

GUJARAT TECHNOLOGICAL UNIVERSITY**BE - SEMESTER-VII (NEW) EXAMINATION – SUMMER 2024****Subject Code: 3173211****Date: 22-05-2024****Subject Name: System and 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. Simple and non-programmable scientific calculators are allowed.

MARKS

- | | | |
|------------|---|-----------|
| Q.1 | (a) What is the difference between substitution and transposition cipher techniques? | 03 |
| | (b) Differentiate the OSI and TCP/IP in terms of architectural complexity. | 04 |
| | (c) What is RSA algorithm? Explain generation of public key, private key, and generation of cipher text through RSA with help of example? | 07 |
| | | |
| Q.2 | (a) What are the various types of firewalls? Explain anyone in detail. | 03 |
| | (b) Why security of web is necessary to protect data from unauthorized user? | 04 |
| | (c) Explain IP security architecture. Show how ESP works in transport and tunnel mode. | 07 |
| | | |
| OR | | |
| | (c) What is the need of Authentication? Explain different Authentication protocols. | 07 |
| | | |
| Q.3 | (a) Explain the terms integrity and confidentiality. | 03 |
| | (b) What are the properties that digital signature should have? | 04 |
| | (c) How does PGP create a secure network? Explain PGP in detail. | 07 |
| | | |
| OR | | |
| Q.3 | (a) Compare Active and Passive Attacks. | 03 |
| | (b) X.509 is a good security protocol. How this protocol is different from IPSec? | 04 |
| | (c) S/MIME and PGP are sister protocols. Study the two protocols and discuss the quality they share. | 07 |
| | | |
| Q.4 | (a) What is the key distribution? How can it be achieved? | 03 |
| | (b) What is Intrusion Detection? Write some measures used for Intrusion Detection. | 04 |
| | (c) Explain SSL protocol. List the service provided by SSL protocol. | 07 |
| | | |
| OR | | |
| Q.4 | (a) What is the difference between Symmetric and Asymmetric key encryption? | 03 |
| | (b) Confidentiality, Integrity and Availability are core attributes in security. Identify THREE (3) threats to a wireless network that could compromise security. | 04 |
| | (c) Explain Kerberos authentication system in detail. | 07 |
| | | |
| Q.5 | (a) Outline what it means for a cryptosystem to be scalable and how scalability is achieved. | 03 |
| | (b) Discuss 3D Secure protocol in brief. | 04 |
| | (c) Explain Diffie Hellman key Exchange in detail with an example? | 07 |

OR

- Q.5**
- | | | |
|------------|---|-----------|
| (a) | Compare Diffusion & Confusion. | 03 |
| (b) | Public Key Infrastructure (PKI) is security architecture/ framework that has been introduced to provide an increased level of confidence for exchanging information. Justify this sentence. | 04 |
| (c) | What is DDoS? How it is different from other security attacks? | 07 |
