Seat No.: _____ *Enrolment No._____*

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E. - SEMESTER – I • EXAMINATION – WINTER • 2013

Subject code: 710104N **Date: 06-01-2014**

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 types of firewall and explain its working and methods.	**07**
	(b)	What are the contents of DNS query and reply messages.	**07**
Q.2	**(a)**	Explain the key generation in DES algorithm.	**07**
	(b)	Explain and compare link Vs. end-to-end encryption.	**07**
		OR	
	(b)	Explain types of Intrusion Detection System.	**07**
Q.3	**(a)**	List three general approaches to deal with replay attacks.	**07**
	(b)	Explain client level E-mail threats.	**07**
		OR	
Q.3	**(a)**	What is digital signature? What requirements should a digital signature scheme satisfy? Explain direct and arbitrated digital signature.	**07**
	(b)	Explain RSA algorithm in detail.	**07**
Q.4	**(a)**	Give Fermat's theorem and its importance in public-key cryptography.	**07**
	(b)	Explain MD5 Algorithm and how it differs from MD4.	**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)	(i) How is the S-box constructed in Advanced Encryption Standard?	**04**
		(ii) Write extended Euclidean algorithm to find multiplicative inverse.	**03**
Q.5	**(a)**	Explain server-level web threats like repudiation, information disclosure, evaluation of privileges, and denial of service.	**07**
	(b)	Explain (i) anomaly based misuse detection pattern (ii) purpose of NAT.	**07**
		OR	
Q.5	**(a)**	What is poly-alphabetic Ciphers? How can it be broken?	**07**
	(b)	Explain the digital signature algorithm.	**07**

****