GYANMANJARI INNOVATIVE UNIVERSITY

Gyanmanjari Institute of Technology

B.Tech.- End Semester Examination (ESE)- Summer - 2026

Enrollment No.:_____ **Date: 16/05/2026**

Subject Code: BETIT16326 **Semester: 6**

Subject Name: Cryptography and Network Security **Total Marks: 100**

Time: 10:30AM To 01:30PM

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) Define the following terms: (i) Cryptography (ii) Cryptanalysis (iii) Brute-force attack	05
	(b) In a public key system using RSA, the cipher text intercepted is C=12 which is sent to the user whose public key is e=5, n=35. What is the plaintext M?	05
	(c) What is Substitution? Explain any 3 algorithms with example.	10
Q.2	(a) What is a Denial of Service (DoS) attack? How does it affect network availability?	05
	(b) Explain Chosen-Plaintext Analysis and Ciphertext-Only Analysis.	05
	OR	
	(b) Explain the working of Cipher Block Chaining Mode (CBC) and Counter Mode (CTR) with suitable diagrams and examples.	05
	(c) What are the different types security attack available in Cryptography?	10
	OR	
	(c) Justify how DES (Data Encryption standard) algorithm observes Fiestel structure. Discuss use of S-box in DES algorithm.	10
Q.3	(a) Why not Double DES? What is a meet-in-the-middle attack?	05
	(b) Explain Diffie Hellman key exchange algorithm with example.	05
	(c) What is a nonce? What is the difference between a session key and a master key?	10
	OR	
	(a) Discuss Man-in-the-Middle Attack.	05
	(b) What is digital signature? Explain Elgamal digital signature scheme in detail.	05

(c) Describe the architecture of Advanced Encryption Standard (AES) in details. 10

Q.4 (a) Explain Schnorr Digital Signature Scheme. 05

(b) Differentiate between hashing and encryption. What are the practical applications of hashing? 05

(c) Describe MAC? Explain HMAC algorithm in details. 10

OR

(a) Encrypt the message "Asymmetric key cryptography is fun" using Transposition cipher with key (3 2 6 1 5 4). 05

(b) Consider ElGamal cryptosystem in Z17 with generator 6. If the message is 13 and the randomness chosen is 10, then find the ciphertext computed using the public key 7. 05

(c) Describe the principle of digital signature algorithm (DSA). Explain the signing and verifying function in DSA. 10

Q.5 (a) Write the Euclid's algorithm and show the steps of Euclid's algorithm to find gcd (401,700). 05

(b) Differentiate between IDS and IPS. How does an IPS enhance network security? 05

(c) Explain Symmetric Key Distribution using Symmetric Encryptions. 10

OR

(a) Message authentication code and a one-way hash function? Write the basic uses of Message authentication code. 05

(b) Demonstrate the working SSL Record Protocol. 05

(c) Using diagram explain how RSA algorithm can be used to digitally sign the message. 10