Law 2211: Cyber and Intellectual Property Law

Made by Md. Mehedi Hasan Rafy

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

Solution:

Cyberspace

Cyberspace refers to the virtual environment of the internet where digital communications, transactions, and interactions occur. It includes computer networks, websites, social media, and online data exchanges.

Cyber Law

Cyber law, also known as internet law, governs legal issues related to cyberspace. It includes regulations on cybercrimes, e-commerce, intellectual property, data protection, and online transactions.

Advantages of Cyber Law

1. Protects individuals and organizations from cybercrimes.
2. Regulates e-commerce and digital transactions.
3. Safeguards intellectual property rights online.
4. Ensures privacy and data protection.
5. Establishes legal frameworks for digital contracts.

Disadvantages of Cyber Law

1. Difficult to enforce across international borders.
2. Cybercriminals continuously find loopholes.
3. Some laws may infringe on digital freedom.
4. Requires constant updates due to evolving technology.
5. Legal processes for cybercrimes can be complex and time-consuming.

2. ***Discuss the various Cybercrime related to online banking.***

Solution:

Cybercrimes Related to Online Banking

1. ***Phishing*** – Fraudulent emails or websites trick users into revealing banking credentials.
2. ***Vishing*** – Voice phishing where scammers use phone calls to steal sensitive information.
3. ***Smishing*** – SMS-based phishing to deceive users into sharing financial details.
4. ***Card Skimming*** – Unauthorized copying of debit/credit card information using skimming devices.
5. ***Hacking*** – Unauthorized access to bank accounts through malware or brute force attacks.

6. ***Identity Theft*** – Criminals use stolen personal details to make fraudulent transactions.
7. ***Man-in-the-Middle (MITM) Attacks*** – Hackers intercept communication between users and banks to steal data.
8. ***Ransomware Attacks*** – Cybercriminals encrypt banking data and demand ransom for decryption.
9. ***SIM Swap Fraud*** – Criminals duplicate a user's SIM card to bypass two-factor authentication and access bank accounts.
10. ***Fake Banking Apps*** – Fraudsters create counterfeit apps to steal user credentials.

3. What is identity theft? Explain with example.

Solution:

Identity Theft

Identity theft is a cybercrime where someone illegally obtains and uses another person's personal or financial information, such as name, bank details, or social security number, to commit fraud or theft. Identity theft can lead to financial loss, legal issues, and damage to the victim's reputation.

Example : A hacker steals a person's credit card details and makes unauthorized online purchases. Another example is when a fraudster uses someone's identity to apply for a loan, leaving the victim in financial trouble.

4. Discuss various International conventions and Treaties on Cybercrime.

Solution:

International Conventions and Treaties on Cybercrime

1. ***Budapest Convention (2001)*** – First global treaty on cybercrime; focuses on legal harmonization, cooperation, and investigation.
2. ***UN Resolutions*** – Promote global cooperation and legal frameworks against cyber threats.
3. ***Tallinn Manual (2013, 2017)*** – Guides how international law applies to cyber warfare.
4. ***Malabo Convention (2014)*** – African Union's legal framework for cybersecurity, data protection, and e-transactions.
5. ***APEC Cybersecurity Strategy*** – Strengthens cybersecurity in the Asia-Pacific region.
6. ***SCO Cyber Agreements*** – Focus on combating cyberterrorism and enhancing security cooperation.

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

Solution:

Powers of Cyber Appellate Tribunal

The ***Cyber Appellate Tribunal*** is a specialized judicial body that hears appeals against decisions made by cyber adjudicating authorities. Its powers include:

1. ***Hearing Appeals*** – Reviews decisions from lower cybercrime courts.
2. ***Summoning & Evidence Collection*** – Can summon witnesses and demand documents.
3. ***Issuing Orders & Penalties*** – Imposes fines, awards compensation, and passes judgments.

4. ***Overruling Decisions*** – Can modify or reverse lower authority rulings.
5. ***Enforcing Compliance*** – Ensures individuals and organizations follow cyber laws.
6. ***Judicial Review*** – Ensures decisions align with national laws and constitutional rights.

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

Solution:

Protection of Digital Signature in Bangladesh

Yes, digital signatures are protected under the ***Information and Communication Technology (ICT) Act, 2006*** of Bangladesh. The Act recognizes digital signatures as legally valid and enforceable.

Method Adopted by the Act

1. ***Public Key Infrastructure (PKI)*** – Uses cryptographic methods for security.
2. ***Certification Authority (CA)*** – Licensed CAs issue digital signature certificates.
3. ***Legal Recognition*** – Digital signatures are legally equivalent to handwritten signatures.
4. ***Security Measures*** – Unauthorized use, forgery, or tampering is punishable.

