INDIRAGANDHINATIONALOPENUNIVERSITY

Regional Centre Delhi-3

Format for Assignment Submission

For Term End Exam June/December- JUNE **(Year)** 2025

(Please read the instructions given below carefully before submitting assignments)

1. **Name of the Student** : Ashu Chaurasiya
2. **Enrollment Number** : 250132132 6
3. **Programme Code** : MCA_NEW
4. **Course Code** (Use this format course-wise separately) : ~~MCS-215~~ MCS-215
5. **Study Centre Code** : LSC-38046
6. **Name of the Study Centre With complete address** : RAJDHANI COLLEGE RAJA GARDEN NEW DELHI
7. **Mobile Number** : 8448713694
8. **E-mail ID** : Intermezzobrilliance@gmail.com
9. **Details if this same assignment has been submitted anywhere else also** : No
10. **Above information is cross checked and it is correct: Yes/No** ✓

Date of Submission: 01-06-25

Ashu

(Signature of the student)

A. Important Instructions:-

1. Please do not send any assignment at any email of the Regional Centre, it will not be considered.
2. Please avoid duplicacy. Do not re-submit the same assignment anywhere else or by any other means.
3. About the mode of submission of assignments, pl wait for instructions from IGNOU Hqtrs. As soon as we shall come to know, we will share it with all.
4. Please do not use plastic covers. Use plain A4 size pages for assignments for uniformity and better management with this cover page format on each assignment.
5. Please write your name and enrollment no. at the bottom of each page of your assignment.
6. Please retain a photocopy set of assignment submitted with you for record(may be asked to submit at later stage) and also keep the assignment submission receipt in safe custody.
7. If assignment awards are not updated in your Grade Card **within next 09 months**, please write to us at **rcdelhi3@ignou.ac.in** giving your complete details and attaching the proof of assignment submission.
8. Assignment Question Paper can be downloaded from: https://webservices.ignou.ac.in/assignments/

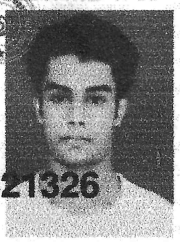
B. Compulsory sequence of the Assignment Set:

1. Duly Filled in Assignment Submission Cover Page (This Format Page).
2. Copy of IGNOU Identity Card.
3. Print out of valid/applicable assignment question paper.
4. Handwritten Assignment, written on both the sides of page (preferably plain A4 size).

ignou
THE PEOPLE'S
UNIVERSITY

इंदिरा गांधी राष्ट्रीय मुक्त विश्वविद्यालय
मैदान गढ़ी, नई दिल्ली - 110068
Indira Gandhi National Open University
Maidan Garhi,New Delhi - 110068

IGNOU - Student Identity Card



2501321326

Enrolment Number :	2501321326
RC Code :	38: DELHI 3 Naraina
Name of the Programme :	MCA_NEW : Master of Computer Applications
Name :	ASHU CHAURASIYA
Father's Name :	VIJAY
Address :	Flat No. 270,G, F Block-14, Pocket 13, Sector-20 RNORTH WEST
Pin Code :	110086

Instructions :
1. This card should be produced on demand at the Study Center, Examination Center or any other Establishment of IGNOU to use its facilities.
2. The facilities would be available only relating to the Programme/course for which the student is registered.
3. This ID Card is generated online. Students are advised to take a color print of this ID Card and get it laminated.
4. The student details can be cross checked with the QR Code at www.ignou.ac.in

Registrar
Student Registration Division

Course Code	:	**MCS-215**
Course Title	:	**Security and Cyber Laws**
Assignment Number	:	**MCA_NEW(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?

Enrollment No. 2501321326

Question no. Q): (a) Explain the terms Confidentiality, Integrity and Availability in digital security. Explain the Pros and Cons of digital security.

Answer: Confidentiality: Protecting information from unauthorized access.
Integrity: Ensuring information is accurate and has not been tampered with.
Availability: Guaranteeing authorized users can access information when needed.
Pros of digital security: Protects data, ensures privacy, maintains trust, enables secure transactions. Cons of digital security: Can be complex and costly to implement, may impact usability, requires constant updates, can be bypassed by sophisticated attacks.

