Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

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

Subject Code: 725104 **Date: 29-11-2014**

Subject Name: PKI Biometrics

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)**	Differentiate between active attacks and passive attacks with example.	**07**
	(b)	Discuss stream cipher and Why is it not desirable to reuse a stream cipher key?	**07**
Q.2	**(a)**	Explain IPSec and L2TP protocols.	**07**
	(b)	How Biometric is most secure way of authentication? Also discuss skin scans.	**07**
		OR	
	(b)	Briefly describe the Shift Rows and Byte Substitution layers of Rijndael	**07**
Q.3	**(a)**	Show that the transposition cipher is vulnerable to a known plaintext attack.	**07**
	(b)	What types of information might be derived from a traffic analysis attack?	**07**
		OR	
Q.3	**(a)**	List approaches to dealing with replay attack.	**07**
	(b)	What is secure Email Implementation? explain	**07**
Q.4	**(a)**	Why do the Stream Ciphers seem to be inherently weaker than the Block Ciphers?	**07**
	(b)	What are the ways in which secret keys can be distributed to two communicating parties?	**07**
		OR	
Q.4	**(a)**	Discuss legal issues of Network Security.	**07**
	(b)	What are the basic components of PKI infrastructure?	**07**
Q.5	**(a)**	What are the advantages of PKI approach?	**07**
	(b)	Compare DES, AES and RSA encryption algorithm by comparing their implementation complexities for encryption, time for decryption, the key length, block size.	**07**
		OR	
Q.5	**(a)**	Explain Diffie-Hellman algorithm.	**07**
	(b)	Discuss single sign on solution.	**07**

****