Roll No. _____

Pandit Deendayal Energy University

(Formerly Pandit Deendayal Petroleum University)

Re-Mid Semester Examination - November 2022

B. Tech. (Computer Science & Engineering)

Semester - V

Date: 10.11.2022

Course Name : Information Security **Time: 2 hours**

Course Code : 20CP304T **Max. Marks: 50**

Instructions:

1. Do not write anything other than your roll number on question paper.
2. Assume suitable data wherever essential and mention it clearly.
3. Writing appropriate units, nomenclature, and drawing neat sketches/schematics wherever required is an integral part of the answer.

Ques. No.	Description	Marks	CO Mapped	BL
Q. 1	Distinguish between the following: i. Confusion and Diffusion ii. Data authentication and Data confidentiality iii. Monoalphabetic and Polyalphabetic substitution cipher iv. Stream cipher and Block cipher v. Cryptography and Cryptanalysis	02*5	CO-1	L-2
Q. 2	i. Define Euler's Totient function. ii. State Euler's Theorem. iii. Write the Miller-Rabin algorithm to test a number for primality.	2+2+6	CO-2	L-3
Q. 3	i. Construct playfair matrix with the key "PLAYFAIR" ii. Demonstrate the playfair cipher by showing encryption on the plain text: "LET US MEET AT OUR USUAL PLACE" using the key in Q.3 i. iii. What is transposition cipher? Identify one advantage and one disadvantage of transposition cipher.	2+5+3	CO-3	L-4
Q. 4	i. What is the need of S-box? Explain two types of S-boxes. ii. What is the need of D-box? How many types of D-boxes can be used in modern block ciphers? Explain.	05*2	CO-3	L-2
	OR			
	Describe Advanced Encryption Standard.	10	CO-3	L-2
Q. 5	Discuss multiple encryption in DES. Mention the merits of opting for multiple DES.	05*2	CO-3	L-4
	OR			
	Describe the following modes and discuss the security issues in a) cipher feedback mode b) output feedback mode	05*2	CO-3	L-4