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

SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

FIRST SEMESTER M.TECH DEGREE EXAMINATION (Regular), DECEMBER 2023
COMPUTER SCIENCE AND SYSTEMS ENGINEERING
(2021 Scheme)

Course Code: 21SE104-C

Course Name: Computer Systems Engineering

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

PART A
(Answer all questions. Each question carries 3 marks)

1. Differentiate between validation and verification in system engineering.
2. What are the RPC semantics used to ensure modularity?
3. Describe the steps involved in translating the virtual address to the physical address in memory.
4. Explain about clock page removal algorithm.
5. Differentiate between MTTF and MTTR.
6. What are the components of the fault-tolerant design model?
7. Define the term "Cache Snooping".
8. Differentiate between strict consistency and eventual consistency.

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

MODULE I

9. Describe the power of system engineering.   (6)

OR

10. Discuss how the problems in the systems are classified.   (6)

MODULE II

11. Outline on the types of techniques used for coping with complexity.   (6)

OR

12. What do you mean by RPC? How RPC handles no response strategy.   (6)

MODULE III

13. Detail about any two strategies to minimize thrashing due to page fault and swapping mechanism with a suitable example.   (6)

OR

14. Discuss any three congestion control mechanisms in a network.   (6)

MODULE IV

15. Describe about the broadcast aspects of ethernet.   (6)

OR

16. Describe the strategical responses used by the module designer for dealing with active faults in the system.   (6)

MODULE V

17. Discuss about various types of RAID models for fault tolerance.   (6)

OR

18. Explain the various types of constraints and consistency models used in transactions.   (6)

MODULE VI

19. Define the threats with respect to Information Security. Explain the various classes of threats.   (6)

OR

20. Explain in detail SSL protocol.   (6)

****