Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E. - SEMESTER – II • EXAMINATION – WINTER • 2014

Subject code: 2725103 **Date: 04-12-2014**

Subject Name: Information System and Network Security

Time: 02:30 pm - 05:00 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 threat, vulnerability and countermeasure. Also distinguish between information level threat and network threat with example.	**07**
	(b)	Describe an information system, types and how it helps organizations?	**07**
Q.2	**(a)**	Briefly explain about OSI security architecture	**07**
	(b)	Discuss different classical encryption techniques in detail	**07**
		OR	
	(b)	Explain the Cipher-block chaining mode of operation used in block cipher?	**07**
Q.3	**(a)**	Discuss the possible approaches to attacking the RSA algorithm.	**07**
	(b)	Perform encryption and decryption using the RSA algorithm for p=3,q=11, e=7, M=5.	**07**
		OR	
Q.3	**(a)**	Distinguish between quantitative and qualitative risk assessment	**07**
	(b)	Explain management controls?	**07**
Q.4	**(a)**	Define the terms diffusion and confusion. What is the purpose of S-box in DES? Explain the avalanche effect in DES	**07**
	(b)	Explain the types of attacks on double DES and triple DES	**07**
		OR	
Q.4	**(a)**	What is meant by suppress replay attack? Mention any one method to avoid suppress replay attack.	**07**
	(b)	What is meant by Timing Attacks? Mention any one method to avoid Timing attack	**07**
Q.5	**(a)**	Explain message digests and steps in creation of digital certificate	**07**
	(b)	Discuss the following with respect to scope of applicability and their relative location on TCP/IP stack. (i) SSL (ii) IPSec (iii) PGP	**07**
		OR	
Q.5	**(a)**	Discuss security policies in mobile devices and cryptographically generated addresses (CGA) technique.	**07**
	(b)	Evaluate the following in the context of peripheral security with respect to ease of implementation, their effectiveness of security, and performance overhead. i. Firewall. ii. Virtual private networks. iii. Application Gateways	**07**

****