Seat No.: _____ *Enrolment No._____*

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E. 1ST Semester Remedial Examination –July- 2011

Subject code: 710104

Subject Name: Information Security

Date:12/07/2011 **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) Which scheme produces random output that bears no statistical relationship to the plaintext? What are the fundamental difficulties with them?	**04**
		(ii) What is cross site scripting? What are the impacts of cross site scripting?	**03**
	(b)	Write algorithm to find multiplicative inverse. Apply this algorithm to find multiplicative inverse of 550 in GF(1759).	**07**
Q.2	**(a)**	(i) What is the purpose of the State array in AES? How many bytes in State are affected by ShiftRows in AES?	**04**
		(ii) Explain Blum Blum Shub generator.	**03**
	(b)	Write four possible approaches to attack RSA algorithm.	**07**
		OR	
	(b)	List three general approaches to deal with replay attacks.	**07**
Q.3	**(a)**	(i) What are the two basic functions used in encryption algorithms?	**04**
		(ii) Write a snort rule for udp traffic coming from any port and destination ports ranging from 1 to 1024.	**03**
	(b)	Explain client level E-mail threats.	**07**
		OR	
Q.3	**(a)**	(i) Briefly describe MixColumns in AES.	**04**
		(ii) What is dual homed host? What is the problem with dual homed host?	**03**
	(b)	Let S be the set of even integers (positive, negative and 0) under the usual operations of addition and multiplication. Is S a commutative ring?	**07**
Q.4	**(a)**	(i) List characteristics of link and end-to-end encryption.	**04**
		(ii) Explain packet filtering firewall.	**03**
	(b)	Write digital signature algorithm.	**07**
		OR	
Q.4	**(a)**	(i) Explain anomaly based misuse detection pattern.	**04**
		(ii) What is the purpose of network address translation?	**03**
	(b)	Write arbitrated digital signature technique.	**07**

Q.5	**(a)**	In the corresponding ping reply packet, what are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?	**07**
	(b)	(i) Explain central and distributed control approach in network based IDs?	**04**
		(ii) Explain Discover/offer/request/ACK in DHCP(Dynamic host configuration protocol).	**03**

OR

Q.5	**(a)**	How elevation of privileges threats on a web server can be caused?	**07**
	(b)	(i) What are signatures? Explain state based analysis.	**04**
		(ii) List the metrics that can be used for deleting anomalous activities.	**03**

****