is a bigger version of a DoS attack. It uses multiple infected computers (botnet) from different locations to attack a website or server at the same time.

- **Example:** A hacker controls thousands of infected devices and uses them to flood an e-commerce website with fake traffic, causing it to crash.

**Rapid development of science and technology Cybercrime are increasing day by day. Explain in the light of the given statement.**

### Rapid Development of Science and Technology & Increasing Cybercrime

Science and technology are advancing **very fast**, making life easier and more connected. The internet, smartphones, AI, cloud computing, and digital banking have transformed how we live and work. However, with these advancements, cybercrime is also increasing day by day.

---

### How Science & Technology Growth Leads to Cybercrime?

1️⃣ **More Internet Users = More Cyber Threats**

- Billions of people use the **internet, social media, and online banking** every day.
- Cybercriminals **target online users** through fraud, hacking, and scams.

2️⃣ **Advanced Hacking Techniques**

- **AI & automation** help both companies and hackers.
- **Hackers use AI** to create smarter **malware, phishing attacks, and deepfakes** to steal information.

3️⃣ **Increase in Online Transactions**

- Digital banking, e-commerce, and **cashless payments** have become common.
- Hackers **steal credit card details, passwords, and financial data** through cyberattacks.

4️⃣ **Weak Cybersecurity in Many Sectors**

- Small businesses and individuals often **lack strong security**.
- Hackers **exploit weak passwords, outdated software, and security gaps**.

5️⃣ **Growth of IoT (Internet of Things) Devices**

- Smart gadgets (CCTV, smartwatches, smart homes) **connect to the internet**.
- Many of these devices **lack proper security**, making them easy targets for cybercriminals.

**Short notes on e-mail, internet and social media abuse for harassment.**

# 1. E-mail Abuse for Harassment

E-mail abuse occurs when someone **uses e-mails to threaten, harass, or intimidate others**. This can include:

- **Spam or phishing emails** to steal personal data.

- **Threatening or abusive messages** sent repeatedly.
- **Fake e-mails** spreading false information about a person.

### Example:

A person receives repeated emails containing **threats, insults, or blackmail** from an unknown sender.

---

## 2. Internet Abuse for Harassment

Internet abuse refers to the **misuse of online platforms to harm or harass others**. This includes:

- **Cyberstalking** – Repeatedly monitoring or sending unwanted messages to someone online.
- **Doxxing** – Publishing someone's private information without permission.
- **Online threats** – Sending harmful messages through websites or forums.

### Example:

A hacker leaks someone's **personal photos and contact details** on a public forum to harm them.

---

## 3. Social Media Abuse for Harassment

Social media abuse happens when **people misuse platforms like Facebook, Instagram, Twitter, or TikTok to harass others**. It includes:

- **Cyberbullying** – Posting hurtful comments or spreading false rumors.
- **Trolling** – Posting offensive or provocative content to provoke reactions.
- **Impersonation** – Creating fake profiles to ruin someone's reputation.

### Example:

A group of people **target an individual with negative comments, fake stories, or hate speech** on social media.

***An unknown company use a domain name smaller to IBM and post absence matter on the website. What is the offense committed by the company? Explain.***

### Offense Committed by the Company

The unknown company has committed **cybersquatting and trademark infringement** by using a domain name similar to IBM and posting false content.

## 1. Cybersquatting (Domain Name Infringement)

- **Cybersquatting** occurs when someone **registers, uses, or sells a domain name similar to a well-known brand** to mislead users or gain profit.
- In this case, the company **used a domain name similar to IBM**, which can confuse users and damage IBM's reputation.

✅ **Example:** If someone registers **"IBMM.com"** or **"IBM-info.com"** without IBM's permission, it is cybersquatting.

## 2. Trademark Infringement

- IBM is a **registered trademark**, and using a similar name **without permission** violates **intellectual property laws**.
- Trademark laws **protect businesses from others using their name to mislead customers**.

✅ **Example:** Selling fake Apple products using the name **"Aple"** would be trademark infringement.

## 3. Defamation (If False Content is Posted)

- If the company **posted false and damaging information about IBM**, it can be **defamation**.
- **Defamation laws protect individuals and companies from false statements that harm their reputation**.

***Smart Bangladesh Vision 2041 is about more than a futuristic Bangladesh, built on the 4 pillars of Smart Citizens, Smart Government, Smart Economy and Smart Society. In the light of the statement discuss the reediness and challenges.***

## Smart Bangladesh Vision 2041: Readiness and Challenges

The **Smart Bangladesh Vision 2041** aims to create a **digitally advanced nation** based on **four key pillars: Smart Citizens, Smart Government, Smart Economy, and Smart Society**.