Question no. Q): (b) Explain the following in the context of security issues/attacks: (i) Unauthorised access (ii) Social Engineering Attacks (iii) Internet of Things (IoT) attacks

Answer: (i) Unauthorised access: Gaining entry to a system or data without proper permissions (e.g., a hacker accessing a private database).
(ii) Social Engineering Attacks: Manipulating individuals to divulge confidential information or perform actions that compromise security (e.g., phishing emails).
(iii) Internet of Things (IoT) attacks: Exploiting vulnerabilities in connected devices (e.g., smart cameras, smart home devices) to gain control or access networks.

Question no. Q): (c) Explain (any three) ways technology can help you to counter different types of cyber security attacks.

Answer:

Firewalls: Act as a barriers between a trusted internal network and untrusted external networks, filtering traffic.

Encryption: Converts data into a coded format to prevent unauthorized access, making it unreadable without the key.

Antivirus Software: Detects, prevents, and removes malicious software like viruses, worms, and Trojans.

Question no. Q1: (d) What are the laws related to Distributed Denial of Service Attacks and Crypto-jacking?

Answer: Distributed Denial of Service (DDoS) attacks: Often covered under laws prohibiting unauthorized access, computer misuse, or disruption of services (e.g., India's IT Act 2000, US Computer Fraud and Abuse Act).

Crypto-jacking: Typically falls under laws against unauthorized access, computer misuse, theft of services, or illicit mining (e.g., sections of the IT Act 2000 in India related to unauthorized access or damage to computer systems).

Question no. Q2: (a) Transposition Ciphers

Answer: Transposition Ciphers: Rearrange the order of letters in a message without changing the letters themselves. Example: "HELLO" encrypted with a simple columnar transposition might become "EHLLO" by writing it in columns and reading down.

Question no. Q2: (b) Advantages and Disadvantages of Symmetric Key Cryptography

Answer: Advantages: Fast encryption/decryption, computationally efficient, suitable for large data sets. Disadvantages: Key distribution is a challenge (securely sharing the secret key), key management can be complex for many users.

Question no. Q2: (c) Steganography

Answer: Steganography: Hiding a secret message within another non-secret message or data (e.g., embedding text within an image file without visible changes). Example: Hiding a secret document within the pixel data of a seemingly ordinary JPEG image.

Question no. Q2: (d) Data Encryption Standard (DES)

Answer: Data Encryption Standard (DES): A symmetric-key algorithm for the encryption of electronic data, using a 56-bit key. Example: Encrypting a block of text using the DES algorithm to secure its transmission.

Question no. Q2: (e) Hash functions

Answer: Hash functions: Mathematical algorithms that take an input (or message) and return a fixed-size string of bytes, typically a 'digest' or 'hash value'. They are one-way. Example: Calculating the SHA-256 hash of a file to verify its integrity; any change in the file will result in a different hash.

Question no. Q2: (f) Key Establishment, Management and Certification in the context of cryptography

Answer: Key Establishment: The process by which cryptographic keys are created and agreed upon between communicating parties. Management: The handling of

cryptographic keys throughout their lifecycle, including generation, storage, usage, archiving, and destruction. Certification: The process of verifying the authenticity and validity of public keys, often through digital certificates issued by Certificate Authorities (CAs). Example: Using Diffie-Hellman for key establishment, a Key Management System (KMS) for storing keys, and X.509 certificates for public key certification.

Question no. Q3: (a) What are the practices for implementing the CIA triad in data security? Explain.

Answer: Confidentiality: Access control (least privilege), encryption, data masking, secure storage. Integrity: Hashing, digital signatures, version control, input validation, checksums. Availability: Redundancy (backups, RAID), disaster recovery plans, load balancing, regular maintenance.

Question no. 3: (b) Explain the following: (i) Ransomware attacks (ii) Cyber-physical attacks

Answer: (i) Ransomware attacks: Malicious software that encrypts a victim's files, demanding a ransom payment (usually cryptocurrency) for decryption.

(ii) Cyber-physical attacks: Attacks that target and manipulate physical systems (e.g., industrial control systems, power grids) through cyber means, causing real-world damage or disruption.

Question no. Q3: (c) Explain the following data security measures: (i) Email Security (ii) Risk-Assessment Analysis

Answer:

(i) Email Security: Measures to protect email communications from unauthorized

access, loss, or compromise (e g, spam filters, encryption, sender authentication like SPF/DKIM/DMARC, user training against phishing).

