Question Paper Solution

Date of Examination: 30-11-2023

Session: July-December 2024

Section A

Ans1

a) E-commerce or electronic commerce refers to the buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the internet. E-commerce provides consumers with more choices and improved services, such as the ability to shop from home 24/7 and find deals more easily through price comparisons. It provides businesses access to new markets and customers globally.

b) Cyber security refers to the techniques used to protect computers, networks, programs, and data from unauthorized access or attacks that are aimed for exploitation. It protects against threats like data breaches, cyber attacks, viruses, malware etc. Effective cyber security reduces the risk of cyber attacks and protects organizations and individuals from threats that can cause financial losses, theft of personal information, and damage to reputation.

c) Ransomware is a type of malicious software that blocks access to a computer system or data by encrypting the files or locking the system. It then demands that a ransom be paid to get access restored Once installed, ransomware uses encryption to lock valuable data and asks for cryptocurrency to decrypt it. Failure to pay the ransom could result in the data being lost forever. Ransomware often spreads through phishing emails or compromised websites.

d) A computer virus is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions. It can corrupt, delete data, or download more viruses. Vinuses often spread through email attachments, infected programs, infected storage devices etc. Anti-virus software should be used to prevent, detect and remove viruses.

e) A certifying authority in cryptography and network security is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others to rely upon signatures or assertions made by the private key that corresponds to the certified public key. Certifying authorities validate identity and issue certificates to provide authentication for secure communication over the internet.

f) The labor theory of value states that the economic value of a good or service is determined by the total amount of labor required to produce it. According to this theory, the more labor that goes into producing something, the more it is worth. This theory was developed by classical economists like Adam Smith and David Ricardo and later became central to Marxian economics. It argues that labor is the fundamental unit of production and establishes the link between labor and value.

g) Copyright grants the creator of an original work exclusive rights to its use and distribution for a certain time period. The copyright holder has the right to reproduce, print, publish, translate, distribute copies of the work etc. Copyright provides an incentive for creators to produce original works and protects the creator's intellectual property from unauthorized use by others. It is a form of intellectual property that covers literary works, films, music, artistic works, and other creative works.

h) Privacy refers to the ability of an individual or group to keep their personal information, matters, relationships, opinions etc. private and thereby reveal them selectively. It involves the right to protect one's personal identifiable data from being freely distributed or accessed. Privacy enables one to limit who can access their personal information and protects against misuse or exploitation of such data. It is a fundamental human right that fosters human dignity.

i) A patent is a form of intellectual property that gives its holder the legal right to exclude others from making, using or selling an invention for a limited period of years in exchange for publishing an enabling public disclosure of the invention. It protects inventions that are novel, non-obvious and useful. Patents provide incentives to invent, invest in R&D and publicly disclose technical information about the invention that can lead to further innovation.

Section B

Ans 2 Indian Law Enforcement Agencies for Cyber Crimes:

- CBI - Central Bureau of Investigation has a specialized Cyber Crime Investigation Cell that handles major cyber crimes.
- State Police - All states have a Cyber Crime cell under the state police departments like Mumbai Police Cyber Cell, Delhi Police Cyber Cell etc. They investigate cyber crimes within their jurisdiction.
- Cyber Crime Cells - Many cities have dedicated Cyber Crime cells under the city police commissioner to tackle computer related crimes. Eg. Bengaluru Cyber Crime Cell.
- Indian Cyber Crime Coordination Centre - Set up under MHA to coordinate between various agencies, provide technical assistance, research etc. on cyber crimes.
- CERT-In - Indian Computer Emergency Response Team handles cyber attacks, vulnerability assessment, and advises on security compliance.
- NCIIPC - National Critical Information Infrastructure Protection Centre works for security of critical information infrastructure in India.

Ans 3 Infringement of Copyright:

- Copyright infringement means using the copyright-protected material without permission of the copyright holder.
- Direct infringement involves directly copying or reproducing the original work without authorization. This could mean copying books, artwork, photographs, articles etc. completely or partly.
- Indirect infringement does not directly copy but facilitates others to copy a work. Examples are providing technology designed for circumventing copyright measures, inducing others to infringe copyright etc.
- Downloading, sharing, distributing copyrighted material through file sharing sites or P2P networks without permission is also infringement.
- Types of infringement include plagiarism, unauthorized file sharing, reproducing artworks, photocopying books, reproducing trademarks etc. beyond fair use.
- Remedies for copyright infringement include injunctions, damages, account of profits, criminal proceedings etc. Enforcement is done through civil litigation and criminal prosecution.

