GUJARAT TECHNOLOGICAL UNIVERSITY
MCA INTEGRATED– SEMESTER VIII - EXAMINATION –WINTER-2022

Subject Code: 4480603   **Date: 20/12/2022**
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)**	Answer the following	**07**
		1) Define Active attacks.	
		2) The secret key for the sender and the receiver is same in which kind of encryption?	
		3) What is the size of the message digest for SHA-512?	
		4) What is Kerberos?	
		5) Give the difference between transport mode and tunnel mode.	
		6) What are the three classes of intruders?	
		7) Explain what do you understand by data integrity?	
	(b)	Explain in detail security attacks.	**07**
Q.2	**(a)**	Explain the Feistel Cipher structure.	**07**
	(b)	Differentiate between AES and DES. Also explain Triple DES in detail.	**07**
		OR	
	(b)	Explain the various cipher block modes of operations.	**07**
Q.3	**(a)**	1) Explain the basic five ingredients of Symmetric Encryption principles.	**04**
		2) What do you understand by digital signatures?	**03**
	(b)	What is secure hash function? Explain the properties of a good hash function.	**07**
		OR	
Q.3	**(a)**	Explain RC4 algorithm.	**07**
	(b)	What is public key cryptography? Explain any one public key cryptography algorithm in detail.	**07**
Q.4	**(a)**	Explain the IEEE 802 Protocol architecture.	**07**
	(b)	Write a note on SSL record protocol.	**07**
		OR	
Q.4	**(a)**	What do you mean by port forwarding? Explain local forwarding and remote forwarding.	**07**
	(b)	What is ESP(Encapsulating Security Payload) used for? Explain the ESP format.	**07**
Q.5	**(a)**	Write a note on PGP (Pretty Good Privacy).	**07**
	(b)	What do you understand by intrusion? Explain how statistical anomaly Detection does instruction detection?	**07**
		OR	
Q.5	**(a)**	List out the various categories of malicious software. Explain any two in detail.	**07**
	(b)	Define a Firewall. Explain packet filtering firewall in detail.	**07**

****