Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

ME – SEMESTER II (NEW) – • EXAMINATION – SUMMER 2016

Subject Code: 3725104 **Date: 31/05/2016**

Subject Name: PKI and Biometrics

Time:10:30 am to 01:00 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 stream and block cipher modes in detail.	[7]
	(b)	How many types of attack in network security? Explain with proper diagram.	[7]
Q.2	(a)	Write a short note on IP SEC architecture.	[7]
	(b)	What do you mean by non- repudiation? Explain non-repudiation using public key and secret key.	[7]
		OR	
	(b)	Discuss legal issues of Network security.	[7]
Q.3	(a)	Discuss issues in PKI Deployment	[7]
	(b)	What is certificate? Explain x.509 in detail.	[7]
		OR	
Q.3	(a)	Explain Digital signature standard in detail.	[7]
	(b)	Explain RSA Algorithm and its attack in detail.	[7]
Q.4	(a)	Discuss issues with secure email in detail.	[7]
	(b)	Explain advantages and drawback of biometric.	[7]
		OR	
Q.4	(a)	Give comparison between AES and DES algorithm.	[7]
	(b)	Explain PKI components and its functions in detail.	[7]
Q.5	(a)	Give approaches to share a secret key and explain briefly	[7]
	(b)	Explain what is the role of single sign on in authentication technologies?	[7]
		OR	
Q.5	(a)	Explain Diffie - Hellman key exchange algorithm in detail	[7]
	(b)	Explain types of Biometric Techniques briefly.	[7]

.**********