(ii) Risk-Assessment Analysis: The process of identifying, analyzing, and evaluating risks to an organization's information assets, determining the likelihood and impact of potential threats and vulnerabilities.

Question no. Q3: (d) What is a Security audit? Explain with the help of an example. What are the different trade-offs between security and usability?

Answer: Security audit: A systematic evaluation of the security of a company's information system by measuring how well it conforms to a set of established criteria.

Example: A company hires an external firm to conduct a penetration test on its web application to identify vulnerabilities. Trade-offs: Increased security often means reduced usability (e g, strong passwords are secure but harder to remember; multi-factor authentication is secure but adds steps). Balancing these is crucial.

Question no. Q4: (a) How can cyberspace be regulated? Explain.

Answer: Cyberspace can be regulated through various approaches:

Legislation: Laws enacted by governments (e g, data protection acts, cybercrime laws).

Technology: Technical standards, protocols, and security measures embedded in systems.

Self-regulation: Industry codes of conduct, best practices, and ethical

guidelines.

Market forces: Consumer demand for secure products and services, reputation.

International cooperation: Treaties and agreements between nations to address cross-border cyber issues.

Question no. Q4: (b) What are the different approaches of regulating Internet content? Explain.

Answer:

Government Censorship/Filtering: Direct blocking or removal of content deemed illegal or undesirable by authorities (e.g., China's Great Firewall).

Intermediary Liability: Holding Internet Service Providers (ISPs) or platforms responsible for content hosted or transmitted through their services (e.g., Section 230 in the US, IT Act in India).

Self-regulation/Industry Codes: Platforms setting their own content policies and moderation guidelines (e.g., social media community standards).

User Reporting/Flagging: Empowering users to report inappropriate content for review by platform moderators.

Notice and Takedown: A system where content is removed upon notification of infringement (e.g., copyright infringement).

Question no. Q4: (c) What are the doctrines and Articles of UNCITRAL model law? Explain.

Answer: The UNCITRAL Model Law on Electronic Commerce (1996) aims to facilitate the use of electronic means in commerce by removing legal obstacles. Doctrines:

Functional Equivalence: Electronic communications should be given the same legal validity as paper-based communications if they fulfill similar functions (e g, electronic signatures equivalent to handwritten ones).

Non-discrimination: Electronic communications should not be denied legal effect solely because they are in electronic form. Articles: Key articles cover topics like legal recognition of data messages (Art. 5), writing (Art. 6), signature (Art. 7), originality (Art. 8), and admissibility and evidential weight of data messages (Art. 9).

Question no. Q4: (d) What are the regulations for cyberspace content in India? Explain

Answer: In India, cyberspace content is primarily regulated by the Information Technology (IT) Act, 2000, and its subsequent amendments and rules. Key aspects include:

Intermediary Guidelines: Rules for social media platforms and other intermediaries regarding content moderation, due diligence, and grievance redressal (e g, IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021).

Obscenity and Harmful Content: Prohibition of publishing or transmitting obscene material (Section 67 IT Act) and content depicting children in sexually explicit acts (Section 67B).

Defamation: Content that harms reputation can lead to civil or criminal liability.

Copyright Infringement: Laws protect intellectual property, and infringing

content can be subject to takedown notices.

National Security: Content that incites violence, hatred, or poses a threat to national security can be restricted.

Question no. Q5: (a) How is cybercrime defined? Explain the classification of cybercrimes with the help of examples.

Answer: Cybercrime: Any criminal activity that involves a computer, networked device, or network. Classification:

Against Individuals: Cyberstalking (e.g., harassing someone online), online fraud (e.g., fake lottery scams), identity theft (e.g., stealing personal data for financial gain).

Against Property: Hacking (e.g., unauthorized access to a server), intellectual property theft (e.g., pirating software), data theft (e.g., stealing customer lists).

Against Government/Society: Cyberterrorism (e.g., using cyber attacks to disrupt critical infrastructure), cyber warfare (e.g., state-sponsored attacks), spreading misinformation.

Question no. Q5: (b) List the Penalties and compensation in Section 44 of the Information Technology Act 2000.

