Course Code	**:**	**MCS-215**
Course Title	**:**	**Security and Cyber Laws**
Assignment Number	**:**	**MCAOL(I)/215/Assign/2025**
Maximum Marks	**:**	**100**
Weightage	**:**	**30%**
Last date of Submission	**:**	**30th April 2025 (for January session)** **31st October 2025 (for July session)**

This assignment has six questions. Answer all questions. The remaining 20 marks are for viva voce. You may use illustrations and diagrams to enhance the explanations. Please go through the guidelines regarding assignments given in the Programme Guide for the format of the presentation.

Q1: **(3*4= 12 Marks)**

(a) Explain the terms Confidentiality, Integrity and Availability in digital security. Explain the Pros and Cons of digital security.

(b) Explain the following in the context of security issues/attacks:
- (i) Unauthorised access
- (ii) Social Engineering Attacks
- (iii) Internet of Things (IoT) attacks

(c) Explain (any three) ways technology can help you to counter different types of cyber security attacks.

(d) What are the laws related to Distributed Denial of Service Attacks and Crypto-jacking?

Q2: Explain the following terms with the help of an example of each. **(3*6=18 Marks)**

(a) Transposition Ciphers
(b) Advantages and Disadvantages of Symmetric Key Cryptography
(c) Steganography
(d) Data Encryption Standard (DES)
(e) Hash functions
(f) Key Establishment, Management and Certification in the context of cryptography

Q3: **(3*4= 12 Marks)**

(a) What are the practices for implementing the CIA triad in data security? Explain.

(b) Explain the following:
- **(i)** Ransomware attacks
- **(ii)** Cyber-physical attacks

(c) Explain the following data security measures:
- **(i)** Email Security
- **(ii)** Risk-Assessment Analysis

(d) What is a Security audit? Explain with the help of an example. What are the different trade-offs between security and usability?

Q4: **(3*4= 12 Marks)**

(a) How can cyberspace be regulated? Explain.
(b) What are the different approaches of regulating Internet content? Explain.
(c) What are the doctrines and Articles of UNCITRAL model law? Explain.
(d) What are the regulations for cyberspace content in India? Explain

Q5: **(3*5= 15 Marks)**

(a) How is cybercrime defined? Explain the classification of cybercrimes with the help of examples.
(b) List the Penalties and compensation in Section 44 of the Information Technology Act 2000.
(c) List any six offences under sections 65 and 66 as per the Information Technology Act, 2000.

(d) What are the grounds which exempt the network service providers from liability? Explain.
(e) What are the different cyber forensic investigation tools? Explain

Q6: **(6+3+2= 11 Marks)**

(a) Explain the following forms of IPR with the help of an example of each:
(i) Copyrights and related rights.
(ii) Trade Secrets
(iii) Geographical Indication
(b) Explain cyber-squatting and abuse of search engines with the help of an example of each.
(c) What remedies are available against infringement of IPR?

MCS-215

SOLVED ASSIGNMENT 2025

Q.1 -

(a)- Explain the terms Confidentiality, Integrity and Availability in digital security. Explain the Pros and Cons of digital security

ANS.- **Confidentiality, Integrity, and Availability in Digital Security:**

- **Confidentiality** ensures that sensitive information is accessible only to authorized users, preventing data breaches.
- **Integrity** ensures that data remains accurate, consistent, and unaltered by unauthorized users.
- **Availability** ensures that data and services are accessible when needed, minimizing downtime.

Pros of Digital Security:

- Protects personal and financial data
- Prevents cyber threats like hacking and malware
- Ensures compliance with legal regulations

Cons of Digital Security:

- Can be expensive to implement
- May slow down system performance
- Requires constant updates and monitoring

(b)- Explain the following in the context of security issues/attacks:

(i) Unauthorised access

(ii) Social Engineering Attacks

(iii)Internet of Things (IoT) attacks

ANS.- (i) **Unauthorized Access**: This occurs when an individual gains access to a system, network, or data without permission. It can result from weak passwords, system vulnerabilities, or hacking techniques like brute force attacks. Unauthorized access can lead to data breaches, financial loss, or identity theft.
(ii) **Social Engineering Attacks**: These attacks manipulate individuals into revealing confidential information. Common methods include phishing, pretexting, and baiting. Attackers exploit human psychology rather than technical vulnerabilities to gain unauthorized access.
(iii) **Internet of Things (IoT) Attacks**: IoT devices are often vulnerable due to weak security measures. Cybercriminals exploit these vulnerabilities to launch attacks like botnets (e.g., Mirai), data breaches, or device takeovers.

