Reg. No. : E N G G T R E E . C O M

Question Paper Code : 40455

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2024.

Fifth/Sixth Semester

Computer Science and Engineering

CCS 354 — NETWORK SECURITY

(Common to : Computer Science and Engineering (Artificial Intelligence and Machine Learning)/Computer and Communication Engineering/Artificial Intelligence and Data Science/Information Technology)

(Regulations 2021)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Compare and contrast symmetric and asymmetric encryption.
2. How does a digital signature ensure data integrity?
3. Outline the role of X.509 certificates in secure communications.
4. Define remote user authentication and why it is essential in network security.
5. Mention the function of the Extensible Authentication Protocol (EAP).
6. Show the two phases of the Internet Key Exchange (IKE) protocol.
7. How does Domain Keys Identified Mail (DKIM) verify the authenticity of an email message?
8. Outline the role of public and private keys in Pretty Good Privacy (PGP)
9. List the key characteristics of a strong password policy for an organization.
10. How does Intrusion Prevention System (IPS) differ from Intrusion Detection System (IDS) in application?

PART B — (5 × 13 = 65 marks)

11. (a) Examine the RSA algorithm. Outline its mathematical foundation, and critically assess its security and efficiency in modern applications.

Or

(b) Discuss various methods of cryptographic authentication, including password-based, token-based, and biometric approaches.

12. (a) Explain the principles of the Kerberos authentication system. Analyze its strengths and weaknesses in providing secure user authentication.

Or

(b) Evaluate the principles and components of remote user authentication in distributed networks, discussing how encryption methods are used to achieve secure authentication in real-world applications.

13. (a) Describe the architecture of IP Security (IPSec) and discuss its modes of operation. Critically analyze how IPSec provides confidentiality, integrity, and authentication over IP networks.

Or

(b) Discuss the design and functionality of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols.

14. (a) Summarize the steps involved in implementing S/MIME in an organizational email system and illustrate the process of message encryption and digital signatures in S/MIME.

Or

(b) Interpret a secure email communication framework using a combination of PGP, S/MIME, and DKIM to address authentication, integrity and confidentiality in a corporate setup.

15. (a) (i) Explain a network architecture utilizing different types of firewalls, such as packet-filtering, proxy and stateful firewalls, for optimal security. (7)

(ii) Discuss the positioning, configuration, and management of each firewall type, emphasizing their unique roles in protecting various network segments. (6)

Or

(b) (i) Explain how blockchain technology can be integrated into a supply chain system to enhance transparency, security and traceability of transactions. (7)

(ii) Summarize the practical steps for implementing blockchain, along with potential challenges like privacy concerns and high resource consumption. (6)

PART C — (1 × 15 = 15 marks)

16. (a) Assume an enterprise wants to implement strict access control measures to secure its internal network.

(i) Describe how IEEE 802.1X port-based network access control could be applied within this organization. (5)

(ii) Outline how Extensible Authentication Protocol (EAP) integrates with IEEE 802.1X. (5)

(iii) Evaluate potential security benefits and challenges that might arise. (5)

Or

(b) Develop a firewall strategy for an enterprise network, including selecting firewall types (e.g., packet-filtering, proxy, and stateful inspection firewalls) based on network segments and security needs. Detail considerations for firewall placement, configuration settings, and ongoing management to prevent unauthorized access and optimize network performance.

———————