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

# SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

**SIXTH SEMESTER B. TECH DEGREE EXAMINATION (R), MAY 2024**

**(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. Differentiate between viruses and Trojans
2. Define the terms
   i)Risk
   ii)Vulnerability
   iii)Attack
3. Describe the various security aspects dealt by Kerberos V4.
4. List out the features of IKE Key determination.
5. What are the security services provided for email communication?
6. "A key ring in PGP stores public key information about each key". Justify.
7. Compare between SSL connection and SSL session.
8. Describe how HTTPS ensures security in web-based applications.
9. What is WML? Illustrate the features of WML.
10. Describe services involved in the distribution of messages within a DS of 802.11.

## PART B

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

### MODULE I

11. a) Describe about issues and challenges in network security. (4)
    b) Given a prime filed q=19 with its primitive root α=10 from various primitive roots {2,3,10,13.14,15}. A user generates it private key Xa=16 for sending a message. A random number is chosen to compute the signature as K=5, to authenticate the message and send to the other side and the hash value of the message is taken as m=14. Using the ElGamal signature scheme, verify the signatures generated by the sender and receiver. (10)

**OR**

12. a) Differentiate between Host-based and network-based intrusion (6)

detection system.

b) Illustrate the Digital signature Algorithm. (8)

**MODULE II**

13. a) Design a full-service Kerberos environment consisting of a Kerberos server, a number of clients, and a number of application servers which is able to send and receive messages from various entities with neat sketches by describing about the various entities in it. (9)

b) Differentiate between Transport and tunneling modes of IP security. (5)

**OR**

14. a) Define perfect forward secrecy? Describe how a protocol achieves perfect forward secrecy with necessary figure. (7)

b) Detail how various trust models ensures confidence over certification authority (CA). (7)

**MODULE III**

15. a) Describe how authentication of the source is done in email communication. (6)

b) Describe how certificate revocation and key revocation is happening in PGP. Mention how PGP deals with anomalies. (8)

**OR**

16. a) How integrity and nonrepudiation are ensured in Privacy Enhanced mail. (7)

b) Compare clear Signed data and signed data operations in S/MIME. (7)

**MODULE IV**

17. a) Illustrate the working of SSL handshake protocol with neat sketches. (7)

b) Differentiate between SSL and TLS protocol. (7)

**OR**

18. a) Identify and describe the architecture of a secure protocol that provides remote login with neat figures. (9)

b) Describe the various security threats and its countermeasures. (5)

**MODULE V**

19. a) Illustrate the protocol architecture of IEEE 802.11 with neat sketches. (7)

b) Describe about the vulnerabilities of WEP protocol. (7)

**OR**

20. a) Compare WPA and WPA2 protocols in terms of encryption and decryption. (6)

b) Why firewalls are needed? Compare the features of packet filters and circuit level firewalls. (8)

**********