

T.Y. B.Sc COMP SCI - Sem - V dt - 20/02/2025

(2 1/2 Hours.)

[Total Marks: 75]

N. B.: (1) All questions are compulsory.(2) Make suitable assumptions wherever necessary and state the assumptions made.(3) Answers to the same question must be written together.(4) Numbers to the right indicate marks.(5) Draw neat labelled diagrams wherever necessary.(6) Use of non-programmable calculators is allowed.**1. Attempt any four of the following:**

20

- a. What are the types of security attacks?
- b. List and explain different categories of security Mechanisms.
- c. Describe the Symmetric Cipher Model in detail.
- d. Explain ECB and CBC mode of operation of cipher.
- e. Write a note on the Data Encryption standard algorithm.
- f. Differentiate between Stream cipher & Block cipher technique.

2. Attempt any four of the following:

20

- a. Describe the Public key infrastructure in detail.
- b. Write a short note on Kerberos.
- c. Explain the Diffie Hellman key exchange Algorithm.
- d. Describe RSA algorithm in detail.
- e. Explain the format of X. 509 certificate.
- f. Differentiate between symmetric and asymmetric key cryptography.

3. Attempt any four of the following:

20

- a. Discuss the Public key Distribution Scenario.
- b. Write a brief note on SSL Protocol.
- c. Describe the lifecycle of a virus.
- d. Define malicious software. Explain different types of viruses.
- e. Write a short note on Honeypots.
- f. What are firewalls? Explain packet filtering firewall.

4. Attempt any five of the following:

15

- a. What do you mean by confidentiality, Integrity & availability?
- b. Describe Man in middle attack.
- c. Distinguish between Stateless and Stateful Firewall.
- d. Explain IPSec Protocol in detail.
- e. Write a short note on MAC.
- f. Describe rail-fence Cipher with suitable example.