7. Classify Cybercrime with example and categorize Cyber criminals.

Solution:

Classification of Cybercrime

1. ***Cyber Crimes Against Individuals***
   - ***Identity Theft*** – Stealing personal data for fraud.
   - ***Cyberstalking*** – Harassing through emails/social media.
   - ***Phishing*** – Fake emails tricking users into sharing credentials.
2. ***Cyber Crimes Against Organizations***
   - ***Hacking*** – Unauthorized access to company databases.
   - ***Ransomware Attacks*** – Encrypting files, demanding ransom.
   - ***DoS Attacks*** – Flooding websites to disrupt services.
3. ***Cyber Crimes Against Government***
   - ***Cyber Terrorism*** – Hacking government networks.
   - ***Espionage*** – Spying on government agencies.
   - ***Website Defacement*** – Altering official government sites.
4. ***Cyber Crimes Against Property***
   - ***Credit Card Fraud*** – Using stolen card details.
   - ***IP Theft*** – Software, music, or film piracy.
   - ***Cryptocurrency Fraud*** – Hacking wallets for digital assets.

Categories of Cyber Criminals

1. ***Hackers*** – Individuals who break into systems, either ethically (White Hat) or maliciously (Black Hat).
2. ***Crackers*** – Cybercriminals who bypass security measures to cause damage or theft.
3. ***Cyber Terrorists*** – Attack government systems to spread fear or political agendas.
4. ***Hacktivists*** – Hackers who attack systems for political or social causes.
5. ***Fraudsters*** – Individuals involved in online scams, phishing, and identity theft.
6. ***Insiders*** – Employees or former employees who misuse company data for personal gain.
7. ***Script Kiddies*** – Inexperienced hackers who use pre-made tools to launch attacks.

8. Write the strategies can be used to prevent Cybercrime.

Solution:

Strategies to Prevent Cybercrime

1. ***Strong Passwords*** – Use complex, unique passwords and enable multi-factor authentication (MFA).
2. ***Regular Software Updates*** – Keep operating systems, antivirus, and applications updated to patch vulnerabilities.
3. ***Firewalls & Antivirus Protection*** – Install and maintain strong security software to detect and block threats.
4. ***Awareness & Training*** – Educate individuals and employees on phishing, scams, and safe online practices.
5. ***Secure Networks*** – Use encrypted Wi-Fi, VPNs, and avoid public networks for sensitive transactions.
6. ***Data Encryption*** – Protect sensitive information using encryption techniques to prevent unauthorized access.
7. ***Regular Backups*** – Keep offline and cloud backups to recover from ransomware or data loss.
8. ***Restrict Access*** – Limit user access to sensitive data and use role-based permissions.
9. ***Legal Compliance*** – Follow cybersecurity laws and regulations to ensure legal protection.
10. ***Incident Response Plan*** – Establish a strategy to detect, report, and recover from cyber incidents.

9. What is phishing? Explain with example.

Solution:

Phishing

Phishing is a cybercrime where attackers trick individuals into revealing sensitive information, such as passwords, credit card details, or personal data, by pretending to be a trustworthy entity. It is usually done through fraudulent emails, messages, or websites.

Example: A user receives an email appearing to be from their bank, stating that their account will be locked unless they verify their credentials. The email contains a fake link that leads to a website resembling the bank's official site. When the user enters their login details, the attacker captures them and gains access to the account.

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

Solution:

Digital Forensic Analysis

Digital forensic analysis is the process of collecting, preserving, and analyzing electronic data to investigate cybercrimes. It helps in identifying, recovering, and presenting digital evidence in legal cases.

Digital Forensic Lab

A Digital Forensic Lab is a specialized facility equipped with tools and software for conducting forensic investigations. It includes:

1. ***Data Recovery Tools*** – Extract lost or deleted files.
2. ***Network Analysis Systems*** – Monitor and analyze cyber threats.
3. ***Malware Analysis Tools*** – Detect and examine malicious software.
4. ***Cryptographic Analysis*** – Decrypt and analyze encrypted data.
5. ***Secure Storage*** – Preserve digital evidence without tampering.

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

Solution:

Insider Threat

An insider threat occurs when an employee, contractor, or business partner misuses their access to an organization's systems, data, or resources, either intentionally or unintentionally, causing harm.

Effects on Organizations

1. ***Data Breach*** – Confidential information may be leaked or sold.
2. ***Financial Loss*** – Fraud or theft by insiders can result in huge losses.
3. ***Reputation Damage*** – Loss of customer trust due to insider leaks.
4. ***Operational Disruptions*** – Malicious insiders may delete or alter critical data.
5. ***Legal Consequences*** – Violations of data protection laws can lead to lawsuits and penalties.

