Enrolment No./Seat No_____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE- SEMESTER– VI EXAMINATION – SUMMER 2026

Subject Code:3161606 Date:22-05-2026

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.**
   Simple and non-programmable scientific calculators are allowed.

			MARKS
Q.1	**(a)**	Define Cryptography, Cryptanalysis and Cryptology.	**03**
	(b)	Encrypt the following text with Caesar cipher: (Key=3) "Cryptography and Network Security".	**04**
	(c)	Discuss Public Key Cryptosystems with Applications.	**07**
Q.2	**(a)**	Define security attack, security mechanism and security services.	**03**
	(b)	Construct a playfair matrix with the key "moonmission" and encrypt the message "greet".	**04**
	(c)	Describe working of AES(Advance Encryption standard).	**07**
		OR	
	(c)	Discuss Data Encryption Standard with working structure.	**07**
Q.3	**(a)**	Find 3^{31} mod 7 using Fermat's little theorem.	**03**
	(b)	Find GCD(2740, 1760) using Euclidean algorithm. Show each intermediate result.	**04**
	(c)	Compare and contrast various block cipher mode of operations.	**07**
		OR	
Q.3	**(a)**	With the help of Euler Totient function find $\phi(15)$.	**03**
	(b)	What is Hash Function? Explain requirements for hash functions.	**04**
	(c)	List types of digital signature and discuss in detail Elgamal digital signature scheme.	**07**
Q.4	**(a)**	What is the difference between HTTP and HTTPS?	**03**
	(b)	In a public key system using RSA, the ciphertext intercepted is C=10 which is sent to the user whose public key is e=5, n=35. What is the plaintext M?	**04**
	(c)	Demonstrate the working of SSL Record Protocol with the help of necessary diagrams.	**07**
		OR	
Q.4	**(a)**	Explain X.509 authentication service.	**03**
	(b)	Find out inverse of 550 with extended Euclidean algorithm in Galois Field 1759.	**04**
	(c)	Explain Diffie Hellman scheme with diagram. For Diffie-Hellman algorithm, two publically known numbers are prime number 23 and primitive root of it is 9. A selects the random	**07**

integer 4 and B selects 3. Compute the public key of A and B. Also compute common secret key.

Q.5	**(a)**	Discuss MAC based on Block Ciphers.	**03**
	(b)	Discuss various ways of Distribution of Public Keys.	**04**
	(c)	Demonstrate the working of Kerberos Version 4 Authentication Dialogue with detailed steps.	**07**

OR

Q.5	**(a)**	Illustrate Man-in-Middle attack.	**03**
	(b)	Discuss MAC based on Hash Functions (HMAC).	**04**
	(c)	Consider a scenario where Prachi wants to send a secret message M and her signature to Prayag. Prachi takes help of Prayag to validate her digital signature, but does not want to reveal M to Prayag. Prayag performs the necessary steps to send Prachi ‘s messages to Pramod. Draw and explain this scenario using symmetric key cryptography.	**07**

****