K. K. Wagh Institute of Engineering Education and Research, Nashik
(An Autonomous Institute from A. Y. 2022-23)

End-Sem Examination- Winter 2025
Model Answer

Academic Year: 2025-2026	Semester: I
Name of Programme: MCA	Pattern: 2024
Name of Course: Elective II: Cyber Security	Course Code: 2409515A
Max. Marks: 60	Duration: 2:30Hr.

Q. No.	Details	Max. Marks
1	**Explain the basic components and elements of Information Security with reference to Confidentiality, Integrity, and Availability. (8 marks)** **Answer:** Information Security refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The main goal is to ensure the security of data in all forms. [Definition of Information Security – 1M] The basic components of Information Security include people, processes, and technology. People are responsible for following security policies, processes define security procedures, and technology provides tools such as firewalls and encryption. [Basic components – 2M] The elements of Information Security are represented by the CIA triad. Confidentiality ensures that information is accessible only to authorized users, achieved using encryption and access control. [Confidentiality – 1M] Integrity ensures that data remains accurate and unaltered during storage or transmission, maintained using hashing and digital signatures. [Integrity – 1M] Availability ensures that information and systems are accessible when required, achieved using backups and fault-tolerant systems. [Availability – 1M] Thus, the CIA triad forms the foundation of Information Security. [Conclusion – included]	[6]

2	**Explain encryption methods and standards with reference to symmetric and asymmetric encryption, DES, and AES.** **Answer:** Encryption is the process of converting plaintext into ciphertext to protect data from unauthorized access. It is a core concept of cryptography and ensures data confidentiality. [Definition of encryption – 1M] Symmetric encryption uses the same secret key for both encryption and decryption. It is fast and suitable for bulk data encryption. Examples include DES and AES. However, secure key distribution is a major limitation. [Symmetric encryption – 1M] Asymmetric encryption uses a pair of keys: a public key for encryption and a private key for decryption. It provides better key management and security but is computationally slower. [Asymmetric encryption – 1M] Data Encryption Standard (DES) is a block cipher that operates on 64-bit blocks using a 56-bit key and follows the Feistel cipher structure. It uses 16 rounds of substitution and permutation. Weak keys in DES can produce identical subkeys, reducing security. [DES explanation & weak keys – 1M] Advanced Encryption Standard (AES) is a modern symmetric block cipher that supports 128, 192, and 256-bit keys. It offers high security, efficiency, and resistance to cryptographic attacks, making it the current encryption standard. [AES explanation – 2M]	[6]
Q.3	**a) Interpret the concept of risk management in information security with reference to risk identification, assessment, and control strategies.** **Answer:** Risk management in information security is the process of identifying, assessing, and minimizing risks to protect information assets. It helps organizations understand potential threats and their impact. [Definition of risk management – 2M] Risk identification involves recognizing assets, threats, vulnerabilities, and possible security incidents. Common threats include malware, unauthorized access, and data breaches. [Risk identification – 2M] Risk assessment evaluates the likelihood and impact of identified risks. It can be performed using qualitative (low, medium, high) or quantitative (numerical values) methods.	[16]

[Risk assessment – 2M]

Risk control strategies include risk avoidance, risk mitigation, risk transfer, and risk acceptance. These strategies reduce the probability or impact of security incidents.
[Risk control strategies – 2M]

Thus, effective risk management ensures systematic protection of information systems.
[Conclusion – included]

OR

b) Compare qualitative and quantitative risk assessment practices used in information security (8 marks)
Answer:
Risk assessment helps determine the severity of risks to information systems. Two commonly used approaches are qualitative and quantitative risk assessment.
[Introduction – 1M]

Qualitative risk assessment uses descriptive scales such as high, medium, and low. It is simple, cost-effective, and based on expert judgment. However, it lacks numerical precision.
[Qualitative risk assessment – 3M]