Answer: Section 44 of the Information Technology Act 2000 deals with penalties for failure to furnish information, return, etc. It states that if any person who is required to furnish any information, document, or return to the Controller or Certifying Authority fails to do so, he shall be liable to a penalty not exceeding Rs. 1,50,000 for each such failure

Question no. Q5. (c) List any six offences under sections 65 and 66 as per the Information Technology Act, 2000.

Answer: Section 65 (Tampering with Computer Source Documents):

Intentionally concealing, destroying, or altering computer source code.

Causing others to conceal, destroy, or alter computer source code.

Section 66 (Computer Related Offences):

Hacking (unauthorized access to a computer system with intent to cause wrongful loss/gain).

Sending offensive messages through communication service.

Receiving stolen computer resource or communication device.

Cheating by personation by using computer resource.

Publishing or transmitting obscene material in electronic form.

Publishing or transmitting material containing sexually explicit act, etc, in electronic form.

Question no. Q6. (d) What are the grounds which exempt the network service providers from liability? Explain.

Answer: Network service providers (intermediaries) are generally exempt from liability under Section 79 of the IT Act, 2000, if they:

Do not initiate the transmission.

Do not select the receiver of the transmission.

Do not select or modify the information contained in the transmission.

Observe due diligence in discharging their duties under the Act and rules.

Have not conspired or abetted or facilitated the commission of the

unlawful act.

Upon receiving actual knowledge or upon being notified by the appropriate Government or its agency, they expeditiously remove or disable access to the unlawful material.

Question no. Q6: (e) What are the different cyber forensic investigation tools? Explain

Answer: Cyber forensic investigation tools are used to collect, preserve, analyze, and present digital evidence.

Disk Imaging Tools: Create bit-for-bit copies of storage devices to preserve evidence (e.g., FTK Imager, EnCase).

Data Recovery Tools: Recover deleted or corrupted files from storage media (e.g., Recuva, PhotoRec).

Password Crackers: Attempt to recover passwords from encrypted files or systems (e.g., John the Ripper, Hashcat).

Network Forensic Tools: Capture and analyze network traffic to identify malicious activity (e.g., Wireshark, Snort).

Mobile Forensic Tools: Extract data from mobile devices (e.g., Cellebrite, UFED).

Registry Analysis Tools: Examine Windows Registry for evidence of user activity, installed programs, etc. (e.g., RegRipper).

Question no. Q6: (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

Answer:

(i) Copyrights and related rights: Legal rights granted to creators of original literary, dramatic, musical, and artistic works. Example: The author of a novel holds the copyright, preventing others from reproducing or distributing it without permission. Related rights include those of performers or broadcasters.

(ii) Trade Secrets: Confidential information that provides a business with a competitive edge. Example: The formula for Coca-Cola is a famous trade secret, protected as long as it remains confidential.

(iii) Geographical Indication: A sign used on products that have a specific geographical origin and possess qualities or a reputation due to that origin. Example: Darjeeling Tea, which can only be produced in the Darjeeling region of India, has a specific quality attributable to its origin.

Question no. Q6: (b) Explain cyber-squatting and abuse of search engines with the help of an example of each.

Answer: Cyber-squatting: Registering, trafficking in, or using a domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else. Example: Registering "google.co.in" (if not owned by Google) to sell it to Google at an inflated price or to mislead users.

Abuse of search engines: Manipulating search engine algorithms to unfairly rank websites higher in search results, often through unethical or black-

hat SEO techniques. Example: "Keyword stuffing" (filling a webpage withirrelevant keywords) or creating numerous low-quality backlinks toartificially boost a site's ranking.

Question no. Q6: (c) What remedies are available against infringement of IPR?

Answer: Remedies against infringement of IPR (Intellectual Property Rights) typically include:

Injunctions: Court orders prohibiting the infringer from continuing the infringing activity.

Damages: Monetary compensation for the losses suffered by the IPR owner due to the infringement.

Account of Profits: The infringer may be ordered to pay the profits they made from the infringing activity to the IPR owner.

Delivery up or Destruction: Infringing goods or materials used in the infringement may be ordered to be delivered up to the IPR owner or destroyed.

Anton Piller Order: A court order allowing the IPR owner to search the infringer's premises and seize evidence.

Mareva Injunction: A court order freezing the infringer's assets to prevent them from being moved out of jurisdiction.