

GUJARAT TECHNOLOGICAL UNIVERSITY**BE - SEMESTER-VII (NEW) EXAMINATION – WINTER 2023****Subject Code:3174202****Date:04-12-2023****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 attacks:	03
	(i) Replay	
	(ii) Masquerade	
	(iii) Denial of Service	
	(b) Explore the OSI security architecture?	04
	(c) List and briefly define categories of security services and security mechanisms.	07
Q.2	(a) What are the differences between a mono-alphabetic cipher and a poly-alphabetic cipher?	03
	(b) Differentiate between a block cipher and a stream cipher.	04
	(c) Specify encryption rules of Playfair cipher and encrypt the following Message: "SUBSTITUTION" (Consider key = SECURITY).	07
	OR	
	(c) Encrypt the message "Information" using the Hill cipher algorithm with the key matrix: $\begin{bmatrix} 9 & 9 \\ 15 & 10 \end{bmatrix}$	07
	Show your calculations and the resultant cipher text.	
Q.3	(a) Which parameters and design choices determine the actual algorithm of a Feistel cipher?	03
	(b) Convert the given text "Engineering" into cipher text using Rail fence technique (Consider depth=3).	04
	(c) Prepare a block diagram of encryption process in DES. Elaborate expansion permutation step of DES algorithm.	07
	OR	
Q.3	(a) Find GCD (24140, 16762) using Euclidean algorithm.	03
	(b) Demonstrate the use of Euclidean algorithm with example.	04
	(c) Explain double DES with its merits and demerits.	07
Q.4	(a) Compare MD5 and SHA algorithm.	03
	(b) What are the five principal services provided by PGP?	04
	(c) Perform encryption and decryption using RSA algorithm for the following. p=7, q=11; e=17; m=8	07
	OR	
Q.4	(a) Differentiate MAC and Hash function.	03
	(b) Elaborate any two applications of X.509 Certificate.	04

(c) Show the purpose of Diffie-Hellman key exchange algorithm with example. 07

Q.5 (a) Give the applications of IP Security. 03

(b) What four requirements were defined for Kerberos? 04

(c) With a neat flowchart, Explain MD5 processing of a single 512 bit block. 07

OR

Q.5 (a) What changes in HMAC are required in order to replace one underlying hash function with another? 03

(b) What are some threats associated with a direct digital signature scheme? 04

(c) How can the signed data entity of S/MIME be prepared? Write down the steps. 07
