Register No.: [ ]

680

April 2024

Time – Three hours
(Maximum Marks: 100)

[N.B. 1. Answer all questions under Part-A. Each question carries 3 marks.

2. Answer all the questions either (a) or (b) in Part-B. Each question carries 14 marks.]

PART – A

1. List the types of security attacks.
2. Differentiate symmetric and asymmetric key cryptography.
3. Why do we need key distribution?
4. What is linear crypt analysis?
5. List out authentication requirements.
6. Can we use RSA algorithm for digital signature? List out any two digital signature algorithms.
7. Compare intrusion detection system and intrusion prevention system.
8. Why do we need Pretty Good Privacy in email security?
9. What is virus and related threats?
10. Define cross site scripting vulnerability.

[Turn over.....

PART – B

11. (a) Explain about security services and security mechanisms.

(Or)

(b) Explain the substitution techniques and transposition techniques with example.

12. (a) Explain about RSA algorithm with an example.

(Or)

(b) Explain about DES algorithm with necessary flow diagram.

13. (a) Discuss about HMAC and CMAC. Compare them.

(Or)

(b) Explain about Kerberos with necessary diagrams.

14. (a) Discuss about VPN and its modes.

(Or)

(b) Explain about IP security architecture.

15. (a) Explain the architecture of firewall with necessary diagrams.

(Or)

(b) Write short notes on:
(i) Secure socket layer. (7)
(ii) Transport layer security. (7)
