Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M.E Sem-I Remedial Examination January /February-2011

Subject code: 710104 Subject Name: Information Security

Date: 02 /02 /2011 Time: 02.30 pm – 05.00 pm

Total Marks: 60

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

Q.1	**(a)**	1. Explain Data Integrity and nonrepudiation security services.	**03**
		2. Write the common ways in which attackers threaten client level security.	**03**
	(b)	1. Write a snort rule to log tcp traffic from priveleged ports less than or equal to 1024 going to ports greater than or equal to 500.	**02**
		2. What is the use of net config command?	**02**
		3. What is the difference between direct and arbitrated digital signature?	**02**
Q.2	**(a)**	1. Explain Euler's totient function.	**03**
		2. Define group, ring and field	**03**
	(b)	1.Explain host based intrusion detection system.	**03**
		2. What is the purpose of S-boxes in DES?	**03**
		OR	
	(b)	1. Explain Linear congruential generators.	**03**
		2. How primality is tested by Miller-Rabin algorithm.	**03**
Q.3	**(a)**	1. Explain anomaly detection mode of the intrusion detection.	**03**
		2. Define the Playfair cipher.	**03**
	(b)	1. Write the six ingredients of public key encryption scheme.	**03**
		2. Explain the phishing attacks.	**03**
		OR	
Q.3	**(a)**	1. How can highly privileged accounts and groups be protected within the domain?	**03**
		2. Give the example of applications those are based on ICMP.	**03**
	(b)	1. What is the sticky bit? How can it be set?	**03**
		2. Explain the header part of the rule in Snort Intrusion detection system.	**03**
Q.4	**(a)**	1. Write the server level threats.	**03**
		2. How can an E-mail be spoofed?	**03**
	(b)	1.Why does ARP maintain cache? How can the cache content be checked? How can cache be cleared out?	**03**
		2. What is DNS? Which tool is used on the client to query DNS server?	**03**
		OR	
Q.4	**(a)**	1. What is the difference between a monoalphabetic cipher and polyalphabetic cipher?	**03**
		2. For what purpose Euclidean algorithm is used? Explain the algorithm.	**03**
	(b)	1. Describe SubBytes and ShiftRows.	**03**
		2. Explain the Blum Blum Shub Generator.	**03**
Q.5	**(a)**	1. What is one way function? What is a trapdoor one way function?	**03**
		2. Give examples of replay attacks.	**03**
	(b)	Describe the different ways in which a hash code can be used to provide message authentication?	**06**
		OR	
Q.5	**(a)**	1. Write two approaches to digital signatures.	**03**
		2. What is Dual homed host and screened host?	**03**
	(b)	Explain the simple hash functions.	**06**

****