## Readiness:

✓ **Digital Infrastructure:** Expansion of high-speed internet, 5G, and smart cities.
✓ **E-Governance:** Online public services, digital ID, and automated systems.
✓ **Economic Growth:** Digital startups, freelancing, and cashless transactions.
✓ **Education & Innovation:** Technology-driven learning and research advancements.

## Challenges:

❌ **Digital Divide:** Unequal internet access in rural areas.
❌ **Cybersecurity Risks:** Increasing cyber threats and data privacy issues.
❌ **Skilled Workforce:** Need for better tech-based education and job training.
❌ **Financial Barriers:** High costs of digital transformation for businesses.

***Write short notes about the infrastructure needed for e_Learning setup in our country. Also discuss the advantages and disadvantages of e-Learning.***

## Infrastructure Needed for E-Learning Setup in Bangladesh

To establish a strong **e-Learning system**, the following infrastructure is required:

✓ **High-Speed Internet:** Stable and affordable internet access for students and teachers.
✓ **Digital Devices:** Laptops, tablets, and smartphones for accessing online classes.
✓ **E-Learning Platforms:** Websites, mobile apps, and Learning Management Systems (LMS).
✓ **Digital Content & Resources:** Interactive videos, e-books, and online assessments.
✓ **Teacher Training:** Educators need proper training in digital teaching methods.

---

## Advantages of E-Learning

✅ **Flexible Learning:** Students can learn anytime, anywhere.
✅ **Cost-Effective:** Reduces transportation and material costs.
✅ **Access to Global Knowledge:** Students can take courses from international institutions.
✅ **Interactive & Engaging:** Multimedia content makes learning more effective.

---

## Disadvantages of E-Learning

❌ **Internet & Device Dependency:** Many students lack access to reliable internet or devices.
❌ **Lack of Practical Learning:** Hands-on training is difficult in subjects like science and engineering.
❌ **Less Student Engagement:** Without face-to-face interaction, students may lose interest.
❌ **Cybersecurity Risks:** Online platforms can be vulnerable to hacking and data breaches.

***Short notes on e-Commerce, e-Governance and e-Voting in Bangladesh***

## *Short Notes on E-Commerce, E-Governance, and E-Voting in Bangladesh*

### *1. E-Commerce in Bangladesh*

E-Commerce (Electronic Commerce) refers to buying and selling goods and services online. In Bangladesh, e-commerce has grown rapidly due to internet access, mobile banking, and digital payments.

✅ **Popular Platforms:** Daraz, Evaly (now defunct), Chaldal, Pathao, Foodpanda.
✅ **Payment Methods:** bKash, Nagad, Rocket, Debit/Credit Cards.
✅ **Challenges: Fraud,** logistics issues, and lack of consumer trust.

---

### 2. E-Governance in Bangladesh

E-Governance means using digital technology to improve government services and communication with citizens.

✅ **Initiatives:** Digital Bangladesh, NID smart card, e-Tax system, e-Passport.
✅ **Benefits:** Faster service delivery, less corruption, and improved transparency.
✅ **Challenges:** Limited internet access in rural areas and cybersecurity threats.

---

### 3. E-Voting in Bangladesh

E-Voting (Electronic Voting) allows people to cast votes digitally instead of using paper ballots.

✅ **Implemented in Some Areas:** Electronic Voting Machines (EVMs) were used in recent elections.
✅ **Advantages:** Reduces vote counting time, prevents fake voting.
✅ **Challenges:** Security risks, technical failures, and lack of voter awareness.

By improving technology, security, and awareness, these digital services can help Bangladesh move towards a Smart Bangladesh Vision 2041.

***Explain the concept of intellectual property rights.***

### Concept of Intellectual Property Rights (IPR)

**Intellectual Property Rights (IPR)** refer to **legal protections given to creators for their inventions, artistic works, designs, and brand names**. These rights allow creators to **control, benefit from, and prevent others from using their work without permission**.

---

### Types of Intellectual Property Rights:

✓ **Copyright:** Protects creative works like books, music, films, and software.
✓ **Patent:** Grants exclusive rights to inventors for new inventions or technologies.
✓ **Trademark:** Protects brand names, logos, and symbols (e.g., Apple, Nike).
✓ **Trade Secrets:** Protects confidential business information (e.g., Coca-Cola recipe).
✓ **Industrial Design:** Protects the unique design or shape of a product.

