Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

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

Subject Code:2170709 Date:05-01-2023

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

Q.1	**(a)**	What is cryptography? What are the applications of it?	**03**
	(b)	Compare block cipher modes of operation.	**04**
	(c)	Briefly explain the public key encryption system.	**07**
Q.2	**(a)**	What is brute force attack? Explain with an example.	**03**
	(b)	What is diffusion and confusion? How are they used in DES?	**04**
	(c)	Explain RSA algorithm with suitable example.	**07**
		OR	
	(c)	Explain the single round of DES algorithm.	**07**
Q.3	**(a)**	Compare symmetric key encryption with asymmetric key encryption	**03**
	(b)	Explain key distribution process using Key Distribution Center (KDC).	**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)	What is digital signature? What are the properties a digital signature should have?	**04**
	(c)	Explain the Deffie Hellman key exchange scheme in detail with an example.	**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)	What is Kerberos? How it works? Explain in detail.	**07**
		OR	
Q.4	**(a)**	What is SSL? Which security services do it offers?	**03**
	(b)	Explain the process of public key distribution using public key authority.	**04**
	(c)	Define the Digital Signature Standard (DSS) scheme based on Digital Signature Algorithm (DSA) and briefly discuss it.	**07**
Q.5	**(a)**	What is MAC? Why it is required?	**03**
	(b)	Briefly discuss the working of SSL Record Protocol.	**04**
	(c)	Briefly explain HMAC algorithm.	**07**
		OR	
Q.5	**(a)**	What is HTTPS? How it works?	**03**
	(b)	Briefly discuss web security threats.	**04**
	(c)	Briefly explain SHA algorithm.	**07**

****