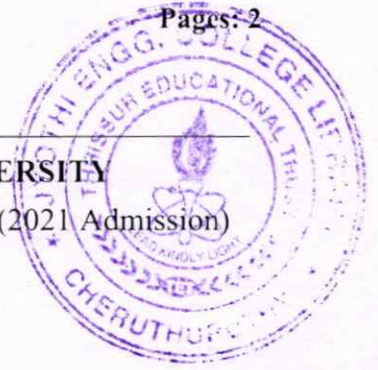


Reg No.: _____

Name: _____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Sixth Semester B.Tech (Hons.) Degree Examination June 2024 (2021 Admission)

**Course Code: CST394****Course Name: NETWORK SECURITY**

Max. Marks: 100

Duration: 3 Hours

PART A*Answer all questions, each carries 3 marks.*

- | | | Marks |
|----|---|-------|
| 1 | Define network security and list at least three security requirements essential for a secure network. | (3) |
| 2 | Explain spyware and adware. | (3) |
| 3 | Define dual signature with an example. | (3) |
| 4 | Explain the authentication and encryption processes in Kerberos v4. | (3) |
| 5 | Explain the importance of message integrity and non-repudiation in email security. | (3) |
| 6 | List the four steps for preparing an EnvelopedData MIME entity. | (3) |
| 7 | Define web security and explain its importance. | (3) |
| 8 | Explain the process of initiating a secure HTTPS connection. | (3) |
| 9 | Discuss the improvements introduced in WPA2 over WPA. | (3) |
| 10 | Explain the main services provided by an IEEE 802.11 Wireless LAN. | (3) |

PART B*Answer one full question from each module, each carries 14 marks.***Module I**

- 11 a) Discuss two techniques used by IDS to detect malicious activities. (8)
- b) Differentiate between worms, viruses, and trojans, providing one example of each. (6)

OR

- 12 a) Explain the Schnorr digital signature algorithm and its advantages. (7)
- b) Illustrate the ElGamal digital signature scheme in detail. (7)

Module II

- 13 a) Compare the cryptographic algorithms and message formats used in Kerberos V5 with those in V4. (7)
- b) Describe the Encapsulating Security Payload (ESP) in IPsec and how it enhances security. (7)

OR

- 14 a) Outline the phases of the Internet Key Exchange (IKE) process in IPsec. (7)
b) Explain the role of the Authentication Header (AH) in IPsec. (7)

Module III

- 15 a) Discuss the security features provided by S/MIME for email communication. (7)
b) Illustrate the encryption process in Privacy Enhanced Mail (PEM). (7)

OR

- 16 a) Identify and explain any two anomalies associated with PGP. (7)
b) Illustrate how does PGP handle certificate and key revocation. (7)

Module IV

- 17 a) Illustrate the connection protocol in SSH and its role in secure communication. (7)
b) Explain the transport layer protocol in Secure Shell (SSH). (7)

OR

- 18 a) Compare the differences between SSL and Transport Layer Security (TLS). (7)
b) Illustrate TLS Handshake Protocol with a neat diagram. (7)

Module V

- 19 a) Compare the security features of Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). (7)
b) Explain the Discovery phase and Authentication phase of IEEE 802.11i operation. (7)

OR

- 20 a) Compare the features of packet filters and circuit level firewalls. (7)
b) Explain the purpose of the IEEE 802.11 architectural model (7)
