Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

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

Subject Code:3170720 Date:12-01-2023

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)**	List and explain various types of attacks?	**03**
	(b)	What is Hill Cipher? Generate a Cipher text for plain text "hi" using key "jefh" using hill cipher.	**04**
	(c)	List various mode of cryptographic operation. Explain any one with the help of diagram.	**07**
Q.2	**(a)**	List advantages of asymmetric cryptography over symmetric key cryptography.	**03**
	(b)	Explain encryption and decryption of RSA algorithm	**04**
	(c)	Explain avalanche effect in DES algorithm.	**07**
		OR	
	(c)	Does DES algorithm Secure? Discuss security of DES.	**07**
Q.3	**(a)**	List the requirements of public key cryptography.	**03**
	(b)	List application of RSA algorithm.	**04**
	(c)	Discuss security of Diffie Hellman Key exchange algorithm with the help of example.	**07**
		OR	
Q.3	**(a)**	Using diagram explain how RSA algorithm can be used to digitally sign the message.	**03**
	(b)	Compute public key and private key of RSA with p-11, q=17 and e = 7.	**04**
	(c)	Compute Inverse of b=550 mod m=1759 using Euclid algorithm	**07**
Q.4	**(a)**	Explain cryptanalysis attack on cryptographic hash function.	**03**
	(b)	Explain pre-image resistance and second pre-image resistance.	**04**
	(c)	Write a note on birthday attack.	**07**
		OR	
Q.4	**(a)**	What is collision resistance property of hash function?	**03**
	(b)	Explain a simple hash function and its limitation.	**04**
	(c)	What is block size and message digest size in SHA 512? With the help of diagram explain a round of SHA-512 algorithm	**07**
Q.5	**(a)**	Explain mutual authentication using symmetric key cryptography	**03**
	(b)	Compare authentication and authorization.	**04**
	(c)	Explain Schnorr algorithm for digital signature.	**07**
		OR	
Q.5	**(a)**	Explain one way authentication using symmetric key cryptography	**03**
	(b)	Compare link encryption and end to end encryption	**04**
	(c)	Explain NIST Digital signature algorithm	**07**

****