Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

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

Subject Code:2170709 Date:03/06/2022

Subject Name:Information 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)**	Differentiate data confidentiality and data integrity.	**03**
	(b)	Differentiate Caesar cipher and mono alphabetic cipher.	**04**
	(c)	Explain vigenere cipher with example.	**07**
Q.2	**(a)**	Explain working of rotor machine.	**03**
	(b)	Show encryption using columnar transposition Cipher.	**04**
	(c)	Show various blocks of simplified DES (S-DES).	**07**
		OR	
	(c)	Explain fiestal structure for multi round encryption.	**07**
Q.3	**(a)**	Explain encryption and decryption using RSA.	**03**
	(b)	Explain Digital signature generation using RSA key pair.	**04**
	(c)	Differentiate Hash code with MAC code.	**07**
		OR	
Q.3	**(a)**	How Diffie Hellman algorithm is used for key exchange?	**03**
	(b)	Explain problem in key exchange using Diffie Hellman algorithm.	**04**
	(c)	Explain use of KDC with proper diagram.	**07**
Q.4	**(a)**	How digital public key certificate is useful in public key distribution.	**03**
	(b)	How encryption is done using triple DES with two keys.	**04**
	(c)	Show steps for authentication between two different Kerberos realm.	**07**
		OR	
Q.4	**(a)**	What is role of SSL?	**03**
	(b)	Why security is required in public key distribution.	**04**
	(c)	Explain Digital Signature Algorithm signature generation and verification process.	**07**
Q.5	**(a)**	Explain required property of Hash code.	**03**
	(b)	Explain counter mode of DES operation.	**04**
	(c)	Write a short note on public key infrastructure.	**07**
		OR	
Q.5	**(a)**	Explain MAC code generation using block cipher.	**03**
	(b)	Explain HTTPs.	**04**
	(c)	How MAC code is generated using HMAC algorithm?	**07**

****