Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

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

Subject code: 2725104 **Date: 29-11-2014**

Subject Name: PKI and 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)**	What are the core components of PKI?	**07**
	(b)	Discuss certificates, certificate authorities and registration authorities.	**07**
Q.2	**(a)**	Define encryption and explain types encryption?	**07**
	(b)	Explain cryptosystem.	**07**
		OR	
	(b)	What are the differences between symmetric and asymmetric cryptography?	**07**
Q.3	**(a)**	How diffusion and Confusion works in cryptographic system.	**07**
	(b)	Explain digital signature. What are some threats associated with a direct digital signature scheme	**07**
		OR	
Q.3	**(a)**	Discuss Cryptographic issues.	**07**
	(b)	What are the key exchange algorithms?	**07**
Q.4	**(a)**	Discuss encryption with block ciphers.	**07**
	(b)	What is substitution cipher?	**07**
		OR	
Q.4	**(a)**	Explain cipher text attack.	**07**
	(b)	What is two factor authentication ?	**07**
Q.5	**(a)**	Differentiate between hashing and encryption algorithm	**07**
	(b)	How do you differentiate message confidentiality from message integrity? Can you have one without the other? Justify your answer.	**07**
		OR	
Q.5	**(a)**	How do you differentiate message confidentiality from message integrity? Can you have one without the other? Justify your answer.	**07**
	(b)	What do you mean by biometric authentication?	**07**

****