MAY 2023 **P/ID 16311/PIT3J**

Time : Three hours Maximum : 80 marks

PART A — (10 × 2 = 20 marks)

Answer any TEN questions.

1. What is malicious code?

2. Differentiate between threat and attack.

3. What are the basic principles of security?

4. How does an operating system manage security?

5. What is two factor authentication?

6. What are the various ways for memory and address protection?

7. Define state and transition constraints.

8. What is meant by inherently sensitive data? Give example.

9. What is the use of SSL protocol?

10. What is the need for IPsec Protocol?

11. Compare and Contrast Cold site and Hot site.

12. Define the fundamentals of Symmetric encryption.

PART B — ($5 \times 6 = 30$ marks)

Answer any FIVE questions.

13. What is the difference between attack and vulnerability? List and explain any five attacks.

14. During its lifetime, a typical virus goes through the four phases. Explain.

15. Describe the access matrix model used for protection purpose.

16. Explain the file directory mechanism to project an object.

17. Explain the characteristics of good security policy.

18. Discuss the physical security controls and how the protection is planned for the natural disasters.

19. Discuss the different types of malicious code and its characteristics.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

20. Explain the non-malicious program error types with suitable example.

21. Explain the access control matrix, procedure oriented access control and role based access control.

22. Explain the mechanisms that can help to implement multilevel security for databases.

23. Explain the following firewall configurations:

    (a) Firewall with screening Router

    (b) Firewall with proxy and screening router

    (c) Firewall on Separate LAN.

24. Discuss the respective rights of employers and employees to their computer products.

———————