Code No.: R22IT702PC

| R22 | H.T.No. | | | 8 | R | | | | | | |

## CMR ENGINEERING COLLEGE: : HYDERABAD
## UGC AUTONOMOUS
### IV–B.TECH–I–Semester End Examinations (Regular) - December- 2025
### INFORMATION SECURITY
### (IT)

[Time: 3 Hours]                                                    [Max. Marks: 60]

**Note:** This question paper contains two parts A and B.
   Part A is compulsory which carries 10 marks. Answer all questions in Part A.
   Part B consists of 5 Units. Answer any one full question from each unit. Each question
   carries 10 marks and may have a, b, c as sub questions.

### PART-A                                                      (10 Marks)

1. a) What is Information Security?                                          [1M]
   b) Define random number generation in encryption techniques.             [1M]
   c) Define key management.                                                 [1M]
   d) Define authentication protocol.                                        [1M]
   e) Define digital signature.                                             [1M]
   f) What is pretty good privacy.                                          [1M]
   g) Define IP security.                                                    [1M]
   h) Define secure electronic transaction.                                 [1M]
   i) What is a virus?                                                       [1M]
   j) Define firewall.                                                       [1M]

### PART-B                                                      (50 Marks)
2. Explain the different types of security attacks and security services.   [10M]
                                **OR**
3. Explain the DES algorithm and its design principles.                     [10M]

4. Explain elliptic curve cryptography and its advantages.                  [10M]
                                **OR**
5. Explain SHA-512 algorithm with steps and draw a neat diagram.            [10M]

6. Illustrate the directory authentication service using X.509.             [10M]
                                **OR**
7. Demonstrate the S/MIME protocol and its services.                        [10M]

8. Explain combining security association and key management in IPSec.      [10M]
                                **OR**
9. Explain SSL and TLS protocols and their operation.                       [10M]

10. Explain different types of viruses and worms.                           [10M]
                                **OR**
11. Explain the architecture of an intrusion detection system.              [10M]

************