(c)- Explain (any three) ways technology can help you to counter different types of cyber security attacks

ANS.- Here are three ways technology can help counter cybersecurity attacks:

1. **Firewalls and Intrusion Detection Systems (IDS)** – Firewalls filter incoming and outgoing traffic to block malicious access, while IDS monitors network activity to detect suspicious behavior.
2. **Multi-Factor Authentication (MFA)** – By requiring multiple verification steps (e.g., password and OTP), MFA prevents unauthorized access even if login credentials are compromised.
3. **Encryption** – Data encryption ensures that sensitive information remains secure by converting it into unreadable formats, making it useless to hackers even if intercepted.

These technologies strengthen cybersecurity and protect against cyber threats.

(d)- What are the laws related to Distributed Denial of Service Attacks and Crypto-jacking?

ANS.- Laws against **Distributed Denial of Service (DDoS) attacks** and **crypto-jacking** vary across jurisdictions but generally fall under cybersecurity and anti-hacking statutes.

- **DDoS Attacks:** In the U.S., the **Computer Fraud and Abuse Act (CFAA)** criminalizes DDoS attacks. The **UK's Computer Misuse Act (CMA) 1990** also penalizes unauthorized access and service disruption. Similar laws exist in the **EU's Cybercrime Directive** and **India's IT Act, 2000**.
- **Crypto-jacking:** This is illegal under laws prohibiting unauthorized computer access, such as the **CFAA (U.S.)**, **CMA (UK)**, and **EU GDPR (if personal data is compromised)**. Many countries classify it as cyber fraud or unauthorized resource exploitation.

Q.2 - Explain the following terms with the help of an example of each.

(a)- Transposition Ciphers

ANS.- A transposition cipher rearranges the letters of a plaintext message according to a specific pattern to create ciphertext. It does not alter the characters but changes their positions. One common type is the **Rail Fence Cipher**, where letters are written in a zigzag pattern and read row by row.

Example:

Plaintext: **HELLO WORLD**

Rail Fence (2 rows):

H L O W R D

E L L O O

Ciphertext: **HLOWRDELLOO**

(b)- Advantages and Disadvantages of Symmetric Key Cryptography

ANS.- **Advantages and Disadvantages of Symmetric Key Cryptography**

Advantages:

- **Fast Encryption & Decryption:** Since only one key is used, encryption is computationally efficient.
- **Less Resource-Intensive:** Requires lower processing power compared to asymmetric encryption.

Disadvantages:

- **Key Distribution Problem:** Securely sharing the key between parties is challenging.
- **Scalability Issues:** For large networks, managing keys becomes complex.

Example: AES (Advanced Encryption Standard) is a widely used symmetric encryption algorithm.

(c)- Steganography

ANS.- Steganography is the practice of hiding messages within other non-secret data, such as images, audio, or videos, to avoid detection. Unlike encryption, which scrambles a message, steganography conceals its existence.

Example:

A hidden message is embedded in an image file by altering the least significant bits (LSB) of pixel values, making the change imperceptible.

Use case: A spy hides a secret text message within an innocent-looking image to bypass surveillance.

(d)- Data Encryption Standard (DES)

ANS.- DES is a symmetric-key encryption algorithm developed by IBM in the 1970s. It encrypts data in **64-bit blocks** using a **56-bit key** through **16 rounds of processing** involving permutation and substitution.

Example:
If a message **"HELLO"** is encrypted with DES, it converts into unreadable ciphertext, ensuring secure transmission.
Limitation: Due to its small key size, DES is vulnerable to brute-force attacks, leading to its replacement by AES.

