Seat No.: ________ Enrolment No.___________

GUJARAT TECHNOLOGICAL UNIVERSITY

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

Subject Code: 725104 **Date: 12-06-2014**
Subject Name: PKI and Biometric
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 various types of attacks on Encrypted messages, along with known information to cryptanalyst.	**07**
	(b)	Differentiate the following: 1. Symmetric and Asymmetric Key Cryptography. 2. Link and End to End encryption.	**07**
Q.2	**(a)**	Construct a playfair matrix with the key ñPLAYFAIREXAMPLEò. Generate the cipher text for the plaintext ñMY NAME IS ATULò.	**07**
	(b)	Explain single round function of DES with suitable diagram.	**07**
		OR	
	(b)	What are the important parameters to be taken care in order to realize the feistel cipher structure? List and explain them.	**07**
Q.3	**(a)**	Explain Advance Encryption Standard (AES) with suitable diagram.	**07**
	(b)	What are the different modes of block cipher operation? Explain any two.	**07**
		OR	
Q.3	**(a)**	Explain the Key Distribution Scenario in detail.	**07**
	(b)	Give steps of RSA algorithm. Perform encryption using RSA algorithm for p=3,q=11, e=7 and m=5.	**07**
Q.4	**(a)**	Give steps of Diffie-Hellman key exchange algorithm. Explain man-in-the middle attack related to the scheme.	**07**
	(b)	What do you mean by Digital Signature? Explain the Digital Signature Standard.	**07**
		OR	
Q.4	**(a)**	Draw and explain PKIX Architectural Model and PKIX management functions.	**07**
	(b)	What is Message Authentication Code (MAC)? Describe the three situations in which MAC is used?	**07**
Q.5	**(a)**	Explain transmission and reception of PGP message with diagram.	**07**
	(b)	Explain Single Sign-on Solution.	**07**
		OR	
Q.5	**(a)**	Explain different Biometric Techniques.	**07**
	(b)	Discuss legal issues in network Security.	**07**

****