Register No.: ..... Name: .....

SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

SIXTH SEMESTER B.TECH DEGREE EXAMINATION (R), MAY 2023

(2020 SCHEME)

Course Code : 20CST392

Course Name: Network Security

Max. Marks : 100 **Duration: 3 Hours**

PART A

(Answer all questions. Each question carries 3 marks)

1. Explain about the basic requirements of Network Security.
2. Write short notes on worms and its characteristics.
3. List the procedures followed by network administrator for Denial of Service protection.
4. Compare Kerberos version 4 and version 5.
5. List the three properties to ensure security in email application.
6. End-to-end privacy is essential for e-mail security. How is it achieved?
7. List any three threats related to web security.
8. Compare Secure Socket Layer (SSL) and Transport Layer Security (TLS).
9. Compare Wi-Fi Protected Access (WPA) and WPA2.
10. List the security services provided by IEEE 802.11i.

PART B

(Answer one full question from each module, each question carries 14 marks)

MODULE I

11. a) Explain the network security model with the help of a neat diagram. (6)
    b) Using the ElGamal scheme, let q=19 and a=10. Find values of s1 and s2. Choose k=5 and m=14. Verify the signature by calculating v1 and v2. (8)

OR

12. a) Explain in detail about Intrusion Detection Systems (IDS) and its different types. (7)
    b) Write short notes on malicious softwares and its different types (7)

MODULE II

13. a) Bob wishes to log into Alice's workstation remotely. List the steps (7)

involved in this if Kerberos V4 is used for communication.

b) Write a short notes on Public Key Infrastructure (PKI) and its use in network security. (7)

OR

14. a) Explain in detail about Internet Protocol Security (IPSec). (8)
    b) Describe in detail about Perfect Forward Secrecy (PFS). (6)

MODULE III

15. a) Explain the Signed data and Clear-signed data functions provided by S/MIME. (8)
    b) Describe about Privacy Enhanced Mail (PEM) in detail. (6)

OR

16. a) List the four steps for preparing an Enveloped Data MIME entity. (6)
    b) Explain in detail about Pretty Good Privacy (PGP). (8)

MODULE IV

17. a) Explain in detail about Secure Sockets Layer (SSL). (8)
    b) Describe how connection initiation and connection closure is done in Hyper Text Transfer Protocol Secure (HTTPS). (6)

OR

18. a) List the sequence of events in Secure Shell (SSH) transport layer protocol packet exchanges. (8)
    b) Describe about Transport Layer Security (TLS). (6)

MODULE V

19. a) Explain in detail about firewalls and different types of firewalls. (9)
    b) Describe about IEEE 802.11 Wireless LAN network components. (5)

OR

20. a) Explain the different phases of IEEE 802.11i operation. (8)
    b) Write short notes on Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). (6)

****