GYANMANJARI INNOVATIVE UNIVERSITY

GYANMANJARI INSTITUTE OF TECHNOLOGY

B.Tech.-Mid Semester Examination (MSE)-S2026

Enrollment No.: _____

Subject Code: BETIT16326 **Date: 18-03-2026**

Subject Name: Cryptography and Network Security **Semester: 06**

Time: 02:30 PM To 04:30 PM **Total Marks: 60**

Instructions:

1. **Question No. 1 is compulsory.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

			Marks
Q.1	(a)	Justify Need for Cryptography in Modern System.	05
	(b)	Discuss Man in Middle Attack.	05
	(c)	Explain single round of DES algorithm. Support your answer with neat sketches.	10
Q.2	(a)	What is public key cryptography? What are the principal elements of a public-key cryptosystem?	05
	(b)	Perform encryption and decryption using the RSA algorithm for p=5, q=11, e=3, M=9.	05
		OR	
	(b)	List down various modes of operations of block cipher and explain any three of them briefly.	05
	(c)	Elaborate AES encryption with neat sketches.	10
		OR	
	(c)	For Diffie-Hellman algorithm, two publicly known numbers are prime number 353 and primitive root of it is 3. A selects the random integer 97 and B selects 233. Compute the public key of A and B. Also compute common secret key.	10
Q.3	(a)	Explain Elgamal algorithm for digital signature.	05
	(b)	Write the Euclid's algorithm and show the steps of Euclid's algorithm to find gcd (401,700).	05
	(c)	Explain the triple DES scheme with two keys. Why not Double DES? What is a meet-in-the-middle attack?	10
		OR	
Q.3	(a)	Explain Cryptanalytic Attack in brief.	05
	(b)	Construct a Play fair matrix with the key "Trust" and encrypt the message "Be confident in yourself".	05
	(c)	Discuss four general categories of schemes for the distribution of public keys.	10