Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

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

Subject code: 710104N **Date: 17-06-2013**

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)**	(I) When system administrator trusts the internal users, what type of fire wall is to be used? What are its limitations and how is to overcome these difficulties?	**04**
		(II) How will you enhance the ability of a system to defend against intruders and malicious programs?	**03**
	(b)	Define the following terms and give the real example of each of them: Security attack, Security mechanism and Security service.	**07**
Q.2	**(a)**	(I) For what purpose Euclidean algorithm is used? Explain the algorithm.	**04**
		(II) Explain the Blum Blum Shub Generator.	**03**
	(b)	What is meet-in-middle attack? Explain triple DES with two keys.	**07**
		OR	
	(b)	Explain the working of Hill cipher with proper example. Give its limitations.	**07**
Q.3	**(a)**	What are Digital Signature Algorithms and show how signing and verification is done using DSS.	**07**
	(b)	Give the Feistel cipher structure and give its design criteria.	**07**
		OR	
Q.3	**(a)**	Explain the following terms with proper example. 1. Digital signature 2. Replay attacks	**07**
	(b)	Why it is not desirable to reuse a stream cipher key? Explain the RC4 algorithm.	**07**
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 the Single Round of DES Algorithm with diagram.	**07**
		OR	
Q.4	**(a)**	What characteristics are needed in a secure hash function? Discuss Birthday attack and its signification.	**07**
	(b)	Write the four possible approaches of attacking RSA algorithm. Discuss the timing attack in detail and show the countermeasures that can be used.	**07**
Q.5	**(a)**	(I) Write the server level threats.	**04**
		(II) How can an E-mail be spoofed?	**03**
	(b)	What do you mean by intrusion detection? Explain the anomaly and pattern base intrusion detection system.	**07**
		OR	
Q.5	**(a)**	(I) Explain the phishing attacks.	**04**
		(II) Write the six ingredients of public key encryption scheme.	**03**
	(b)	Explain dual homed host, bastion host and screened host. Explain split screened subnet.	**07**

****