Quantitative risk assessment assigns numerical values to risk factors, such as probability and financial loss. It provides accurate cost–benefit analysis but requires extensive data and expertise.
[Quantitative risk assessment – 3M]

Both approaches are used depending on organizational needs, resources, and risk complexity.
[Conclusion – 1M]

c) Interpret laws and ethics in information security with reference to cybercrime and legal perspectives in India and globally. (8 marks)
Answer:
Information security laws and ethics provide guidelines for responsible use of information systems and protection of digital assets.
[Introduction – 2M]

Cybercrime refers to illegal activities carried out using computers and networks. Examples include hacking, identity theft, and online fraud.
[Cybercrime explanation – 2M]
In the Indian legal perspective, cyber laws are governed by the Information Technology Act, 2000, which addresses offences such as unauthorized access,

	data theft, and cyber terrorism. [Indian legal perspective – 2M] From a global perspective, international cooperation and laws such as the Budapest Convention help combat cybercrime across borders. [Global legal perspective – 2M] Thus, laws and ethics play a crucial role in maintaining cyber security. [Conclusion – included] OR	
	d) Summarise social engineering attacks, cyber stalking, and cloud computing related cybercrimes. (8) **Answer:** Social engineering is a cyber-attack technique that manipulates individuals into revealing confidential information. Common methods include phishing and pretexting. [Social engineering – 3M] Cyber stalking involves repeated online harassment or monitoring of individuals through emails, social media, or messaging platforms. It violates privacy and can cause psychological harm. [Cyber stalking – 2M] Cloud computing related cybercrimes include data breaches, account hijacking, and insecure APIs due to shared resources and remote access. [Cloud computing & cybercrime – 2M] Understanding these attacks helps individuals and organizations adopt preventive security measures. [Conclusion – 1M]	
Q.4	**a) Classify Public Key Infrastructure (PKI) and X.509 digital certificates used for secure communication. (8 marks)** **Answer:** 1. Public Key Infrastructure (PKI) is a system used to manage public keys and digital certificates to enable secure communication over networks. [Definition – 2M] 2. PKI provides security services such as authentication, confidentiality, integrity, and non-repudiation. [Purpose – 1M] 3. The main components of PKI are: o Certificate Authority (CA) – issues and verifies certificates	[16]

- Registration Authority (RA) – verifies user identity
- Public and Private Keys
- Certificate Repository
  [Components – 2M]

4. X.509 digital certificate is a standard certificate format used in PKI. It binds a public key with the identity of a user or organization.
   [X.509 definition – 1M]
5. An X.509 certificate contains details such as subject name, public key, validity period, serial number, and CA's digital signature.
   [Certificate contents – 2M]

Thus, PKI and X.509 certificates ensure secure identity verification and encrypted communication.

OR

b) Summarize the Needham–Schroeder authentication algorithm and Kerberos authentication system. (8 marks)

Answer:

1. The Needham–Schroeder algorithm is an authentication protocol that uses symmetric key cryptography and a trusted third party.
   [Definition – 2M]
2. It uses session keys and nonces to authenticate communicating parties and prevent replay attacks.
   [Basic working – 2M]
3. The protocol involves three entities: User A, User B, and a Key Distribution Centre (KDC).
   [Entities – 1M]
4. Kerberos is a network authentication protocol based on the Needham–Schroeder concept.
   [Kerberos introduction – 1M]
5. Kerberos uses a Key Distribution Centre (KDC) which consists of:
   - Authentication Server (AS)
   - Ticket Granting Server (TGS)
     [Kerberos components – 1M]
6. Kerberos provides mutual authentication and secure ticket-based access to network services.
   [Advantages – 1M]

c) Summarize IP Security (IPSec) with reference to IPv6 and its security services. (8 marks)

Answer:

1. IPSec (IP Security) is a framework used to secure IP communication by protecting IP packets at the network layer.
   [Definition – 2M]
2. IPSec is mandatory in IPv6 and optional in IPv4, providing built-in security support.