(e)- Hash functions

ANS.- A hash function takes an input (message) and produces a fixed-length output (hash) that uniquely represents the original data. Hash functions are **one-way** and used for integrity verification.
Example:
SHA-256 produces a 256-bit hash:
Input: **"Hello"** → SHA-256 Hash: **2cf24dba5fb0a...**
Use case: Password storage—websites store hashes of passwords instead of plaintext passwords.

(f)- Key Establishment, Management and Certification in the context of cryptography

ANS.- **Key Establishment:** The process of securely generating and exchanging cryptographic keys between parties.
Key Management: Storing, updating, distributing, and revoking cryptographic keys to maintain security.
Key Certification: Using a **Certificate Authority (CA)** to verify the legitimacy of public keys in asymmetric encryption.
Example:
SSL/TLS certificates issued by CAs ensure that a website's public key is authentic, allowing secure HTTPS communication.

Q.3 -

(a)- What are the practices for implementing the CIA triad in data security? Explain.

ANS.- The **CIA triad**—**Confidentiality, Integrity, and Availability**—is fundamental in data security.

1. **Confidentiality**: Protect sensitive data using encryption, access controls, multi-factor authentication (MFA), and strict user permissions.
2. **Integrity**: Ensure data accuracy with hashing, digital signatures, checksums, and version control to prevent unauthorized alterations.
3. **Availability**: Maintain system uptime through regular backups, disaster recovery plans, redundancy, and DDoS protection.

By implementing these practices, organizations safeguard data from unauthorized access, corruption, and downtime, ensuring a secure and reliable information system.

(b)- Explain the following:

(i) Ransomware attacks

(ii) Cyber-physical attacks

ANS.- (i) **Ransomware Attacks**: These are malicious cyberattacks where hackers encrypt a victim's data and demand a ransom for its release. Attackers often spread ransomware through phishing emails or security vulnerabilities. Notable examples include WannaCry and REvil.

(ii) **Cyber-Physical Attacks**: These attacks target systems that integrate digital and physical components, such as power grids, industrial control systems, or smart infrastructure. Hackers exploit vulnerabilities to cause real-world disruptions, like shutting down power stations or tampering with critical machinery. Stuxnet, which targeted Iranian nuclear facilities, is a well-known example.

(c)- Explain the following data security measures:

(i) Email Security

(ii) Risk-Assessment Analysis

ANS.- (i) **Email Security**: Email security involves measures to protect email accounts, communication, and content from cyber threats like phishing, spam, malware, and unauthorized access. Techniques include encryption, multi-factor authentication (MFA), spam filters, and secure email gateways to prevent data breaches.

(ii) **Risk-Assessment Analysis**: Risk-assessment analysis identifies and evaluates potential security threats to an organization’s data. It involves assessing vulnerabilities, determining the likelihood of threats, and implementing mitigation strategies. This proactive approach helps in minimizing security risks, ensuring compliance with regulations, and enhancing overall cybersecurity resilience.

(d)- What is a Security audit? Explain with the help of an example. What are the different trade-offs between security and usability

ANS.- A **security audit** is a systematic evaluation of an organization's information systems to assess security measures, identify vulnerabilities, and ensure compliance with security policies and regulations. It involves reviewing access controls, data protection mechanisms, and network security.

Example: A bank may conduct a security audit to check if customer data is adequately encrypted and protected from cyber threats.

Trade-offs between security and usability:

- **Strong security** (e.g., multi-factor authentication) can make systems less convenient for users.

- **Easy access** (e.g., single sign-on) may reduce security by increasing vulnerability to breaches. Balancing both is crucial.

Q.4 -

(a)- How can cyberspace be regulated? Explain.

ANS.- Cyberspace can be regulated through a combination of legal, technical, and institutional measures. Governments enforce cybersecurity laws, such as the GDPR and IT Act, to protect data and prevent cybercrimes. International cooperation helps combat cyber threats across borders. Technical measures, including encryption and firewalls, enhance security. Organizations implement policies like user authentication and monitoring to regulate online activities. Ethical self-regulation by internet users and tech companies also plays a role. However, balancing regulation with digital freedom remains a challenge, requiring continuous updates to policies and collaboration between stakeholders to ensure a safe and open cyberspace.

