GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VIII(NEW)   EXAMINATION – SUMMER 2019

Subject Code: 2183202   **Date:17/05/2019**

Subject Name: Systems 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.**

			MARKS
Q.1	(a)	Give comparative note of LAN, MAN and WAN.	03
	(b)	Explain conventional cryptosystem model with diagram.	04
	(c)	Explain the OSI reference model with its applications.	07
Q.2	(a)	Write a short note on Steganography.	03
	(b)	Write down the steps of RSA algorithm.	04
	(c)	Define security attack. Explain the types of it in detail.	07
		OR	
	(c)	Explain four general categories of schemes for the distribution of public keys.	07
Q.3	(a)	Explain Avalanche Effect and Timing Attack.	03
	(b)	List and briefly define categories of security services.	04
	(c)	Explain single round function of DES with suitable diagram.	07
		OR	
Q.3	(a)	What do you mean by Stream Cipher and Block Cipher? Differentiate both.	03
	(b)	Use playfair algorithm with key "hello world" and encrypt the text "hide the gold".	04
	(c)	Draw and explain Feistel's structure for encryption and decryption.	07
Q.4	(a)	What is the need of segmentation and reassembly function in PGP?	03
	(b)	Explain X.509 authentication service.	04
	(c)	Write a detailed note on S/MIME.	07
		OR	
Q.4	(a)	Explain Man-in-the-Middle Attack.	03
	(b)	Discuss the parameters that defines a Security Association (SA).	04
	(c)	Explain Kerberos in detail.	07
Q.5	(a)	Give the importance of detached Signature?	03
	(b)	Explain the SSL Alert protocol.	04
	(c)	Explain the types of Firewall.	07
		OR	
Q.5	(a)	What is the role of compression in the operation of a virus?	03
	(b)	Explain Digital Immune System.	04
	(c)	Define intruders? Explain intrusion detection technique in web security.	07

****