Seat No.: _____ *Enrolment No._____*

GUJARAT TECHNOLOGICAL UNIVERSITY

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

Subject code: 2715601 **Date: 07-01-2015**

Subject Name: Cryptography 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)**	(I) Describe the specific security mechanisms and pervasive security mechanisms as per X.800 standard. **(II)** Briefly define categories of passive and active attacks.	**07**
	(b)	(I) What is the difference between an unconditionally secure cipher and a computationally secure cipher. **(II)** Explain the transposition technique.	**07**
Q.2	**(a)**	Briefly define the Hill Cipher.	**07**
	(b)	Explain the Feistel Cipher Decryption algorithm.	**07**
		OR	
	(b)	Describe the block cipher design principles from three aspects i.e. number of rounds, design of function F, and key scheduling.	**07**
Q.3	**(a)**	Explain single round of DES algorithm Encryption.	**07**
	(b)	State the difference between differential and linear cryptanalysis.	**07**
		OR	
Q.3	**(a)**	Briefly describe the AES key extension algorithm.	**07**
	(b)	What are various modes of operation of a block cipher algorithm?	**07**
Q.4	**(a)**	Describe one example of symmetric stream cipher.	**07**
	(b)	What are various techniques of distributing the public keys to two communicating parties?	**07**
		OR	
Q.4	**(a)**	Explain the message authentication code. For what purpose it is used.	**07**
	(b)	Describe the arbitrated digital signature. What problem of direct digital signature is addressed by it.	**07**
Q.5	**(a)**	How is an X.509 certificate revoked? Describe its alternative authentication procedures.	**07**
	(b)	What are the requirements of a secure electronic transaction? What are various categories of SET participants?	**7**
		OR	
Q.5	**(a)**	Explain the followings terms: (I) Guaranteed Avalanche Criterion and Bit Independence Criterion (II) end-to-end encryption (III) Suppress Replay Attack (IV) Stateful inspection firewall	**07**
	(b)	Explain two categories of malicious programs along with examples.	**07**

****