

GUJARAT TECHNOLOGICAL UNIVERSITY**BE- SEMESTER-VII (NEW) EXAMINATION – WINTER 2024****Subject Code:3173211****Date:30-11-2024****Subject Name: System 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) Differentiate between broadcast links and point-to-point links in network. | 03 |
| | (b) Explain VPN (Virtual Private Network) with figure. Also specify its advantages. | 04 |
| | (c) Prepare and explain diagram of generic layered network architecture. Show significance of layers, protocols, and interfaces in detail. | 07 |
| | | |
| Q.2 | (a) Draw diagram for original ARPANET design and explain it. | 03 |
| | (b) Prepare table for Six service primitives that provide a simple connection-oriented service with their meaning. | 04 |
| | (c) Provide details of PAN, LAN and WAN networks with necessary diagram and example. | 07 |
| OR | | |
| | (c) Give comparison of the OSI and TCP/IP reference models and also criticize both models. | 07 |
| | | |
| Q.3 | (a) Define three key objectives (CIA triad) of computer security. | 03 |
| | (b) What is Security service? List out five categories of Security services (X.800) and describe any four of them. | 04 |
| | (c) Define Active attacks. Elaborate given four categories of active attacks: masquerade, replay, modification of messages, and denial of service. | 07 |
| OR | | |
| Q.3 | (a) What are the differences between a monoalphabetic cipher and a polyalphabetic cipher? | 03 |
| | (b) What is steganography? Describe any example of steganography. | 04 |
| | (c) What is Security Mechanism? List out all Security Mechanism (X.800) and describe any six of them. | 07 |
| | | |
| Q.4 | (a) Distinguish between Stream Ciphers and Block Ciphers. | 03 |
| | (b) Encrypt plaintext: "WE ALL ARE ENGINEERS" using Rail fence cipher. (Consider rail depth=3) | 04 |
| | (c) Specify encryption rules for Playfair cipher. Perform encryption using Playfair cipher for the given Plain text: "System Security" and keyword: "Monarchy". | 07 |
| OR | | |
| Q.4 | (a) Show importance of Claude Shannon's concepts of confusion and diffusion for any cryptographic system. | 03 |
| | (b) Apply Vigenere cipher to encrypt Plaintext: "CYBER ATTACK ON WEBSITE" and consider key: "STRENGTH". | 04 |
| | (c) Generate cipher text of Plain text: "HIDE THE INFORMATION" using Hill cipher. Choose suitable key matrix. | 07 |

- Q.5** (a) What are the principal elements of a public-key cryptosystem? Explain those in short. **03**
- (b) Evaluate Diffie-hellman key exchange algorithm with example. **04**
- (c) Draw and explain complete general structure of DES algorithm. Describe expansion permutation step of DES with example. **07**

OR

- Q.5** (a) Prepare diagram for general format of X.509 certificate. **03**
- (b) Write about detail working of Digital Signature Algorithm (DSA). **04**
- (c) Create block diagram of structure of AES algorithm. Briefly describe MixColumns phase of AES with example. **07**