12. What is difference between DOS and DDOS?

Solution:

DoS vs DDoS Attacks

Feature	***DoS (Denial of Service)***	***DDoS (Distributed Denial of Service)***
Definition	A cyberattack that overwhelms a system or network with excessive requests from a single source.	A large-scale attack using multiple systems or botnets to flood a target with traffic.
Attack Source	Single attacker/machine.	Multiple attackers or infected devices (botnet).
Impact	Slows down or crashes the targeted service.	More severe, often making the system completely unavailable.

Complexity	Easier to detect and block.	Harder to mitigate due to multiple attack sources.

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

Solution:

<u>Cybercrime and the Rapid Development of Science & Technology</u>

The rapid advancement of science and technology has transformed communication, business, and daily life, but it has also led to a sharp rise in cybercrime. The increasing dependence on digital platforms has created new vulnerabilities that cybercriminals exploit.

<u>Reasons for Increasing Cybercrime</u>

1. ***Widespread Internet Use*** – More people online means more targets for cybercriminals.
2. ***Advanced Hacking Techniques*** – Attackers use AI, automation, and sophisticated malware.
3. ***Growth of Digital Transactions*** – Online banking and e-commerce attract fraud and scams.
4. ***IoT and Smart Devices*** – Insecure smart gadgets can be hacked for data theft.
5. ***Anonymity on the Dark Web*** – Criminals use encrypted platforms to hide identities.
6. ***Lack of Awareness*** – Many users fall victim to phishing, scams, and weak security practices.

14. Write a detail note on Cyber defamation.

Solution:

<u>Cyber defamation</u>

Cyber defamation is harming a person's or organization's reputation through false and defamatory statements online via social media, websites, emails, etc.

<u>Types</u>

1. ***Libel*** – False statements published online (e.g., fake news, defamatory posts).
2. ***Slander*** – Spoken defamation via videos, voice messages, or live streams.

<u>Examples</u>

- Posting false allegations on social media.
- Publishing defamatory blogs/articles.
- Spreading fake reviews to harm businesses.
- Sharing doctored images/videos to mislead.

<u>Legal Provisions</u>

- ***Bangladesh – ICT Act 2006 & Digital Security Act 2018*** (punishment: fines/imprisonment).
- ***India*** – Section 499 & 500 IPC (criminal defamation).
- ***USA & Europe*** – Covered under **Defamation Laws**, with free speech limitations.

Punishment & Remedies

- Filing legal complaints.
- Court orders to remove content.
- Compensation for damages.
- Criminal charges in severe cases.

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

Solution:

E-mail Abuse for Harassment

- Sending threatening, abusive, or offensive emails to intimidate or blackmail someone.
- Phishing emails trick users into revealing personal or financial information.
- Spamming with unwanted messages, often containing malicious links or scams.
- ***Example:*** Repeatedly sending hate emails to harass an individual.

Internet Abuse for Harassment

- ***Cyberstalking*** – Monitoring or threatening someone online.
- ***Doxxing*** – Publishing personal information (address, phone number) without consent.
- ***Trolling*** – Posting hateful or provocative content to incite conflict.
- ***Example:*** Hacking someone's account and misusing their data for harassment.

Social Media Abuse for Harassment

- ***Cyberbullying*** – Using social media to insult, shame, or threaten someone.
- ***Impersonation*** – Creating fake profiles to spread false information or ruin reputations.
- ***Revenge Porn*** – Sharing explicit images or videos without consent.
- ***Example:*** Posting false rumors about someone on Facebook or Twitter to damage their reputation.

16. 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.

Solution:

Offense Committed by the Company

The company has committed cybersquatting and cyber defamation by using a domain name similar to IBM and posting false or misleading content.

Cybersquatting

- Cybersquatting refers to the act of registering, using, or selling a domain name similar to a well-known brand to mislead users or gain unfair advantage.
- In this case, the unknown company is using a domain resembling IBM, which can confuse users and harm IBM's brand reputation.
- ***Legal Consequences:*** Many countries, including the U.S. (Anti-Cybersquatting Consumer Protection Act) and international regulations (ICANN's UDRP), prohibit cybersquatting. IBM can file a complaint and request domain cancellation.

Cyber Defamation

- Posting false or offensive content about IBM constitutes cyber defamation, which damages the company's reputation.
- ***Legal Action:*** IBM can sue for defamation under intellectual property laws and cyber laws in various jurisdictions.

17. 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.

Solution:

Smart Bangladesh Vision 2041 aims to transform Bangladesh into a technologically advanced nation based on four pillars: Smart Citizens, Smart Government, Smart Economy, and Smart Society.

Readiness for Smart Bangladesh Vision 2041

1. ***Digital Infrastructure Development*** – Expansion of high-speed internet, 5G rollout, and digital financial services.
2. ***Government Initiatives*** – Policies like "Digital Bangladesh" and e-Governance services promote transparency and efficiency.
3. ***Tech-Savvy Workforce*** – Increasing focus on ICT education, freelancing, and skill development programs.
4. ***Startup & Innovation Growth*** – Emerging fintech, e-commerce, and AI-driven businesses.
5. ***Sustainable Development Goals (SDGs) Alignment*** – Digital solutions for healthcare, education, and agriculture.

