

Term End Examination January – 2026

Date : 26/02/2026
Time : 03:00pm to 05:15pm
Duration : 02.15 Hours
Max. Marks : 70

Section A

Answer the following (Attempt any three)

(30)

1. Define Cyber Security. Explain the CIA Triad (Confidentiality, Integrity, and Availability) and its importance in protecting information systems.
2. What is Cryptography? Differentiate between Symmetric and Asymmetric Key Encryption with suitable diagrams and examples.
3. Explain the various types of Cyber Attacks such as Phishing, Denial of Service (DoS), and Man-in-the-Middle (MitM) attacks.
4. Discuss the role of Firewalls and Intrusion Detection Systems (IDS) in network security. How do they prevent unauthorized access?
5. Explain the Indian IT Act, 2000. Discuss the major legal provisions and amendments related to cybercrimes in India.

Section B

Answer the following (Attempt any four)

(20)

1. Explain the concept of Intellectual Property Rights (IPR) in the cyber world, specifically focusing on Copyrights.
2. What is Digital Signature? Explain how it ensures the authenticity and non-repudiation of a document.
3. Discuss the different types of Malicious Software (Malware) like Viruses, Worms, and Trojans.
4. What is Social Engineering? Describe common techniques used by attackers to manipulate users.
5. Write a short note on Steganography and its role in secure communication.
6. Explain the importance of Cyber Ethics and the "Ten Commandments of Computer Ethics."

Section C

Part – A (Multiple Choice Questions)

(10)

- 1 Which of the following is the primary goal of the CIA Triad?
A. Complexity
B. Confidentiality
C. Connectivity
D. Computation
- 2 In asymmetric encryption, which key is used to encrypt data sent to a specific user?
A. Private Key
B. Public Key
C. Shared Key
D. Session Key
- 3 A program that replicates itself and attaches to other files is called a:
A. Trojan
B. Worm
C. Virus
D. Spyware

- 4 Which attack floods a system with traffic to make it unavailable to legitimate users?
A. Phishing B. DoS
C. SQL Injection D. Sniffing
- 5 Which act provides the legal framework for electronic governance in India?
A. Indian Penal Code B. IT Act, 2000
C. Copyright Act D. Patents Act
- 6 The process of converting cipher text back into plaintext is called:
A. Encryption B. Decryption
C. Hashing D. Steganography
- 7 Which device inspects incoming and outgoing network traffic based on security rules?
A. Router B. Firewall
C. Switch D. Hub
- 8 Intellectual Property Rights (IPR) generally include:
A. Patents B. Trademarks
C. Copyrights D. All of the above
- 9 Steganography is the art of:
A. Breaking codes B. Hiding information
C. Locking files D. Deleting logs
- 10 Non-repudiation ensures that a sender:
A. Cannot deny sending a message B. Can hide their identity
C. Encrypts the data D. Deletes the message

Part – B (Do as Directed)

(10)

State whether the following statements are true or false

- 1 Ethical hacking is the same as criminal hacking.
- 2 Hashing is a reversible process used to recover original data.
- 3 Phishing involves tricking users into revealing sensitive information via fake emails.
- 4 A Trojan horse does not replicate itself like a virus.
- 5 The Indian Copyright Act was first enacted in 1957.
- 6 Two-factor authentication (2FA) adds an extra layer of security.
- 7 Symmetric encryption uses two different keys for encryption and decryption.
- 8 Cyber bullying is considered a cybercrime under various legal jurisdictions.
- 9 Malware stands for "Malfunctioning Software."
- 10 Digital certificates are used to verify the identity of a website or user.
