

Enrolment No./Seat No\_\_\_\_\_

## GUJARAT TECHNOLOGICAL UNIVERSITY

BE- SEMESTER-VII EXAMINATION – WINTER 2025

Subject Code:3174202

Date:15-11-2025

Subject Name:Cryptography and 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. Simple and non-programmable scientific calculators are allowed.

|                                                                                                                       | MARKS |
|-----------------------------------------------------------------------------------------------------------------------|-------|
| <b>Q.1</b> (a) Define the following terms in brief:                                                                   | 03    |
| i) Confidentiality                                                                                                    |       |
| ii) Non-repudiation                                                                                                   |       |
| iii) Access Control.                                                                                                  |       |
| (b) Compare Symmetric encryption and Asymmetric encryption with an appropriate example.                               | 04    |
| (c) Giving example, explain cryptanalytic attacks in detail.                                                          | 07    |
| <b>Q.2</b> (a) Illustrate encryption using columnar transposition Cipher.                                             | 03    |
| (b) Let the keyword in playfair cipher be “Check Mee”. Encrypt a message “Eagle in the Market” using playfair cipher. | 04    |
| (c) Explain RSA algorithm in detail with suitable example.                                                            | 07    |
| <b>OR</b>                                                                                                             |       |
| (c) Briefly explain Diffie Hellman Key exchange with an example.                                                      | 07    |
| <b>Q.3</b> (a) Define the following terms:                                                                            | 03    |
| Masquerade attack, Source repudiation and Destination repudiation                                                     |       |
| (b) Explain different ways for distribution of public keys?                                                           | 04    |
| (c) What is digital signature? Explain hash code base digital signature.                                              | 07    |
| <b>OR</b>                                                                                                             |       |
| <b>Q.3</b> (a) Write a short note on fiestal structure.                                                               | 03    |
| (b) Discuss man-in-the middle attack on Diffie-Hellman key exchange.                                                  | 04    |
| (c) Explain HMAC algorithm in detail.                                                                                 | 07    |
| <b>Q.4</b> (a) What is role of SSL?                                                                                   | 03    |
| (b) Describe Elgamal digital signature.                                                                               | 04    |
| (c) Define KDC? With the help of diagram explain how KDC does key distribution.                                       | 07    |
| <b>OR</b>                                                                                                             |       |
| <b>Q.4</b> (a) Define Digital Signature. What is DSS approach?                                                        | 03    |
| (b) Write a brief note on Public key Infrastructure in security.                                                      | 04    |
| (c) Explain DSA (Digital Signature Algorithm) in detail.                                                              | 07    |

- Q.5** (a) What is SSH? How it works? **03**  
(b) Explain Authentication Header (AH) in brief. **04**  
(c) What is Kerberos? How it works? Explain in detail. **07**

**OR**

- Q.5** (a) What is digital certificate? What is the purpose of X.509? **03**  
(b) What Is Email Security? List some ways to secure your email. **04**  
(c) Enlist block cipher modes of operation. Justify the use of Electronic Codebook (ECB) mode in Cipher Block Chaining (CBC) mode. **07**

\*\*\*\*\*