---

## Why is IPR Important?

✅ **Encourages Innovation:** Inventors and creators get rewards for their work.
✅ **Protects Businesses:** Prevents others from copying ideas or brand names.
✅ **Boosts Economy:** Helps industries grow by promoting creativity and investment.
✅ **Ensures Fair Competition:** Stops unfair use of someone else's work.

**List out the basic principles of design rights.**

## What is a Trademark?

A Trademark is a unique sign, word, symbol, logo, or combination of these that represents a business, product, or service. It helps consumers identify and distinguish a brand from others.

In Cyber Law, trademarks also protect online businesses, domain names, and digital platforms from misuse, fraud, and infringement.

---

## Essential Elements of a Trademark:

1. **Distinctiveness –** The trademark must be unique and recognizable.
2. **Non-Deceptiveness –** It should not mislead consumers about the product or service.
3. **Non-Functionality –** It should only serve as a brand identifier, not a functional feature.
4. **Legal Protection –** A registered trademark gives exclusive rights to its owner.
5. **Use in Commerce –** It must be actively used in business, including online platforms.

---

## Functions of a Trademark:

1. **Brand Recognition –** Helps consumers identify a trusted business.
2. **Prevents Imitation & Fraud –** Protects against counterfeit brands and online infringement.
3. **Legal Protection –** Gives the owner exclusive rights to use and defend the mark in court.
4. **Supports Online Presence –** Protects domain names and digital assets from cyber threats like cybersquatting.

5. **Builds Consumer Trust –** Ensures authenticity and credibility in online and offline markets.

## Basic Principles of Trademark

1. **Distinctiveness** – The trademark must be unique and capable of distinguishing goods or services from others.
2. **Non-Deceptiveness** – It should not mislead consumers about the nature, quality, or origin of the product or service.
3. **Exclusive Rights** – The owner of a registered trademark has the sole right to use and protect it from unauthorized use.
4. **Use in Commerce** – A trademark must be actively used in business to maintain its legal protection.

**Explain digital signature and digital certificate with block diagram.**

## Digital Signature & Digital Certificate

### 1. Digital Signature:

A **Digital Signature** is an electronic signature that ensures the authenticity and integrity of a digital message or document. It is created using cryptographic techniques, specifically **public-key encryption**, to verify that a document has not been altered and that it comes from a trusted source.

#### Working of Digital Signature:

- The sender's private key is used to create the signature.
- The receiver verifies the signature using the sender's public key.
- If the verification is successful, it ensures the document's authenticity and integrity.

---

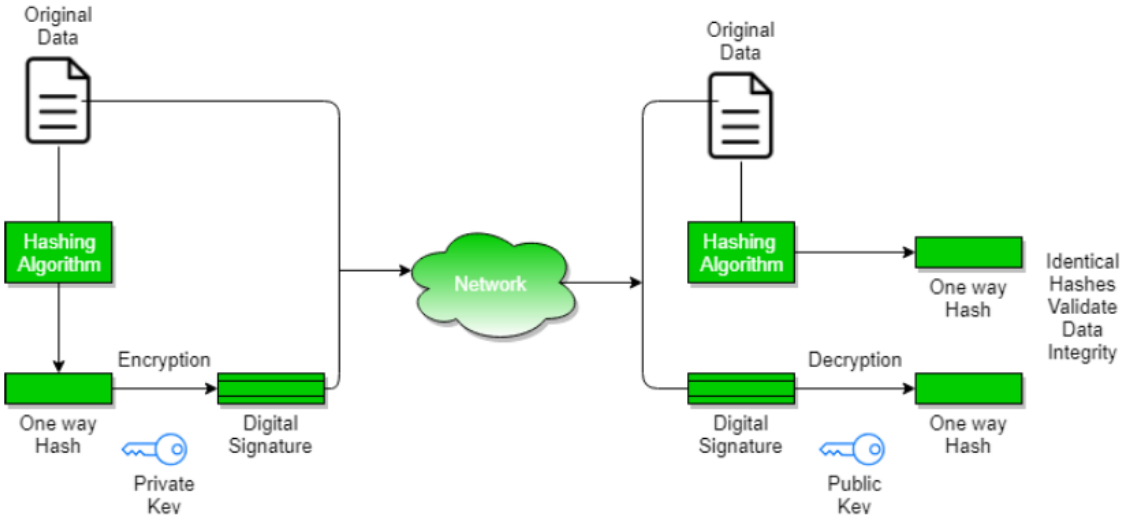
### 2. Digital Certificate:

A **Digital Certificate** is an electronic document issued by a **Certificate Authority (CA)** that verifies the identity of an individual, organization, or website. It contains information like the user's **public key, name, expiration date, and the CA's digital signature**.

