Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

ME - SEMESTER– II (Old course)• REMEDIAL EXAMINATION – SUMMER 2015

Subject Code: 725104 **Date:29/05/2015**

Subject Name: PKI AND BIOMETRICS

Time: 2:30 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)**	What are the basic principles of cryptography? Give the model of cryptography system and explain role of each element.	**07**
	(b)	Differentiate the following: 1. Confusion and diffusion 2. ShiftRows and RotWord	**07**
Q.2	**(a)**	Construct a playfair matrix with the key ñMONARCHYò. Generate the cipher text for the plaintext ñBALLOONò.	**07**
	(b)	Explain differential and linear Cryptanalysis.	**07**
		OR	
	(b)	Draw and explain Feistel cipher structure.	**07**
Q.3	**(a)**	Explain S-box generation process in AES.	**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 and discuss four approaches to attack RSA algorithm.	**07**
Q.4	**(a)**	Explain Double DES and meet-in-the-middle attack on it.	**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.	**07**
	(b)	Explain SHA-512.	**07**
Q.5	**(a)**	Describe PGP cryptographic functions with diagrams.	**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**

****