Enrolment No. /Seat No.: ______________

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA INTEGRATED– SEMESTER VIII- EXAMINATION –SUMMER-2024

Subject Code: 4480603 **Date: 04/05/2024**

Subject Name: Network Security

Time: 10:30 AM TO 01:00 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)** Answers the following: **07**

1. Define Message Authentication
2. Define Active attacks.
3. What do you mean by Asymmetric encryption?
4. MIME coverts ASCII-data into non-ASCII data. [True/False]
5. Define Denial of Service.
6. What are the three classes of intruders?
7. Explain the term “Salt”.

(b) Explain in detail security attacks. **07**

Q.2 **(a)** 1. Compare DES, 3DES and AES. (3) **07**
2. List different fields of Authentication Header.(4)

(b) Explain AES with diagram. **07**

OR

(b) Explain Diffie-Hellman key exchange with highlighting the need of it **07**

Q.3 **(a)** Explain SHA-256 with diagram. **07**

(b) Explain HMAC algorithm with suitable diagram. **07**

OR

Q.3 **(a)** What is public key cryptography? Explain any one public key cryptography algorithm in detail. **07**

(b) Briefly explain the structure/format indicating the different fields of Public Key Ring in PGP. **07**

Q.4 **(a)** Discuss Kerberos protocol with diagram. **07**

(b) What is random number generator? Discuss TRNG, PRNG and PRF with suitable diagram. **07**

OR

Q.4 **(a)** Explain Intrusion Detection System. **07**

(b) What do you mean by port forwarding? Explain local forwarding and remote forwarding. **07**

Q.5 **(a)** Describe RSA algorithm with example. **07**

(b) Describe Firewall with its types. **07**

OR

Q.5 **(a)** List out the various categories of malicious software. Explain any two in detail. **07**

(b) Write notes on X.509 certificate. **07**

****