Seat No.: _____   Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY
MCA INTEGRATED– SEMESTER-VIII EXAMINATION –SUMMER-2020

Subject Code: 4480603   **Date:06-11-2020**
Subject Name: 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.

Q.1	**(a)**	1.	Explain any three challenges of computer security. (3)	**07**
		2.	Explain a model for network security in detail. (4)	
	(b)	1.	Explain the use of random and pseudorandom numbers in encryption. (5)	**07**
		2.	Write any two advantages of counter mode. (2)	
Q.2	**(a)**		What is the need of hash function? Explain steps of SHA-512 algorithm with suitable diagram.	**07**
	(b)		Explain RSA public key cryptography algorithm taking suitable example. Show encryption and decryption process for example.	**07**
			OR	
	(b)		Explain AES symmetric encryption algorithm in detail with suitable diagram.	**07**
Q.3	**(a)**	1.	Explain KDC and its operations. (4)	**07**
		2.	Explain the role of TGT, TGS and AS with respect of kerberos V4. (3)	
	(b)		Explain SSL record protocol in detail with suitable diagram.	**07**
			OR	
Q.3	**(a)**	1.	Explain the use of public key certificates. (2)	**07**
		2.	Explain X.509 V2 certificates in detail. (5)	
	(b)		Explain pseudorandom function and cryptographic computations for TLS with suitable diagram.	**07**
Q.4	**(a)**		Explain 802.11 protocol architecture in detail using suitable diagram.	**07**
	(b)		Explain the two reasons to grow PGP explosively. (2)	**07**
			Explain confidentiality and authentication operation of PGP using suitable diagram. (5)	
			OR	
Q.4	**(a)**		Explain ESP packet format in detail using suitable diagram.	**07**
	(b)		Explain different fields associated in general format PGP message with diagram.	**07**
Q.5	**(a)**	1.	Differentiate between transport mode SA and tunnel mode SA functionality for AH, ESP and ESP with authentication. (3)	**07**
		2.	Explain classes of intruders. (4)	
	(b)		Explain the types of firewall in detail using suitable diagram.	**07**
			OR	
Q.5	**(a)**		Explain the three parts and four phases of computer virus.	**07**
	(b)		Explain password selection strategies in detail.	**07**

****