

Seat No.: _____

Enrolment No. _____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER-VII (NEW) EXAMINATION – WINTER 2023

Subject Code:2170709

Date:14-12-2023

Subject Name:Information 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

- | | | |
|------------|---|-----------|
| Q.1 | (a) Define following Principles of Security:
1) Confidentiality 2) Integrity 3) Availability | 03 |
| | (b) Differentiate poly alphabetic cipher and mono alphabetic cipher. | 04 |
| | (c) Perform encryption in Playfair Cipher algorithm with plain text as “INFORMATION AND NETWORK SECURITY”, Keyword is “MONARCHY”. | 07 |
| Q.2 | (a) What is brute force attack? Explain with an example. | 03 |
| | (b) What is diffusion and confusion? How are they used in DES? | 04 |
| | (c) Draw neat diagram of AES key generation. Explain encryption process of AES. | 07 |
| | OR | |
| | (c) Enlist block cipher modes of operation. Justify the use of Electronic Codebook (ECB) mode in Cipher Block Chaining (CBC) mode. | 07 |
| Q.3 | (a) Explain encryption and decryption using RSA. | 03 |
| | (b) Perform encryption and decryption using RSA algorithm for following:
$p=3; q=11, e=7; M=2$ | 04 |
| | (c) Differentiate Hash code with MAC code. | 07 |
| | OR | |
| Q.3 | (a) Compare symmetric key encryption with asymmetric key encryption | 03 |
| | (b) Explain man in the middle attack. | 04 |
| | (c) Explain the Diffie Hellman key exchange scheme in detail with an example | 07 |
| Q.4 | (a) What characteristics are needed in a secure hash function? | 03 |
| | (b) What is digital signature? What are the properties a digital signature should have? | 04 |
| | (c) Discuss SHA-512. | 07 |
| | OR | |
| Q.4 | (a) Differentiate confidentiality and authentication. | 03 |
| | (b) Describe Birthday attack. | 04 |
| | (c) What is Kerberos? How it works? Explain in detail. | 07 |
| Q.5 | (a) What is HTTPS? How it works? | 03 |
| | (b) Briefly discuss web security threats. | 04 |
| | (c) Write a brief note on X.509 certificate. | 07 |
| | OR | |
| Q.5 | (a) What is role of SSL? | 03 |
| | (b) What is SSH? How it works? | 04 |
| | (c) Write a short note on public key infrastructure | 07 |
