Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

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

Subject Code:3161606 Date:14-12-2022

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)**	Explain the following terms in brief: i) Confidentiality ii) Non-repudiation iii) Access Control.	**03**
	(b)	Construct a Play fair matrix with the key "Trust" and encrypt the message "Be confident in yourself".	**04**
	(c)	List down various modes of operations of block cipher and explain any three of them briefly.	**07**
Q.2	**(a)**	Encrypt the message "Coronavirus" using the Hill Cipher with the key- $\begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix}$	**03**
	(b)	Differentiate Following: i)Stream Cipher and block cipher ii)Active attack and Passive attack	**04**
	(c)	Explain single round of DES algorithm.	**07**
		OR	
	(c)	Explain Key Expansion in AES algorithm.	**07**
Q.3	**(a)**	Differentiate conventional encryption and public key encryption.	**03**
	(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?	**04**
	(c)	Explain SHA1 hashing algorithm in detail.	**07**
		OR	
Q.3	**(a)**	Alice meets Bob and says "Wshu H pz uva dvyrpun wyvwlysf. dl ohcl av tvcl av aol wshu I." If she is using Caesar Cipher, what does she want to convey?	**03**
	(b)	User A & B exchange the key using Diffie Hellman algorithm Assume public numbers P=17 G=2 and private values X=3 Y=7 respectively. Find the Public Value R1,R2 and key K of user A and B.	**04**
	(c)	Describe MAC? Explain HMAC algorithm in details.	**07**
Q.4	**(a)**	List and explain transposition techniques in cryptography.	**03**
	(b)	Write the Euclid's algorithm and show the steps of Euclid's algorithm to find gcd(401,700).	**04**
	(c)	Describe the principle of digital signature algorithm (DSA).Explain the signing and verifying function in DSA.	**07**
		OR	
Q.4	**(a)**	Explain replaying attack with example.	**03**
	(b)	Describe Elgamal digital signature.	**04**

	(c)	Define KDC? With the help of diagram explain how KDC do key distribution.	**07**
Q.5	**(a)**	What is the purpose of HTTPS?	**03**
	(b)	Write a short note on Secure Socket Layer.	**04**
	(c)	Draw and explain Kerberos protocol in details.	**07**

OR

Q.5	**(a)**	Define Following Terms: i) Group ii) Ring iii) Field	**03**
	(b)	Explain Public key Infrastructure in security.	**04**
	(c)	Explain X.509 authentication service.	**07**

****