Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

ME - SEMESTER– I (New course)• REMEDIAL EXAMINATION – SUMMER 2015

Subject Code: 2710211 **Date:18/05/2015**

Subject Name: **Information Security**

Time: 10:30 am to 1:00 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)**	Define the term information security. List and briefly define the categories of security attacks and services.	**07**
	(b)	How substitution cipher differs from Transposition cipher? Discuss unigram frequency attack on Caesar cipher.	**07**
Q.2	**(a)**	Explain the avalanche effect. What is the difference between differential and linear cryptanalysis?	**07**
	(b)	What is Brute force attack? Explain the difference between an unconditional secure cipher and a computationally secure cipher.	**07**
		OR	
	(b)	What are the differences between a block cipher and stream cipher? Discuss different design criteria for evaluating block ciphers.	**07**
Q.3	**(a)**	Explain Deffie Hellman key exchange scheme in detail. Explain man-in-the-middle attack for Deffie Hellman key exchange.	**07**
	(b)	Describe SubBytes, ShiftRows, MixColumns and AddRoundKey in AES (Advanced Encryption standard).	**07**
		OR	
Q.3	**(a)**	Explain RSA algorithm in detail. RSA algorithm is vulnerable to which cryptanalytic attack? Justify your answer.	**07**
	(b)	Explain AES key expansion in detail.	**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)	What are the properties digital signatures should have? Write digital signature algorithm.	**07**
		OR	
Q.4	**(a)**	What characteristics are needed in a secure hash function? Discuss Birthday attack and its signification.	**07**
	(b)	Give the working of the Kerberos detail. What are the principal differences between version 4 and version 5 of Kerberos?	**07**
Q.5	**(a)**	Explain Anti-disassembly and Anti-Debugging Techniques in detail.	**07**
	(b)	Explain in detail the link and end-to-end encryption.	**07**
		OR	
Q.5	**(a)**	Explain Buffer overflow, Incomplete Mediation and Race Conditions with respect to software flows	**07**
	(b)	Explain Output Feedback Mode (OFB) and Counter Mode (CTR) for symmetric key ciphers.	**07**

****