

GUJARAT TECHNOLOGICAL UNIVERSITY**BE- SEMESTER-VII (NEW) EXAMINATION – WINTER 2024****Subject Code:3174202****Date:22-11-2024****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
Q.1	(a) Define the following terms: 1. Authentication 2. Repudiation 3. Integrity	03
	(b) Differentiate Substitution and Transposition techniques	04
	(c) What is a product cryptosystem. Explain with the help of an example.	07
Q.2	(a) Why is there a need for security at multiple levels in an organization? Explain with examples.	03
	(b) Differentiate between a block cipher and a stream cipher	04
	(c) Encrypt the message “Thing of beauty is joy forever” with key as MAGNETIC using Playfair cipher technique	07
	OR	
	(c) What are block cipher modes of operations? Explain any one in detail	07
Q.3	(a) Differentiate unconditionally secure and computationally secured algorithm	03
	(b) Explain Diffie Hellman key Exchange in detail with an example	04
	(c) What is an RSA algorithm explain it's working with the help of an example.	07
	OR	
Q.3	(a) What is an Avalanche Effect. Explain	03
	(b) Analyze the differences between Message Authentication Code (MAC), hash codes, and HMAC, focusing on their functionalities and applications	04
	(c) Create a detailed explanation of a single round of the DES algorithm, including well-labeled diagrams to illustrate the process	07
Q.4	(a) What is the importance of Fermat's and Euler's theorem in cryptography?	03
	(b) What is a digital signature? List out the properties of digital signature and enlist attacks against it.	04
	(c) Apply your understanding of the Shift Rows step in the AES algorithm to demonstrate its effect on the state matrix during encryption	07
	OR	
Q.4	(a) Describe Elgamal digital signature.	03
	(b) Explain various public key distribution techniques	04
	(c) Explain the role of Kerberos in user authentication	07
Q.5	(a) Analyze the role of key management in cryptography by examining its processes, challenges, and implications for data security	03
	(b) What is IP Security (IPSec) and what role does Encapsulating Security Payload (ESP) play in it	04
	(c) Define SSL and list its mechanisms for ensuring transport layer security.	07

OR

- | | | | |
|------------|------------|---|-----------|
| Q.5 | (a) | Give the applications of IP Security | 03 |
| | (b) | What are X.509 Certificates, and how are they used in Public Key Infrastructure (PKI) | 04 |
| | (c) | What are the main security threats to email communication, and how does S/MIME provide comprehensive email security | 07 |
