Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

ME - SEMESTER– III • EXAMINATION – SUMMER 2015

Subject Code: 2735302 **Date: 01/05/2015**

Subject Name: Security in Wireless and Mobile System

Time: 2:30 pm to 5:00 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)**	Explain differences between Symmetric Key and Asymmetric Key Cryptography (Seven points).	**07**
	(b)	Explain active attack and passive attack in detail with relevant examples.	**07**
Q.2	**(a)**	What is difference between DES and 3DES and explain 3DES in detail.	**07**
	(b)	What is digital certificate? Explain Diffie Hellman key exchange algorithm.	**07**
		OR	
	(b)	What are intrusions? Discuss intrusion detection system.	**07**
Q.3	**(a)**	Explain Elliptic Curve Cryptography algorithm with example.	**07**
	(b)	Perform encryption and decryption using the RSA algorithm for the following: p=5, q=12, e=3, M=9 [p, q = prime number, M = plain text, and e is relatively prime to ű(pq)]	**07**
		OR	
Q.3	**(a)**	What is Message Authentication Code? Explain in detail.	**07**
	(b)	Explain block cipher and stream cipher in detail.	**07**
Q.4	**(a)**	Explain distributed system security in brief.	**07**
	(b)	What is various security solution constraints in MANET? Discuss various security aspects in MANET.	**07**
		OR	
Q.4	**(a)**	Why security is important for distributed systems? Discuss various security issues for distributed systems.	**07**
	(b)	Discuss the basic guidelines for designers of security components of distributed systems.	**07**
Q.5	**(a)**	List out four classification of network attacks, and explain each in detail.	**07**
	(b)	What is difference between spoofing and snooping? Explain IP spoofing in detail.	**07**
		OR	
Q.5	**(a)**	What is DoS attack? List out and explain various types of DoS attacks in detail. What are the consequences of DoS attack in MANET?	**07**
	(b)	Explain hashing in detail. Differentiate between SHA1 and MD5 algorithm.	**07**

****