Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII (NEW) EXAMINATION – WINTER 2023

Subject Code:3170720 Date:19-12-2023

Subject Name: Information 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)**	Explain Caesar Cipher technique with Example.	**03**
	(b)	Explain with example any two principles of Security.	**04**
	(c)	Define the following terms related to Information Security: i. Cryptography ii. Cryptanalysis iii. Sniffing iv. Spoofing v. Interception vi. Fabrication vii. Masquerade	**07**
Q.2	**(a)**	Differentiate between Block Cipher and Stream Cipher.	**03**
	(b)	Explain One-Time Pad Substitution technique with the help of example.	**04**
	(c)	Explain in detail single round of DES algorithm.	**07**
		OR	
	(c)	Explain in detail single round of AES algorithm.	**07**
Q.3	**(a)**	What is meet in the middle attack?	**03**
	(b)	Explain Electronic Code Book and Cipher Block Chaining Mode in detail.	**04**
	(c)	In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 17 and primitive root = 5. If Alice's secret key is 4 and Bob's secret key is 6, what is the secret key they exchanged? Explain it with proper steps.	**07**
		OR	
Q.3	**(a)**	Define Hash function in Cryptographic and list its application.	**03**
	(b)	Differentiate between Symmetric key cryptography and Asymmetric key cryptography.	**04**
	(c)	Explain RSA algorithm with example in detail.	**07**
Q.4	**(a)**	What is MAC? State the main difference between MAC & Hash function.	**03**
	(b)	Explain hill cipher algorithm with example.	**04**
	(c)	Explain Message Digest Generation Using SHA-512.	**07**
		OR	
Q.4	**(a)**	Explain the types of attacks are addressed by message authentication?	**03**
	(b)	What are the requirements for a Cryptographic Hash Function?	**04**
	(c)	Explain with the diagrams Basic Uses of Message Authentication code (MAC).	**07**
Q.5	**(a)**	What is the role of Key Distribution Centre? Give the several techniques for the distribution of public keys.	**03**
	(b)	Give the difference between Session key and Master key.	**04**
	(c)	Explain with neat diagram Digital Signature Algorithm.	**07**
		OR	

Q.5	**(a)**	What is the role of AS and TGS in Kerberos?	**03**
	(b)	Draw X.509 certificate format.	**04**
	(c)	Explain SSL Architecture with neat diagram.	**07**