Seat No.: ________ Enrolment No.______________

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E. - SEMESTER – III • EXAMINATION – WINTER • 2014

Subject code: 2735302 **Date: 25-11-2014**

Subject Name: Security in Wireless and Mobile System

Time: 02:30 pm - 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)**	Explain main differences between Symmetric Key and Asymmetric Key Algorithms with an example.	**07**
	(b)	What is PKI? What are the components of PKI? Explain Registration Authority in detail.	**07**
Q.2	**(a)**	What is cryptography? What are the goals of cryptography? Explain Strength of cryptosystems	**07**
	(b)	What is symmetric key cryptography? List out various symmetric key algorithms and explain Caesar cipher in detail.	**07**
		OR	
	(b)	What is asymmetric key cryptography? Explain ECC algorithm in detail.	**07**
Q.3	**(a)**	Explain one time Pad in detail. What are the practical issues of this algorithm?	**07**
	(b)	If plain text is ñhackerò, and key value is ñtestteò, what will be the cipher text? Use vigenere cipher.	**07**
		OR	
Q.3	**(a)**	P and Q are two prime numbers. P=7, and Q=17. Take public key E=5. If plain text value is 5, then what will be cipher text value according to RSA algorithm? Explain each steps in detail.	**07**
	(b)	What is hashing? Differentiate between SHA1 and MD5 algorithm.	**07**
Q.4	**(a)**	Populate key matrix for key value ñPLAYFAIR EXAMPLEò using playfair cipher algorithm.	**07**
	(b)	Explain the digital signature in security field.	**07**
		OR	
Q.4	**(a)**	What is Message Authentication Code? Explain in detail.	**07**
	(b)	What is malware? Clarify the difference between virus, worm and Trojan.	**07**
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 block cipher and stream cipher in detail	**07**
		OR	
Q.5	**(a)**	Explain active attack and passive attack in detail with relevant examples.	**07**
	(b)	What is Pharming attack? How it could be hazardous in wireless Networking scenario?	**07**

****