Seat No.: _____ *Enrolment No._____*

GUJARAT TECHNOLOGICAL UNIVERSITY

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

Subject code: 710104N **Date: 24-06-2014**

Subject Name: Information Security

Time: 10.30 am – 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 Caeser cipher, Play-fair cipher, and Rail-fence cipher with Example.	**07**
	(b)	Explain Security services in X.800.	**07**
Q.2	**(a)**	What is digital signature? What requirements should a digital signature scheme satisfy? Explain direct and arbitrated digital signature.	**07**
	(b)	Explain DES Algorithm.	**07**
		OR	
	(b)	Explain AES Algorithm.	**07**
Q.3	**(a)**	Write the Euclid and extended Euclid algorithm and Fermatôs theorem and with its use.	**07**
	(b)	Explain server-level web threats like repudiation, information disclosure, evaluation of privileges, and denial of service.	**07**
		OR	
Q.3	**(a)**	Explain Blowfish Symmetric Block cipher. Specify the key size for Blowfish.	**07**
	(b)	Explain Network IDs and Host IDs with their issues.	**07**
Q.4	**(a)**	Explain the RSA algorithm.	**07**
	(b)	Explain the Key Distribution scenario in public key Encryption.	**07**
		OR	
Q.4	**(a)**	Explain a Message Authentication Code. What is the difference between a message authentication code and a one-way hash function?	**07**
	(b)	Explain diffusion and confusion. What is difference between diffusion and confusion? How are they important to make algorithm strong?	**07**
Q.5	**(a)**	Explain SSL Handshake protocol mechanism.	**07**
	(b)	Explain the server level E-mail threats.	**07**
		OR	
Q.5	**(a)**	Compare link and end-to-end encryption and discuss factors deciding choice between them.	**07**
	(b)	Explain three different types of firewalls.	**07**

****