	[IPv6 relevance – 1M] 3. IPSec provides the following security services: o Authentication o Confidentiality o Integrity o Anti-replay protection [Security services – 2M] 4. IPSec consists of two main protocols: o Authentication Header (AH) – provides authentication and integrity o Encapsulating Security Payload (ESP) – provides encryption and confidentiality [AH and ESP – 2M] 5. IPSec is commonly used in Virtual Private Networks (VPNs) and secure data transmission. [Applications – 1M] OR **d) Summarize secure communication mechanisms used in web and mail security such as SSL/HTTPS, PGP, and S/MIME. (8marks)** **Answer:** 1. SSL (Secure Sockets Layer) is a protocol that provides encrypted communication between a web browser and server. [SSL definition – 2M] 2. When SSL is used with HTTP, it forms HTTPS, which ensures secure web transactions using encryption and digital certificates. [HTTPS explanation – 2M] 3. Pretty Good Privacy (PGP) is used for email security and provides encryption, digital signatures, and authentication. [PGP explanation – 2M] 4. S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard used to secure email using X.509 digital certificates. [S/MIME explanation – 2M] Thus, these protocols ensure confidentiality and authenticity in web and email communication.	
Q.5	**a) Describe phishing and password cracking attacks along with their preventive measures. (8 marks)** **Answer:** 1. Phishing is a social engineering attack where attackers trick users into revealing sensitive information such as passwords or banking details through fake emails or websites. [Phishing explanation – 3M]	[16]

2. Common phishing techniques include email phishing, spear phishing, and website spoofing.
   [Types of phishing – 1M]
3. Password cracking is the process of obtaining passwords by techniques such as brute force, dictionary attacks, and rainbow tables.
   [Password cracking explanation – 2M]
4. Preventive measures include using strong passwords, two-factor authentication, email filtering, and user awareness training.
   [Prevention – 2M]

OR

b) Explain different types of malwares such as viruses, worms, spyware, adware, and ransomware. (8 marks)

Answer:

1. Malware refers to malicious software designed to damage or disrupt computer systems.
   [Malware definition – 1M]
2. A virus attaches itself to a host program and spreads when the infected file is executed.
   [Virus – 2M]
3. A worm is a standalone malware that self-replicates and spreads across networks without user intervention.
   [Worm – 2M]
4. Spyware secretly collects user information, while adware displays unwanted advertisements.
   [Spyware & Adware – 2M]
5. Ransomware encrypts user data and demands payment for decryption.
   [Ransomware – 1M]

c) Explain DoS and DDoS attacks, SQL injection, and buffer overflow attacks. (8 marks)

Answer:

1. A Denial of Service (DoS) attack aims to make a system unavailable by overwhelming it with requests.
   [DoS explanation – 2M]
2. A Distributed Denial of Service (DDoS) attack uses multiple compromised systems to flood the target.
   [DDoS explanation – 2M]
3. SQL injection is an attack where malicious SQL statements are inserted into input fields to access or modify databases.
   [SQL injection – 2M]
4. Buffer overflow occurs when more data is written to a buffer than it can handle, leading to system crashes or code execution.

	[Buffer overflow – 2M] OR **d) Describe antivirus software, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS). (8 marks)** **Answer:** 1. Antivirus software detects and removes malware using signature-based and heuristic techniques. [Antivirus explanation – 2M] 2. Other security measures include firewalls, regular updates, and access control mechanisms. [Security measures – 1M] 3. An Intrusion Detection System (IDS) monitors network or system activities to detect malicious behavior. [IDS definition – 2M] 4. Types of IDS include Network-based IDS (NIDS) and Host-based IDS (HIDS). [Types of IDS – 2M] 5. An Intrusion Prevention System (IPS) not only detects but also blocks malicious activities in real time. [IPS explanation – 1M]	