Challenges in Achieving Smart Bangladesh Vision 2041

1. ***Digital Divide*** – Unequal access to technology in rural vs. urban areas.
2. ***Cybersecurity Threats*** – Growing risks of cybercrime, data breaches, and lack of robust cybersecurity laws.
3. ***Infrastructure Gaps*** – Need for better digital connectivity and reliable power supply.
4. ***Skill Shortage*** – Need for more trained professionals in AI, robotics, and emerging technologies.
5. ***Data Privacy Concerns*** – Strengthening data protection laws to ensure user security.
6. ***Financial Constraints*** – High investment needed for digital transformation projects.

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

Solution:

Infrastructure Needed for e-Learning in Bangladesh

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

1. ***High-Speed Internet*** – Reliable and affordable internet access for students and teachers.

2. ***Digital Devices*** – Availability of computers, tablets, and smartphones for online learning.
3. ***E-Learning Platforms*** – Development of interactive platforms like Learning Management Systems (LMS).
4. ***Digital Content & Resources*** – E-books, recorded lectures, and online assessments.
5. ***Cybersecurity & Data Protection*** – Ensuring safe online access to prevent cyber threats.
6. ***Teacher Training & Support*** – Training educators to effectively use digital tools.
7. ***Electricity & Connectivity*** – Stable power supply and network coverage, especially in rural areas.

Advantages of e-Learning

1. ***Accessibility*** – Learning is available anytime, anywhere.
2. ***Cost-Effective*** – Reduces transportation and accommodation costs.
3. ***Flexible Learning*** – Students can learn at their own pace.
4. ***Diverse Resources*** – Access to global courses, experts, and multimedia content.
5. ***Interactive & Engaging*** – Use of animations, quizzes, and gamification.

Disadvantages of e-Learning

1. ***Digital Divide*** – Limited access to technology in rural areas.
2. ***Lack of Face-to-Face Interaction*** – Reduced engagement between teachers and students.
3. ***Technical Issues*** – Internet disruptions and software/hardware failures.
4. ***Self-Discipline Required*** – Students may struggle with motivation and focus.
5. ***Security & Privacy Risks*** – Exposure to cyber threats and data breaches.

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

Solution:

E-Commerce in Bangladesh

- ***Definition:*** Buying and selling goods and services online through websites and mobile apps.
- ***Growth:*** Rapid expansion due to increased internet access and mobile banking (e.g., bKash, Nagad).
- ***Popular Platforms:*** Daraz, Chaldal, Evaly (defunct), Pathao Food, etc.
- ***Challenges:*** Logistics issues, fraud cases, and lack of consumer protection.
- ***Government Support:*** Digital commerce policies and VAT regulations to ensure a fair market.

E-Governance in Bangladesh

- ***Definition:*** The use of digital platforms to improve government services and transparency.
- ***Key Initiatives:***
    - ***National e-Service Portal*** – Online services for citizens.
    - ***E-Tendering*** – Digital procurement process.
    - ***Online Tax Payment*** – Simplifies financial transactions.
    - ***MyGov App*** – Provides government-related information and services.
- ***Benefits:*** Reduces corruption, enhances efficiency, and ensures quick public service delivery.
- ***Challenges:*** Limited rural accessibility, cybersecurity concerns, and digital literacy gaps.

E-Voting in Bangladesh

- ***Definition:*** The use of electronic systems to conduct elections and vote counting.
- ***Current Status:*** Limited use, with some Electronic Voting Machines (EVMs) introduced.
- ***Advantages:*** Faster results, reduced ballot manipulation, and increased voter convenience.
- ***Challenges:*** Security risks, risk of hacking, and lack of voter trust in the technology.

20. What is unfair competition? How to protect from it?

Solution:

Unfair Competition

Unfair competition refers to dishonest or deceptive business practices that harm competitors or mislead consumers. It includes false advertising, trademark infringement, trade secret theft, and cybersquatting. Some Examples of unfair competition is:

1. ***Trademark Infringement*** – Using a brand name similar to a well-known company to confuse consumers.
2. ***False Advertising*** – Making misleading claims about a product to gain an unfair advantage.
3. ***Trade Secret Theft*** – Stealing confidential business strategies or formulas.
4. ***Dumping*** – Selling products at extremely low prices to eliminate competition.
5. ***Cybersquatting*** – Registering domain names similar to famous brands to deceive users.