(b)- What are the different approaches of regulating Internet content? Explain.

ANS.- There are several approaches to regulating Internet content, including **government regulation**, where authorities impose laws on harmful or illegal content, such as hate speech or piracy. **Self-regulation** involves platforms enforcing their own guidelines and moderation policies. **Co-regulation** combines government oversight with industry self-regulation. **Technical regulation** uses filters, firewalls, and AI moderation to control content access. **User empowerment** allows individuals to use parental controls and content filters. While government control ensures legal compliance, self-regulation fosters flexibility. A balanced approach is necessary to uphold free speech while preventing harm, ensuring a safe and open digital space.

(c)- What are the doctrines and Articles of UNCITRAL model law? Explain.

ANS.- The **UNCITRAL Model Law on International Commercial Arbitration** provides a framework to harmonize arbitration laws worldwide. Key **doctrines** include **party autonomy**, **kompetenz-kompetenz** (tribunal's power to rule on its jurisdiction), **severability** (arbitration clause remains valid even if the contract is void), and **minimal judicial intervention**.

Important **Articles** cover aspects like arbitration agreements (Art. 7), tribunal composition (Art. 10-15), arbitral proceedings (Art. 18-27), awards (Art. 28-33), and enforcement (Art. 35-36). The law ensures **fair, efficient, and enforceable** arbitration while aligning with the **New York Convention (1958)** for cross-border recognition of awards.

(d)- What are the regulations for cyberspace content in India? Explain

ANS.- In India, cyberspace content is regulated primarily under the **Information Technology (IT) Act, 2000**, along with rules and guidelines issued by various authorities. The **IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021** impose obligations on digital platforms to monitor and remove unlawful content. The **Indian Penal Code (IPC)** and laws like the **Copyright Act, 1957** and **Personal Data Protection Bill** also govern online content. The government can block websites under **Section 69A of the IT Act** for national security. Additionally, social media platforms must appoint compliance officers to ensure adherence to Indian regulations.

Q.5 -

(a)- How is cybercrime defined? Explain the classification of cybercrimes with the help of examples.

ANS.- Cybercrime refers to illegal activities carried out using computers or digital networks. It includes offenses that target computer systems or use technology to commit crimes.

Classification of Cybercrimes:

1. **Cyber Fraud** – Online scams, phishing (e.g., fake emails stealing bank details).
2. **Hacking** – Unauthorized access to data (e.g., breaking into government databases).
3. **Identity Theft** – Stealing personal information (e.g., credit card fraud).
4. **Cyberbullying** – Harassing individuals online (e.g., social media threats).
5. **Cyber Terrorism** – Attacks on national security (e.g., hacking critical infrastructure).

Cybercrime laws aim to prevent and penalize such offenses.

(b)- List the Penalties and compensation in Section 44 of the Information Technology Act 2000.

ANS.- Section 44 of the **Information Technology Act, 2000** specifies penalties for failing to furnish required information to authorities. The penalties are:

1. **Failure to furnish required information** – Fine up to **Rs.1,50,000**.
2. **Failure to maintain prescribed books, accounts, or records** – Fine up to **Rs.5,000 per day** during the default period.
3. **Failure to submit returns or reports** – Fine up to **Rs.5,000 per day** during non-compliance.

These penalties aim to ensure compliance with IT regulations and data management obligations.

(c)- List any six offences under sections 65 and 66 as per the Information Technology Act, 2000.

ANS.- Under the **Information Technology Act, 2000**, Sections **65 and 66** deal with cyber offences. Here are six offences covered:

1. **Tampering with Computer Source Documents (Section 65)** – Knowingly altering, destroying, or concealing computer source code.
2. **Hacking (Section 66)** – Unauthorized access to a computer system, causing harm.
3. **Identity Theft (Section 66C)** – Fraudulently using another person's digital identity.
4. **Cheating by Personation (Section 66D)** – Impersonation using electronic communication.
5. **Publishing Obscene Material (Section 66E)** – Violation of privacy by sharing private images.
6. **Cyber Fraud (Section 66F)** – Committing cyber terrorism.

