



End Term (Odd) Semester Examination November 2025

Roll no.....

Name of the Course and semester: B. Tech ECE VII Semester

Name of the Paper: Fundamentals of Cybersecurity

Paper Code: TEC-707

Time: 3 hours

Maximum Marks: 100

Note:

- (i) All the questions are compulsory.
- (ii) Answer any two sub questions from a, b and c in each main question.
- (iii) Total marks for each question is 20 (twenty).
- (iv) Each sub-question carries 10 marks.

Q1. (2X10=20 Marks)

- a. Who are threat actors in the cyberspace? Explain different categories of threat actors based on their motivation and skill level. (CO1)
- b. Compare and contrast the Bell-LaPadula and Biba security models. How do they enforce security differently? (CO2)
- c. Differentiate between symmetric and asymmetric cryptography. Further, discuss suitable use cases for each and provide examples of commonly used algorithms. (CO2).

Q2. (2X10=20 Marks)

- a. Explain how firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) integrate within a defense-in-depth strategy. Discuss how their configuration, rule management, and monitoring contribute to minimizing false positives and improving overall network resilience. (CO3)
- b. Explain the working of wireless encryption protocols (WEP, and WPA). What are their potential security vulnerabilities? (CO4)
- c. Explain how SSL/TLS protocols operate in HTTPS communication. Discuss the role of digital certificates, certificate authorities (CAs), and public key infrastructure (PKI) in establishing trust between client and server. (CO5)

Q3. (2X10=20 Marks)

- a. Explain the RSA algorithm for encryption and decryption with a suitable numerical example. Further, comment on the security of the RSA algorithm. (CO2)
- b. Explain the mathematical foundations of Elliptic Curve Cryptography (ECC) and how it achieves equivalent security with smaller key sizes compared to RSA. Discuss the computational problems that ensure its security. (CO2)
- c. Explain the architecture and working of the Secure Shell (SSH) protocol. Discuss how it ensures confidentiality, integrity, and authentication during remote communication. Use figures in your answer. (CO5)

Q4. (2X10=20 Marks)

- a. Demonstrate how SQL Injection and Cross-Site Scripting (XSS) attacks work. How these attacks can be mitigated? (CO3)
- b. Explain the detailed mechanism of a Cross-Site Request Forgery (CSRF) attack and analyze how it exploits session management weaknesses in modern web applications. Discuss advanced mitigation techniques, including token-based and same-site cookie approaches. (CO5)
- c. Describe the process of reporting and remediation after a penetration test. What are key components of a good report? (CO4)

Q5. (2X10=20 Marks)

- a. Explain how GDPR and HIPAA regulations shape the design and implementation of cybersecurity



End Term (Odd) Semester Examination November 2025

controls within multinational organizations. Discuss the technical and procedural challenges in ensuring compliance across jurisdictions. (CO5)

b. What are social engineering attacks. Critically evaluate how well-designed security awareness programs influence employee behavior and organizational resilience against social engineering attacks. (CO2)

c. Explain the key components of a Disaster Recovery (DR) plan in modern organizations. How do data backup, replication, and the concepts of Recovery Point Objective (RPO) and Recovery Time Objective (RTO) help in maintaining business continuity after a system failure or cyber incident? (CO5)