Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VI (NEW) EXAMINATION – SUMMER 2022

Subject Code:3161606 Date:03/06/2022

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

			MARKS
Q.1	**(a)**	Define Cryptography and Cryptanalysis.	**03**
	(b)	Encrypt the following text with Caesar cipher: (Key=3) "Welcome to the course Information and Network security"	**04**
	(c)	Differentiate public key cryptography and symmetric key cryptography. Explain any one substitution method for symmetric key cryptography with example.	**07**
Q.2	**(a)**	What is the difference between passive and active security threats? List and briefly define categories of passive and active security attacks.	**03**
	(b)	Encrypt the message "security" using Hill Cipher with key (9 4 5 7)	**04**
	(c)	Explain four different stages of AES(Advance Encryption standard) structure.	**07**
		OR	
	(c)	Justify how DES(Data Encryption standard) algorithm observes Fiestel structure. Discuss use of S-box in DES algorithm.	**07**
Q.3	**(a)**	Find out the greatest common divisor GCD of 96256 and 432.	**03**
	(b)	Let p=11 and q=7. Then find multiplicative inverse of 13 modulo Φ(pq).	**04**
	(c)	Discuss need of block cipher mode of operations. Also explain various block cipher mode of operations.	**07**
		OR	
Q.3	**(a)**	What is message authentication? Explain the requirements of message authentication.	**03**
	(b)	Justify the importance of Authentication in Security. Demonstrate the working of Kerberos Version 4 Authentication Dialogue with detailed steps.	**04**
	(c)	What is digital signature? Explain Elgamal digital signature scheme in detail.	**07**
Q.4	**(a)**	What is HTTPS? How it works?	**03**
	(b)	Perform encryption and decryption using RSA algorithm for following: p=3;q=13,e=5;M=10	**04**
	(c)	Justify the Importance of SSL Handshake Protocol with detailed explanation.	**07**

OR

Q.4	**(a)**	Demonstrate the working SSL Record Protocol.	**03**
	(b)	Find out inverse of 12 with extended Euclidean algorithm in Galois Field 79.	**04**
	(c)	Explain Diffie Hellman scheme with diagram. For Diffie-Hellman algorithm, two publically known numbers are prime number 11 and primitive root of it is 2. A selects the random integer 9 and B selects 4. Compute the public key of A and B. Also compute common secret key.	**07**
Q.5	**(a)**	Illustrate the overall operation of HMAC. Define the terms.	**03**
	(b)	Explain the processing of a single block of SHA-1 algorithm in detail.	**04**
	(c)	Explain Kerberos in detail.	**07**

OR

Q.5	**(a)**	Explain X.509 authentication service.	**03**
	(b)	Explain Schnorr Digital Signature Scheme.	**04**
	(c)	Explain key distribution process using Key Distribution Center (KDC).	**07**

****