#### Purpose of Digital Certificate:

- Ensures that a website, email, or entity is legitimate.
- Used in **SSL/TLS encryption** for secure online communication.
- Helps prevent **phishing attacks and fraud**.

**Block Diagram of Digital Signature & Digital Certificate:**




***How digital signature authenticate and protect the documents? Explain with example***

## How Digital Signature Authenticates and Protects Documents

A **digital signature** is a cryptographic method used to verify the authenticity, integrity, and security of digital documents. It ensures that the document has not been altered and confirms the identity of the sender.

---

## How Digital Signature Works?

Digital signatures use **public-key cryptography (asymmetric encryption)**. The process involves two keys:

- **Private Key** (used for signing)
- **Public Key** (used for verification)

**Steps for Authentication and Protection:**

1. **Document Hashing:**
    - A mathematical algorithm creates a unique **hash value** (fixed-length string) from the document.
    - This hash ensures that even a small change in the document results in a completely different hash.
2. **Signing the Document:**
    - The sender encrypts the hash with their **private key**, creating the **digital signature**.
    - The signed document is then sent to the receiver.
3. **Verification by Receiver:**
    - The receiver decrypts the signature using the sender's **public key**, revealing the original hash.

    - The receiver also generates a new hash from the received document and compares it with the decrypted hash.
4. **If Both Hashes Match:**
    - The document is **authentic** (it came from the correct sender).
    - The document is **unchanged** (no modifications were made).

---

## Example of Digital Signature in Use

**Scenario:** A company director digitally signs an important contract and emails it to a business partner.

- **Step 1:** The director's private key encrypts the document's hash, creating a **digital signature**.
- **Step 2:** The signed document is sent to the business partner.
- **Step 3:** The business partner uses the director's **public key** to decrypt the signature and get the original hash.
- **Step 4:** The business partner compares it with a newly computed hash from the received document.

- **If hashes match** → The document is authentic and unchanged.
- **If hashes don't match** → The document was tampered with.

***Define copy rights and patents. Write the differences between copy rights and patents***

## Definition of Copyright and Patent

1. **Copyright:**
   Copyright is a legal right that protects **original works of authorship**, such as books, music, films, software, and artistic creations. It gives the creator the exclusive right to reproduce, distribute, and display their work.
2. **Patent:**
   A patent is a legal right granted to an inventor for a **new and useful invention**. It gives the inventor the exclusive right to make, use, sell, or license the invention for a specific period (usually **20 years**).

---

## Differences Between Copyright and Patent

| Feature | Copyright | Patent |
|---|---|---|
| **Protection** | Protects **original creative works** (literary, artistic, musical, and software). | Protects **new inventions** (products, processes, or machines). |
| **Duration** | Usually lasts for **60+ years** (varies by country). | Lasts for **20 years** from the filing date. |

| | | |
|---|---|---|
| **Type of Work** | Covers **books, movies, software, music, paintings, etc.** | Covers **inventions, new technologies, industrial designs, etc.** |
| **Rights Given** | Allows the creator to **reproduce, distribute, and display** the work. | Allows the inventor to **make, use, sell, or license** the invention. |
| **Requirement for Protection** | Automatically granted when a work is created in a tangible form. | Requires **official application and approval** from a patent office. |
| **Example** | A writer gets copyright for a book. | A scientist gets a patent for a new drug formula. |

**Write short notes on WIPO Treaty.**

## WIPO Treaty – Short Notes (For 4 Marks)

The **WIPO Treaty** includes international agreements overseen by the **World Intellectual Property Organization (WIPO)** to protect intellectual property (IP) globally.

## Key WIPO Treaties:

1. **WIPO Copyright Treaty (WCT) – 1996**: Protects digital copyright, ensuring creators' rights over online works like music, books, and software.
2. **WIPO Performances and Phonograms Treaty (WPPT) – 1996**: Protects performers and producers' rights over digital performances and recordings.
3. **Patent Cooperation Treaty (PCT) – 1970**: Simplifies the process of applying for patents internationally.
4. **Madrid Protocol – 1989**: Allows businesses to register trademarks in multiple countries with a single application.

## Objectives:

- **Harmonize** intellectual property laws globally.
- **Protect** creators' rights.
- Foster **international cooperation** in enforcing IP rights.

