Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII (NEW) EXAMINATION – SUMMER 2021

Subject Code:2170709 Date:04/08/2021

Subject Name:Information 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.**

Q.1	**(a)**	Differentiate asymmetric encryption with symmetric encryption.	**03**
	(b)	What is digital signature? What are the properties a digital signature should have?	**04**
	(c)	Why mode of operation is defined for block ciphers? Compare the block cipher modes of operation?	**07**
Q.2	**(a)**	What is brute force attack? Explain with an example.	**03**
	(b)	Define the terms: Diffusion, Confusion. How are these implemented in DES?	**04**
	(c)	Explain RSA algorithm in detail with suitable example.	**07**
		OR	
	(c)	Explain the Deffie Hellman key exchange scheme in detail with an example.	**07**
Q.3	**(a)**	How can we find out GCD of two numbers using Euclid algorithm? Explain with the help of example.	**03**
	(b)	Perform encryption and decryption using RSA algorithm for following: p=3;q=13,e=5;M=10	**04**
	(c)	Briefly explain the AES encryption structure and discuss its transformation functions.	**07**
		OR	
Q.3	**(a)**	What is a trap-door one way function? What is its use in cryptography?	**03**
	(b)	Let the keyword in playfair cipher is “keyword”. Encrypt a message “come to the window” using playfair cipher.	**04**
	(c)	Explain the single round of DES algorithm	**07**
Q.4	**(a)**	List the security services provided by digital signature.	**03**
	(b)	What characteristics are needed in a secure hash function?	**04**
	(c)	Briefly explain HMAC algorithm.	**07**
		OR	
Q.4	**(a)**	What is MAC? Why it is required?	**03**
	(b)	Explain the process of public key distribution using public key authority.	**04**
	(c)	List out the main features of the SHA-512 cryptographic hash function and briefly explain its compression function.	**07**
Q.5	**(a)**	What is SSH? How it works?	**03**
	(b)	Explain the process of secret key distribution with confidentiality and authentication.	**04**
	(c)	What is Kerberos? How it works? Explain in detail.	**07**
		OR	
Q.5	**(a)**	What is digital certificate? What is the purpose of X.509?	**03**
	(b)	What is HTTPS? How it works?	**04**
	(c)	Write and explain the Digital Signature Algorithm.	**07**

****