Enrolment No./Seat No_____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE- SEMESTER–VI EXAMINATION – WINTER 2025

Subject Code:3161606 Date:17-11-2025

Subject Name:Cryptography and Network security

Time:02:30 PM TO 05:00 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)**	List and define any three security services.	**03**
	(b)	Define Cryptography and Steganography. Which technique (Cryptography or Steganography) is used in each of the following cases for confidentiality? 1) A student writes the answer to a test on a small piece of paper, rolls up the paper and inserts it in a ball-point pen, and passes the pen to another student. 2) To send a message, a spy replaces each character in the message with a symbol that was agreed upon in advance as the character's replacements.	**04**
	(c)	Discuss following attacks. 1) Brute force attack 2) Frequency analysis attack 3) Man in the middle attack 4) Active attack 5) Passive attack 6) Meet in the middle attack 7) Known plaintext attack	**07**
Q.2	**(a)**	Define (i) group (ii) Ring (iii) Field	**03**
	(b)	Let us assign numeric values to the uppercase alphabet (A=0, B=1, …., Z=25). We can now do modular arithmetic on the system using modulo 26. 1) What is (A+N) mod 26 in this system? 2) What is (X+6) mod 26 in this system? 3) What is (Y-5) mod 26 in this system? 4) What is (C-10) mod 26 in this system?	**04**
	(c)	Discuss Playfair Cipher. Construct a Playfair matrix with the key “engineering”. And encrypt the message “test this Balloon”.	**07**
		OR	
	(c)	Discuss encryption and decryption process in Vigenere cipher. Using the Vigenere cipher, encrypt the word “Life is full of surprises” using the key “health”.	**07**
Q.3	**(a)**	What is a hash function and what are its primary uses in cryptography?	**03**
	(b)	Describe the Electronic Codebook (ECB) mode and identify its main advantages and disadvantages.	**04**
	(c)	Describe the key structure of DES.	**07**
		OR	

Q.3	**(a)**	What is a Message Authentication Code (MAC) and what is its primary use in cryptography?	**03**
	(b)	Describe the operation of Cipher Feedback (CFB) mode and how it differs from CBC.	**04**
	(c)	Describe the key structure of AES.	**07**
Q.4	**(a)**	Describe the consequences of not using HTTPS on a website.	**03**
	(b)	Define the greatest common divisor of two integers. Using Euclidean algorithm find the greatest common divisor of 1) 88 and 220 2) 2n+1 and n, assume n is non-negative integer.	**04**
	(c)	Discuss RSA Algorithm in detail.	**07**

OR

Q.4	**(a)**	Explain the differences between TLS and SSL. Why is TLS preferred over SSL today?	**03**
	(b)	Define Multiplicative Inverse. Using Extended Euclidean algorithm find multiplicative inverse of 49 in GF (37).	**04**
	(c)	Describe the general process of establishing a shared secret using the Diffie-Hellman method.	**07**
Q.5	**(a)**	List the duties of a KDC.	**03**
	(b)	Compare and contrast symmetric and asymmetric encryption methods in the context of remote user authentication.	**04**
	(c)	Describe the process of creating and verifying a digital signature.	**07**

OR

Q.5	**(a)**	Describe the role of the Ticket Granting Ticket (TGT) in the Kerberos authentication process.	**03**
	(b)	Describe the purpose of following protocols defined in SSL 1) Handshake Protocol 2) ChangeCipherSpec Protocol 3) Alert Protocol 4) Record Protocol	**04**
	(c)	Explain the components of an X.509 certificate and the importance of each component.	**07**

****