**What is Cyber fraud? Distinguish hackers and crackers.**

## Cyber Fraud

**Cyber fraud** refers to illegal activities conducted through digital means to deceive individuals or organizations for financial gain. It includes identity theft, phishing, online scams, credit card fraud, and hacking into accounts or systems to steal sensitive information.

## Difference Between Hackers and Crackers

| Feature | Hackers | Crackers |
|---|---|---|
| **Definition** | Individuals who gain unauthorized access to computer systems, often to test security or improve cybersecurity. | Individuals who break into systems with malicious intent, such as stealing data or causing damage. |
| **Intent** | Can be ethical (White Hat Hackers) or unethical (Black Hat Hackers). | Always unethical, aiming to damage, steal, or disrupt systems. |
| **Legality** | Ethical hackers work legally to improve cybersecurity. Unethical hackers engage in cybercrime. | Illegal activities, such as hacking passwords, spreading malware, and bypassing security measures. |
| **Examples** | Ethical hackers work for companies to strengthen security. Black hat hackers exploit vulnerabilities for profit. | Crackers steal sensitive data, deface websites, and spread ransomware. |

**Explain computer software as Intellectual Property and its protection.**

## Computer Software as Intellectual Property and Its Protection

**Computer software** is considered a form of **intellectual property (IP)** because it is a product of human creativity and innovation. It includes programs, applications, and systems developed to perform specific tasks on computers and digital devices. As IP, software is protected under **copyright laws** and may also involve **patents** for unique algorithms or functionalities.

**Protection of Computer Software:**

1. **Copyright**:
    - Software is primarily protected by **copyright** as a literary work. The author or developer has exclusive rights to reproduce, distribute, and modify the software.
    - Copyright ensures that unauthorized copying, sharing, or altering of the software is prohibited.
2. **Licensing**:
    - Software developers use licenses (e.g., open-source or proprietary) to define how users can interact with the software. A **license agreement** outlines whether users can modify or redistribute the software.
3. **Patents**:
    - In some cases, **patents** can be granted for innovative software features or processes, particularly if the software introduces a new and useful technological solution.

**Explain protection of copyrights in digital media.**

## Protection of Copyrights in Digital Media

The protection of copyrights in **digital media** addresses the challenges posed by easy reproduction, distribution, and sharing of content online. Digital media includes works like music, movies, software, e-books, and videos. Here are key ways to protect copyrights in this space:

1. **Digital Rights Management (DRM)**:
    - DRM technologies control access to digital content by preventing unauthorized copying, sharing, or distribution. They ensure that creators or distributors retain control over how their content is used.
2. **Anti-Piracy Laws and Enforcement**:
    - Laws like the **Digital Millennium Copyright Act (DMCA)** protect digital content from unauthorized distribution and reproduction. These laws allow content owners to file complaints and request the removal of infringing content from websites or platforms.
3. **Licensing Agreements and Watermarking**:
    - Licensing agreements define how digital content can be accessed, shared, or used. **Watermarking** embeds information into digital files, helping track ownership and deter unauthorized use.

These protections help creators safeguard their intellectual property from unauthorized use and distribution in the digital environment.

**Explain patent protection.**

## Patent Protection

**Patent protection** is a legal right granted to an inventor, allowing them to exclude others from making, using, selling, or distributing their invention without permission for a certain period, usually **20 years** from the filing date. It encourages innovation by providing inventors with exclusive rights to benefit from their creations.

***Justify protection of semi conductor chips. State & explain Semiconductor IC layout design act?***

## Protection of Semiconductor Chips & Semiconductor IC Layout Design Act

### Justification for Protection of Semiconductor Chips

Semiconductor chips are essential in modern electronics, and their protection is necessary because:

1. **High Development Cost** – Designing chips requires heavy investment in research and technology.
2. **Intellectual Property Rights** – Prevents unauthorized copying and protects innovators.
3. **Encourages Innovation** – Ensures companies continue developing advanced chips.
4. **Prevents Counterfeiting** – Stops low-quality duplicate chips from entering the market.

**Semiconductor IC Layout Design Act**

This act protects the **original layout designs** of semiconductor chips to prevent illegal reproduction.

- **Exclusive Rights**: Only the creator can reproduce or use the layout commercially.
- **Duration**: Usually protected for **10 years** after registration.
- **Registration**: The design must be **original and unique** to be legally protected.
- **Penalties for Infringement**: Unauthorized copying can lead to **legal action and fines**.