How to Protect from Unfair Competition

1. ***Register Trademarks & Copyrights*** – Protects brand identity and creative works.
2. ***Implement Trade Secret Policies*** – Secure sensitive business information with legal agreements.
3. ***Monitor Market Practices*** – Regularly check for fraudulent activities affecting business.
4. ***File Legal Actions*** – Take legal steps against companies engaging in unfair competition.
5. ***Consumer Awareness*** – Educate customers to identify deceptive marketing and fraud.
6. ***Government Regulations & Enforcement*** – Strengthening laws against unfair trade practices.

21. Explain the concept of intellectual property rights.

Solution:

Concept of Intellectual Property Rights (IPR)

Intellectual Property Rights (IPR) refer to the legal rights granted to individuals or businesses over their creations or inventions. These rights protect intangible assets such as inventions, literary works, designs, and brand names, allowing creators to control and benefit from their work.

Types of Intellectual Property Rights

1. ***Patents*** – Protects inventions and technological innovations (e.g., a new drug formula).
2. ***Copyright*** – Grants protection to literary, artistic, and musical works (e.g., books, films, software).

3. ***Trademarks*** – Safeguards brand names, logos, and symbols that distinguish goods/services (e.g., Coca-Cola logo).
4. ***Trade Secrets*** – Protects confidential business information (e.g., KFC's secret recipe).
5. ***Industrial Designs*** – Covers the aesthetic or ornamental aspect of a product (e.g., unique car designs).
6. ***Geographical Indications (GI)*** – Identifies products originating from a specific place (e.g., Darjeeling Tea).

Importance of IPR

- ***Encourages Innovation*** – Provides financial incentives for inventors.
- ***Protects Creators' Rights*** – Ensures fair recognition and profit.
- ***Boosts Economic Growth*** – Encourages investment in research and development.
- ***Prevents Unauthorized Use*** – Stops copying, counterfeiting, and piracy.

22. List out the basic principles of design rights.

Solution:

Basic Principles of Design Rights

Design Rights protect the visual appearance of a product, including its shape, pattern, color, and ornamentation. The key principles include:

1. ***Novelty*** – The design must be new and original, not previously disclosed or used.
2. ***Distinctiveness*** – It should have a unique appearance that differentiates it from existing designs.
3. ***Industrial Applicability*** – The design must be applicable to an industrial or commercial product (e.g., furniture, fashion, electronics).
4. ***Aesthetic Appeal*** – Protection is granted for visual aspects, not functional features.
5. ***Non-Offensive & Legal*** – The design must not violate public morality, laws, or existing copyrights/trademarks.
6. ***Fixed Duration of Protection*** – Design rights are granted for a limited time (usually 10-25 years, depending on the country).
7. ***Registration Requirement*** – In most cases, designs need to be registered with relevant authorities (e.g., EUIPO, USPTO, DPDT in Bangladesh).

23. Enumerate the basic principles of Trademark.

Solution:

Basic Principles of Trademark

A trademark is a unique symbol, name, logo, slogan, or design that distinguishes a business's goods or services from others. The basic principles of trademarks include:

1. ***Distinctiveness*** – The trademark must be unique and recognizable, not generic or descriptive.
2. ***Non-Deceptiveness*** – It should not mislead consumers about the nature, quality, or origin of goods/services.

3. ***Exclusivity*** – The registered owner has the exclusive right to use the mark and prevent unauthorized use.
4. ***Territoriality*** – Trademark rights are generally protected within specific jurisdictions where they are registered.
5. ***First-to-Use or First-to-File*** – Protection depends on whether the country follows first-to-use (e.g., USA) or first-to-file (e.g., China) principles.
6. ***Functionality Exclusion*** – A trademark cannot be granted for a functional product feature (e.g., a bottle shape that improves grip).
7. ***Renewability*** – Trademark protection can be indefinitely renewed (usually every 10 years) as long as it is in use.
8. ***Non-Violation of Public Order*** – The mark must not contain offensive, immoral, or illegal elements.
9. ***Protection Against Infringement*** – Owners can take legal action against counterfeiters or unauthorized users.

24. What is a Trademark? What are its essential elements? What are its functions?
Solution:

Trademark
A trademark is a unique symbol, name, logo, slogan, or design that identifies and differentiates a company's goods or services. It provides legal protection against unauthorized use and helps in brand recognition.

