GUJARAT TECHNOLOGICAL UNIVERSITY

MCA INTEGRATED – SEMESTER VIII- EXAMINATION –WINTER-2025

Subject Code: 4480603   **Date: 19/11/2025**
Subject Name: Network Security
Time:02:30 PM TO 05:00 PM   **Total Marks: 70**

Instructions:

1. Attempt all questions.
2. Make Suitable assumptions wherever necessary.
3. Figures to the right indicate full marks.
4. Use of simple calculators and non-programmable scientific calculators are permitted.

Q.1 **(A)** **Do as Directed (Each of 1 mark)**   **07**
1. List out types of attacks on encrypted message
2. RC4 is a example of _____
3. A _____ can be given to any person with whom an individual wants to communicate (Public key / Private key)
4. List out types of Active Attacks
5. SSL Stands for _____
6. Give the digest size of SHA-512 and SHA-256
7. List out types of Malicious Software

(B) Explain OSI Security Architecture in detail   **07**

Q.2 **(A)** Describe Digital Signature with an example.   **07**
(B) Explain any four differences between Kerberos version 4 and Kerberos version 5   **07**

OR

(B) Explain RC4 algorithm   **07**

Q.3 **(A)** Explain HMAC algorithm with suitable diagram.   **07**
(B) Describe SSL methodology with block diagram   **07**

OR

Q.3 **(A)** Explain X.509 Authentication Procedures in brief   **07**
(B) What is SSH? Explain in brief the three protocols of SSH.   **07**

Q.4 **(A)** Explain the various cipher block modes of operations.   **07**
(B) Explain the basic five ingredients of Symmetric Encryption principles

OR

Q.4 **(A)** Discuss IEEE 802.11 Services.   **07**
(B) Explain HMAC algorithm with suitable diagram.   **07**

Q.5 **(A)** Difference between AES and DES   **07**
(B) Describe Firewall with its types.   **07**

OR

Q.5 **(A)** Explain Intrusion Detection System.   **07**
(B) What is Pretty Good Privacy (PGP)? Discuss its services in detail.   **07**

*****