(d)- What are the grounds which exempt the network service providers from liability? Explain.

ANS.- Network service providers are exempt from liability under certain conditions, primarily outlined in the **Information Technology Act, 2000** (India) and similar laws worldwide. The key grounds for exemption include:

1. **Intermediary Status** – If they act as mere conduits, transmitting third-party information without modifying it.
2. **Lack of Knowledge** – They must not have actual knowledge of illegal content or should act promptly to remove it upon notice.
3. **Due Diligence Compliance** – Following prescribed guidelines and content moderation policies.

These exemptions protect service providers unless they actively participate in or facilitate unlawful activities.

(e)- What are the different cyber forensic investigation tools? Explain

ANS.- Cyber forensic investigation tools help experts analyze digital evidence, recover lost data, and track cybercrimes. Key tools include:

1. **Autopsy & Sleuth Kit** – Open-source tools for disk analysis and file recovery.
2. **EnCase** – A professional tool for in-depth forensic analysis.
3. **FTK (Forensic Toolkit)** – Used for data decryption and file recovery.
4. **Wireshark** – Captures and analyzes network traffic.
5. **Volatility** – Extracts data from memory for live forensic analysis.
6. **Oxygen Forensics** – Examines mobile device data.

These tools assist in investigating cybercrimes by analyzing devices, networks, and digital footprints.

Q.6 -

(a)- Explain the following forms of IPR with the help of an example of each:

(i) Copyrights and related rights.

(ii) Trade Secrets

(iii)Geographical Indication

ANS.- **Forms of Intellectual Property Rights (IPR)**

(i) Copyrights and Related Rights

Copyright protects original literary, artistic, musical, and dramatic works, along with software and films. It grants creators exclusive rights to reproduce, distribute, and perform their work. Related rights apply to performers, producers, and broadcasters.

Example: A novelist writes a book and holds the copyright, preventing unauthorized reproduction. Similarly, a singer has related rights over their recorded performances.

(ii) Trade Secrets

Trade secrets refer to confidential business information that provides a competitive edge. They are protected through non-disclosure agreements rather than registration. This includes formulas, practices, and processes unknown to competitors.

Example: The recipe for Coca-Cola is a famous trade secret, kept undisclosed for over a century, maintaining its uniqueness in the market.

(iii) Geographical Indication (GI)

A Geographical Indication protects products that have a specific origin and possess qualities or a reputation due to that location. It prevents unauthorized use by producers outside the region.

Example: Darjeeling Tea has GI status, ensuring that only tea grown in the Darjeeling region of India can be marketed under this name, protecting its authenticity and heritage.

Each of these IPR forms plays a crucial role in safeguarding innovation, creativity, and economic value.

(b)- Explain cyber-squatting and abuse of search engines with the help of an example of each.

ANS.- **Cyber-squatting** refers to the practice of registering, selling, or using a domain name with the intent of profiting from someone else's trademark. For example, a person registers **"NikeShoesOnline.com"** without authorization and tries to sell it to Nike at an inflated price.

Abuse of search engines involves unethical techniques to manipulate search rankings, such as **keyword stuffing** or **cloaking**. For example, a website repeatedly inserts **irrelevant keywords** to appear in search results, misleading users. Another example is **cloaking**, where search engines see different content than users, boosting rankings fraudulently. Both practices violate ethical and legal norms.

(c)- What remedies are available against infringement of IPR?

ANS.- Remedies against the infringement of Intellectual Property Rights (IPR) include **civil, criminal, and administrative** actions:

1. **Injunctions** – Courts can issue temporary or permanent injunctions to stop further infringement.
2. **Damages or Account of Profits** – The infringer may be ordered to pay compensation or surrender profits gained.
3. **Delivery and Destruction of Infringing Goods** – Counterfeit goods may be seized and destroyed.
4. **Criminal Penalties** – Fines and imprisonment for severe infringements.
5. **Customs Remedies** – Authorities can seize imported counterfeit goods.

These measures protect IPR holders and deter violations.