Essential Elements of a Trademark

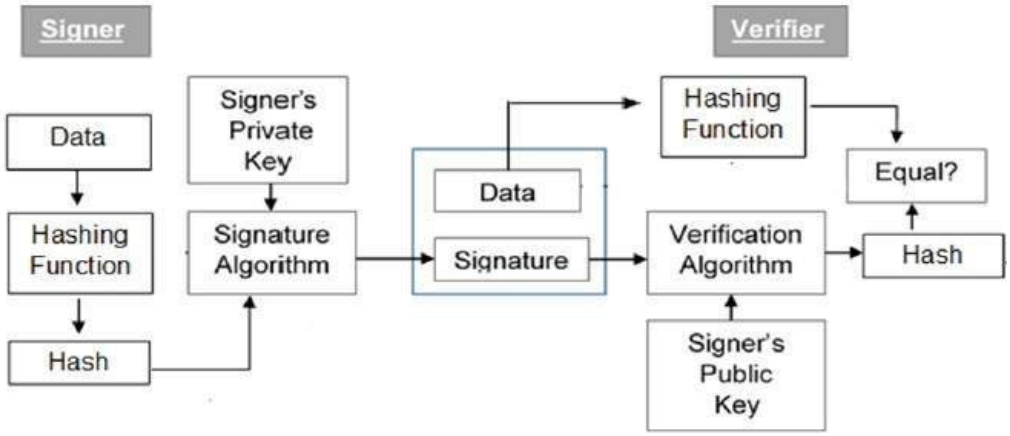
1. ***Distinctiveness*** – Must be unique to distinguish products/services.
2. ***Graphical Representation*** – Must be visually represented (e.g., logos, words, shapes, colors).
3. ***Non-Deceptiveness*** – Should not mislead consumers about goods/services.
4. ***Legality*** – Must not violate public order, morality, or existing trademarks.
5. ***Continuity of Use*** – Should be actively used to maintain trademark rights.
6. ***Registration*** – Not always mandatory, but provides stronger legal protection.

Functions of a Trademark

1. ***Brand Identification*** – Helps consumers recognize and differentiate products.
2. ***Consumer Protection*** – Prevents confusion and deception in the market.
3. ***Legal Protection*** – Grants exclusive rights and prevents infringement.
4. ***Market Value & Reputation*** – Enhances credibility and goodwill.
5. ***Business Growth*** – Aids in marketing, advertising, and expansion.
6. ***Global Recognition*** – Can be registered internationally for broader protection.

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

Solution:



Digital Signature

A digital signature is an electronic equivalent of a handwritten signature that ensures the authenticity, integrity, and non-repudiation of a digital document or message. It uses cryptographic algorithms (e.g., RSA, DSA, ECC) to generate a unique signature.

Digital Signature (Based on Diagram):

- The Signer hashes the data using a Hashing Function.
- The hash is encrypted with the Signer's Private Key using a Signature Algorithm to create a Digital Signature.
- The Data and Signature are sent to the Verifier.
- The Verifier hashes the received data and uses the Signer's Public Key to decrypt the signature.
- If both hashes match, the data is verified as authentic.

Digital Certificate

- A Digital Certificate verifies the authenticity of the Signer's Public Key.
- Issued by a trusted Certificate Authority (CA), it ensures the public key truly belongs to the claimed entity.

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

Solution:

How Digital Signatures Authenticate and Protect Documents

A digital signature ensures authentication, integrity, and non-repudiation.

1. ***Authentication:*** Verifies the sender's identity using their private key.
2. ***Integrity:*** Detects any changes by comparing the document's hash with the decrypted hash from the signature.
3. ***Non-repudiation:*** Prevents the sender from denying their authorship.

Example: Alice sends a contract to Bob.

- Alice hashes the document and encrypts it with her private key, creating a digital signature.
- Bob decrypts the signature using Alice's public key and compares the hash with his own computed hash.
- If they match, the document is verified as authentic and unchanged.

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

Solution:

Copyright

A copyright is a legal protection given to creators of original literary, artistic, musical, and digital works. It grants the creator exclusive rights to reproduce, distribute, or modify the work for a specific period (usually the creator's lifetime + 50-70 years).

Examples: Books, films, songs, paintings, software, articles.

Patent

A patent is an exclusive right granted to inventors for a new and useful invention. It prevents others from making, using, or selling the invention without permission for a fixed period (usually 20 years).

Examples: New drug formulas, electronic devices, industrial processes.

Copyright vs Patent

Feature	***Copyright***	***Patent***
Protects	Creative and artistic works	Inventions and technical solutions
Examples	Books, movies, music, software	Machines, medicines, processes
Rights Granted	Reproduction, distribution, adaptation	Exclusive manufacturing, selling, and licensing rights
Duration	Lifetime of author + 50-70 years	20 years from the filing date
Registration	Automatic upon creation (optional registration)	Must be filed and approved by a patent office
Purpose	Encourages creativity and cultural development	Promotes technological innovation and economic growth
Governing Laws	Copyright Act, Berne Convention	Patent Act, TRIPS Agr

28. Write short notes on WIPO Treaty.

Solution:

Short Notes on WIPO Treaty

The World Intellectual Property Organization (WIPO) Treaties are international agreements that govern intellectual property (IP) rights worldwide, ensuring protection for creators, inventors, and businesses. WIPO administers several key treaties, including:

1. WIPO Copyright Treaty (WCT) – 1996

- Protects literary, artistic, and digital works in the digital era.
- Extends copyright protection to computer programs and databases.
- Prevents unauthorized online reproduction and distribution.

