Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M.E Sem-II Remedial Examination December 2010

Subject code: 720205

Subject Name :Cryptography & Network Security

Date: 22 /12 /2010 **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)**	i) List the various attacks and explain each in brief. ii) What are the security services (x.800) categories ,explain each in brief.	**06**
	(b)	What is the difference between monoalphabetic and polyalphabetic cipher? Explain with example.	**06**
Q.2	**(a)**	What is steganography ? Explain the various methods of steganography. What are the drawbacks and advantages of steganography ?	**06**
	(b)	List and briefly define types of cryptanalytic attacks based on what is known to the attacker.	**06**
		OR	
	(b)	Explain DES algorithm and Explain the design criteria for DES.	**06**
Q.3	**(a)**	What are the various block cipher modes of operation? and give the typical application for each mode.	**06**
	(b)	What was the original set of criteria used by NIST to evaluate candidates AES cipher?	**06**
		OR	
Q.3	**(a)**	Explain all steps of encryption process in AES?	**06**
	(b)	What is triple encryption? What is meet-in-the-middle attack? How many keys are used in triple encryption?	**06**
Q.4	**(a)**	What is the difference link encryption approach vs end to end encryption approach? Write your comments on traffic confidentiality.	**06**
	(b)	Explain the typical key distribution scenario and hierarchical key control.	**06**
		OR	
Q.4	**(a)**	What is the difference between statistical randomness and unpredictability? Explain the techniques to generates pseudorandom number.	**06**
	(b)	List the various authentication protocols, and explain each in brief.	**06**
Q.5	**(a)**	Give the overview of Kerberos and what problem was Kerberos designed to address?	**06**
	(b)	Explain the various web security threats, its consequences and countermeasures for that.	**06**
		OR	
Q.5	**(a)**	What are the principal elements of a public-key cryptosystem? What are three broad categories of applications of public-key cryptosystem? Explain the RSA algorithms.	**06**
	(b)	Explain the typical IP security scenario, and give the overview of IPsec services.	**06**

****