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

SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

SECOND SEMESTER M.TECH DEGREE EXAMINATION (Regular), MAY 2023

COMPUTER SCIENCE AND SYSTEMS ENGINEERING

(2021 Scheme)

Course Code: 21SE205-D

Course Name: Advanced Information Security Concepts

Max. Marks: 60 **Duration: 3 Hours**

PART A

(Answer all questions. Each question carries 3 marks)

1. How do security models help to protect sensitive information? Mention potential drawbacks if any?
2. Differentiate between viruses and worms.
3. What is PGP? What are its advantages?
4. Differentiate between one-way and two-way authentication.
5. How will you detect a DDoS attack?
6. What is IP Traceback?
7. Explain about personal firewall.
8. What is a security token, and how is it used in WS-Trust?

PART B

(Answer one full question from each module, each question carries 6 marks)

MODULE I

9. Discuss the benefits and limitations of Discretionary Access Control (DAC) and Mandatory Access Control (MAC) systems, and provide an example of when each might be more appropriate to use. (6)

OR

10. Compare and contrast the Biba and Bell-La Padula models, and explain how they can be used in conjunction to provide a more comprehensive approach to system security. (6)

MODULE II

11. Briefly explain the worm propagation model. (6)

OR

12. Write a piece of code to simulate Buffer Overflow Attack. (6)

MODULE III

13. How do DoS and DDoS attacks work, and what are some strategies for defending against them in enterprise networks? (6)

OR

14. List and explain the different TCP/IP vulnerabilities. (6)

MODULE IV

15. Explain Kerberos authentication. (6)

OR

16. What is replay attack? How to prevent it? (6)

MODULE V

17. Explain IDS. What are the different types of IDS? (6)

OR

18. Explain Fiat-Shamir Protocol. (6)

MODULE VI

19. How does a firewall work? What are its different types? (6)

OR

20. Explain SAML. (6)

****