2. WIPO Performances and Phonograms Treaty (WPPT) – 1996

- Grants rights to performers (singers, actors, musicians) and producers of sound recordings.
- Protects against unauthorized recording, copying, and online distribution.
- Recognizes moral rights for performers over their work.

3. Patent Cooperation Treaty (PCT) – 1970

- Simplifies the international patent application process.
- Allows inventors to file a single patent application for multiple countries.

4. Madrid Agreement & Protocol – 1891 & 1989

- Facilitates international trademark registration.
- Enables one trademark application to be valid in multiple countries.

5. Berne Convention – 1886

- Standardizes copyright protection across member countries.
- Ensures automatic copyright protection without formal registration.

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

Solution:

Cyber Fraud

Cyber fraud refers to fraudulent activities conducted using digital means (internet, computers, or mobile devices) to deceive individuals or businesses for financial gain or personal data theft.

Examples of Cyber Fraud

- ***Phishing*** – Fake emails/websites tricking users into sharing sensitive data.
- ***Online Banking Fraud*** – Unauthorized fund transfers and account breaches.
- ***Identity Theft*** – Illegally using someone's personal information.
- ***E-Commerce Scams*** – Fake websites selling non-existent products.

Hackers and Crackers

Feature	***Hackers***	***Crackers***
Definition	Skilled individuals who explore systems for security testing or knowledge.	Malicious individuals who break into systems illegally.
Intent	Can be ethical (**White Hat**) or unethical (**Black Hat**).	Always unethical, causing harm.
Purpose	Improve security, find vulnerabilities, or	Steal data, disrupt systems, or commit

	gain knowledge.	cybercrimes.
Methods Used	Penetration testing, security auditing, ethical hacking.	Malware, viruses, ransomware, brute force attacks.
Examples	Ethical hackers working for cybersecurity firms.	Cybercriminals hacking banking systems for fraud.

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

Solution:

Computer Software as Intellectual Property

Computer software is classified as intellectual property (IP) because it involves innovation, coding, and technical expertise. It includes programs, applications, operating systems, and source codes. Since software can be easily copied or misused, strong legal protection is essential.

Protection Methods for Computer Software

1. ***Copyright Protection***
    - Protects the source code, object code, and documentation.
    - Grants exclusive rights to reproduce, distribute, and modify the software.
    - ***Example:*** Windows OS, Adobe Photoshop.
2. ***Patent Protection***
    - Safeguards software-based inventions, such as unique algorithms or processes.
    - Requires the software to be novel, non-obvious, and useful.
    - ***Example:*** Google's PageRank algorithm.
3. **Trade Secret Protection**
    - Protects confidential software codes, formulas, and algorithms.
    - No formal registration is required; protection lasts as long as secrecy is maintained.
    - ***Example:*** Google's search algorithm.
4. ***Trademark Protection***
    - Secures software brand names, logos, and slogans.
    - Prevents unauthorized use of software branding.
    - ***Example:*** Microsoft, Oracle, Android trademarks.
5. ***Licensing Agreements***
    - Allows software creators to grant legal usage rights to users.
    - ***Types of Licenses:***
        - ***Proprietary Software:*** Requires purchase or subscription (e.g., Windows OS).
        - ***Open-Source Software:*** Free to use and modify (e.g., Linux).

31. Explain protection of copyrights in digital media.

Solution:

Protection of Copyrights in Digital Media

Copyright protection in digital media ensures that original digital content (e.g., music, videos, e-books, software, and online articles) is safeguarded from unauthorized use, copying, and distribution.

Methods of Copyright Protection in Digital Media

1. ***Digital Rights Management (DRM)***
    - Uses encryption to restrict unauthorized copying and distribution.
    - Example: Netflix and Spotify use DRM to prevent illegal downloads.
2. ***Watermarking and Digital Fingerprinting***
    - Embeds hidden identifiers in digital content to track ownership.
    - Example: Getty Images applies watermarks on licensed images.
3. ***Copyright Notices and Licensing***
    - Clearly states ownership and terms of use.
    - Example: Creative Commons (CC) licenses allow controlled sharing.
4. ***Anti-Piracy Laws & Enforcement***
    - DMCA (Digital Millennium Copyright Act) in the US and WIPO Copyright Treaty provide legal protection.
    - Legal actions against illegal streaming, piracy, and file sharing (e.g., crackdown on torrent websites).
5. ***Secure Distribution Platforms***
    - Content is distributed through authorized platforms to prevent piracy.
    - Examples: YouTube, Apple Music, Amazon Kindle.
6. ***Blockchain Technology***
    - Uses immutable digital ledgers to verify copyright ownership and track digital transactions.

