Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE / ME / MBA / MCA - SEMESTER– 1• EXAMINATION – WINTER 2014

Subject Code: 2710211 Date:12/01/ 2015

Subject Name: Information Security

Time: 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)**	What is suppress-replay attack? What is the difference between mutual authentication and one-way authentication?	**07**
	(b)	Why it is not desirable to reuse a stream cipher key? Explain the RC4 algorithm in detail.	**07**
Q.2	**(a)**	Explain With diagram that how authentication and secrecy objectives provided by public key cryptosystem.	**07**
	(b)	Explain Cipher feedback mode (CFB) and counter mode in detail.	**07**
		OR	
	(b)	Explain in detail the link and end-to-end encryption.	**07**
Q.3	**(a)**	Write the possible approaches to attack RSA.	**07**
	(b)	Explain meet-in the-middle attack. Explain Triple DES with two keys.	**07**
		OR	
Q.3	**(a)**	Explain Deffie Hellman key exchange scheme in detail. Explain man-in-the-middle attack for Deffie Hellman key exchange.	**07**
	(b)	Explain AES key expansion.	**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 X.509 certificates formats.	**07**
		OR	
Q.4	**(a)**	What is the difference between a session key and a master key? Explain decentralized key distribution.	**07**
	(b)	What is digital signature? What requirements should a digital signature scheme satisfy? Explain direct and arbitrated digital signature.	**07**
Q.5	**(a)**	Explain Salami attack, linearization and time bomb in detail.	**07**
	(b)	Explain remote user authentication technique using Kerberos.	**07**
		OR	
Q.5	**(a)**	What is the role of disassembler and debugger in software reverse engineering? Explain Code Obfuscation in detail.	**07**
	(b)	Explain different methods for malware detection and state advantages and disadvantages of each method.	**07**

****