Ans 4 Grey Areas in Information Technology Act 2000:

- Intermediary Liability - Ambiguity in regulations for liabilities of intermediaries like social media platforms regarding third party content.
- Data Protection - Comprehensive data protection legislation still needs to be enacted to strengthen privacy. Current provisions are inadequate.
- Content Regulation - Clear regulations needed for issues like censorship, freedom of speech vs. public order, defamation etc. on online platforms.
- Data Localization - Requirements of storing data locally in India affect cross-border data flows. Issues exist regarding its security and economic impact.
- Intellectual Property - Clarity required on protection, fair use, anti-circumvention measures, ISP liability regarding online IP violations.
- Reasonable Security Practices - Ambiguity in assessing compliance with reasonable security practices by body corporates as required under Sec 43A.
- Cyber Warfare - Unclear policy for cyber warfare, military cyber operations, countermeasures against state sponsored cyber-attacks.

Ans 5 Types of Malware Attacks:

- Viruses - Malicious code that replicates by infecting other programs. Can corrupt, delete data, slow devices. Spread through downloads, email attachments etc.
- Worms - Self-replicating programs that spread across networks without human interaction. Spread through security holes in software.
- Trojans - Malicious programs disguised as legitimate software. Allows unauthorized remote access to devices.
- Spyware - Secretly monitors activity on devices and sends information to external parties.
- Adware - Software that automatically displays unwanted advertisements to users often installed via freeware or shareware programs.

- Ransomware - Restricts access to system until ransom is paid. Spreads via downloads, attachments. Encrypts files.
- Bots - Automated programs that run command over the internet. Can be used for malicious activities.
- Rootkits - Grant administrator access to malware/unauthorized users to take control of systems undetected.
- Keyloggers - Record keystrokes input on keyboard to gain sensitive passwords, credentials.
- Scareware - Deceives users into purchasing unnecessary software such as fake antivirus protection.

Section C

Ans 6 Explanation of Section 66 of Information Technology Act 2000:

Section 66 deals with various computer related offenses such as hacking, unauthorized access, data theft, virus attacks, damage to computer systems etc. Key provisions are:

- Sec 66A - Punishment for sending offensive or false information with intention to harass, cause injury, deceive receiver or misrepresent facts.
- Sec 66B - Punishment for dishonestly receiving stolen computer resource or communication device.
- Sec 66C - Punishment for identity theft by fraudulently using electronic signature, password or other unique identification of another person.
- Sec 66D - Punishment for cheating by personation using computer resource ie, by pretending to be someone else.
- Sec 66E - Punishment for privacy violation by capturing, publishing or transmitting images of private area of any person without consent.
- Sec 66F - Punishment for cyberterrorism to threaten national security or cause damage to computer systems.
- Imprisonment up to 3 years with or without fine as punishment. More severe in cases of sensitive personal data, critical infrastructure etc.

Ans 7 Difference between Direct and Indirect Copyright Infringement:

- Direct Infringement involves directly violating the exclusive rights granted to the copyright owner without permission. This could mean directly copying, reproducing, distributing, displaying, performing the protected work in whole or substantial part.
- Indirect Infringement does not directly violate the exclusive rights but facilitates or induces others to infringe. Enabling others to make unauthorized copies, sale of devices designed for circumventing copyright access control etc fall under this.
- Downloading a copyrighted music album from an unauthorized source is direct infringement. Running a website that enables users to download such copyrighted content for free would be indirect infringement.

- To prove direct infringement, substantial similarity between original and copy needs to be shown. No proof of intent is required. For indirect infringement, intent and knowledge should be demonstrated.
- Direct infringement has higher risks with stricter punishments. Indirect infringement has more complicated criteria and defense possibilities like fair use, safe harbor provisions etc.

Ans 8 Denial of Service (DoS) Attacks:

- DoS attacks aim to make a computer or network resource unavailable to its intended users by disrupting services. This is done by overloading target machine with superfluous requests and overtaxing the server resources.
- Methods include flooding target with excessive traffic, overloading connection bandwidth, overloading computational resources, exploiting system vulnerability to crash services etc. Perpetrators use botnets, malware, multiple computers to launch attack.
- Distributed DoS or DDoS attacks are more severe where multiple compromised devices coordinate to target victim simultaneously. Attack traffic can come from millions of IP sources across globe.
- Effects include server overload & crash, network saturation, disruption of services like email, websites etc, impacts user access to resources, revenue loss for businesses, reputation damage.
- Protection involves maintaining adequate bandwidth, load balancing, filtering traffic, anti-DDoS software, coordinating with ISPs to block traffic. Cyber security measures like zoneAlarm firewall, intrusion detection systems also help mitigate risks.