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

SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

SECOND SEMESTER M.TECH DEGREE EXAMINATION (Regular), JULY 2022
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. What is Biba model?
2. What are topological worms? Analyze the significance of the statement- 'The rate of spreading of topological worms is potentially faster than internet scanning worms'.
3. Bob receives a PGP message. How can he find out the type of the packet if the tag value is:
   　　a. 8　　　b. 9　　　c. 2
4. Why there is a need for four nonces in the Needham-Schroeder protocol?
5. What is zero-knowledge authentication?
6. What is an Intrusion Detection System (IDS)? Explain the various tasks performed by an IDS.
7. What is WS-Trust standard?
8. What is SAML?

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

MODULE I

9. Explain role based access control with an example.　　　　　　　　　(6)

OR

10. Write a short note on
    a. Bella-La Padula model　　　　　　　　　　　　　　　　　　(3)
    b. Chinese Wall Model　　　　　　　　　　　　　　　　　　　(3)

MODULE II

11. Which are the various categories of worms based on the vector of propagation? Explain the characteristics of worms.　　　　　　　　　　　　　(6)

OR

12. Assume that a certain amount of buffer space is allocated for an array. If array bounds are not checked while populating it, the array will overflow into contiguous memory　　(6)

and corrupt it. Which type of vulnerability can occur due to this? What are the possible ways of exploiting this vulnerability?

MODULE III

13. Explain how MIME can provide security services for e-mail. (6)

OR

14. Name seven types of packets used in PGP and explain their purposes. (6)

MODULE IV

15. Define Kerberos and name its servers. Briefly explain the duties of each server. Sketch the relationship between the different servers. (6)

OR

16. What is one-way authentication? Explain about the two mechanisms by which one way authentication can be implemented. (6)

MODULE V

17. How host based detection of polymorphic/metamorphic viruses can be done? (6)

OR

18. Explain Fiat-Shamir protocol and show the logic behind the protocol using cave example. (6)

MODULE VI

19. List the main functions of a firewall. Explain the different categories of firewalls. (6)

OR

20. Explain about the WS-Security for addressing the most basic problems in securing messages used in web services. (6)

****