32. Explain patent protection.

Solution:

Patent Protection

Patent protection grants inventors exclusive rights to a new product, process, or innovation for 20 years, preventing unauthorized use, making, or selling.

Key Requirements

1. ***Novelty:*** Must be new and undisclosed globally.
2. ***Inventive Step:*** Must offer a non-obvious improvement.
3. ***Industrial Applicability:*** Must be usable in industry, medicine, or technology.
4. ***Detailed Disclosure:*** Requires a clear technical description.

Patent Rights

- ***Exclusive Rights:*** Sole authority to use, sell, or license.
- ***Infringement Protection:*** Legal action against unauthorized use.
- ***Licensing:*** Allows earning through royalties.
- ***Territorial Nature:*** Valid only in granted jurisdictions (e.g., through PCT).

Patent Process

1. ***Search:*** Verify novelty.
2. ***Filing:*** Submit to a patent office (e.g., USPTO, EPO).
3. ***Examination:*** Reviewed for compliance.
4. ***Granting:*** Exclusive rights awarded if approved.

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

Solution:

Protection of semiconductor chips (ICs) is crucial for several reasons:

1. ***High R&D Investment****:* Developing IC designs requires substantial financial and intellectual effort.
2. ***Prevention of Piracy****:* Protection prevents illegal replication and exploitation of designs.
3. ***Encouraging Innovation****:* Legal safeguards encourage further innovation in the semiconductor industry.
4. ***Economic & National Security****:* Protecting ICs secures critical infrastructure and supply chains.

The Semiconductor IC Layout-Design Act ensures:

- ***Protection Scope****:* Covers original IC designs from unauthorized use.
- ***Registration****:* IC layout designs must be registered for protection.
- ***Exclusive Rights****:* Creators have exclusive rights to manufacture, sell, or license designs.
- ***Duration****:* Protection lasts for 10 years from the first use or registration.
- ***Infringement Penalties****:* Unauthorized use leads to legal consequences like fines or bans.

34. What are the duties of the subscriber of digital signature certificate.

Solution:

Duties of a Digital Signature Certificate (DSC) Subscriber

A DSC subscriber is an individual or entity issued a certificate by a Certifying Authority (CA) for secure electronic authentication. Key duties include:

1. ***Protect Private Key:*** Secure it and report any compromise to the CA.
2. ***Authorized Use:*** Use the digital signature only for legitimate transactions.
3. ***Accurate Information:*** Provide truthful details for DSC issuance.
4. ***Update Changes:*** Inform the CA of any changes in personal or organizational details.
5. ***No Unauthorized Disclosure:*** Keep the private key confidential.
6. ***Request Revocation:*** Revoke the DSC immediately if the key is lost or compromised.

35. What is Cyber stalking? As per your understanding is it a crime under the Digital Security Act 2023?

Solution:

Cyber Stalking involves the repeated use of digital communication tools to harass or intimidate someone, including:

- Sending threatening or obscene messages
- Spreading false information
- Monitoring someone's online activities without consent
- Using fake identities to harass or blackmail
- Posting private information (doxxing) to cause harm

Cyber Stalking under the Digital Security Act 2023 (Bangladesh)

Yes, it is a punishable offense under the ***Digital Security Act (DSA) 2023*** of Bangladesh. Relevant sections include:

- ***Section 25****:* Publication of false or offensive information.
- ***Section 29****:* Defamation in digital media.
- ***Section 31****:* Cyber terrorism and threats.
- ***Section 32****:* Breach of privacy.

Punishment for cyberstalking under the DSA 2023 can include fines, imprisonment, or both, depending on the severity of the offense.

36. Explain Cyber terrorism and provision under the Digital Security Act 2023.

Solution:

Cyber Terrorism refers to using digital technology and the internet to carry out terrorist activities, such as:

- Hacking into government or military networks
- Spreading extremist propaganda or recruiting terrorists online
- Disrupting critical infrastructure (e.g., power grids, banking systems)
- Launching cyberattacks on national security systems
- Using ransomware or malware to threaten national security

Cyber Terrorism under the Digital Security Act 2023 (Bangladesh)

The ***Digital Security Act 2023*** criminalizes cyber terrorism with severe penalties:

- ***Section 31****:* Cyber terrorism & digital threats (threats to national security, religious hatred, or terrorism). *Punishment is* up to 10 years imprisonment, fine up to Tk. 25 lakh, or both.
- ***Section 17****:* Unauthorized access to critical information infrastructure (CII). Punishment is up to 14 years imprisonment, fine up to Tk. 1 crore, or both.
- ***Section 21****:* Online extremism & propaganda (spreading extremist content, radicalizing, or recruiting terrorists). Punishment is up to life imprisonment, fine up to Tk. 3 crore.