Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E. - SEMESTER – II • EXAMINATION – WINTER 2012

Subject code: 1720205 **Date: 02/01/2013**

Subject Name: Cryptography and Network Security

Time: 10.30 am – 01.00 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)**	Explain the following security terms with proper example. Non-repudiation, Integrity, Authentication	**06**
	(b)	What do you mean by secret key cryptography? Discuss the design parameters for secret key algorithm.	**08**
Q.2	**(a)**	What do you mean by security attack? Give its classification with examples.	**07**
	(b)	Describe the AES key expansion algorithm.	**07**
		OR	
	(b)	What is triple DES? What are the proposed attacks on triple DES?	**07**
Q.3	**(a)**	Explain the key distribution with the use of the key distribution center.	**07**
	(b)	Explain the concept of digital signature with the digital signature standard.	**07**
		OR	
Q.3	**(a)**	How can you use public key cryptosystem for the authentication? Explain it with proper diagram.	**07**
	(b)	What is hash function? Show its use in security.	**07**
Q.4	**(a)**	Explain the functioning of the Kerberos.	**07**
	(b)	Explain the working of the firewalls to protect the network.	**07**
		OR	
Q.4	**(a)**	What do you mean by Virtual Private Network? Explain it with proper diagrams.	**07**
	(b)	What is SSL? How it is used for Web security?	**07**
Q.5	**(a)**	Discuss the measures to protect the computer systems and networks from the worms and viruses.	**07**
	(b)	Discuss the use of Secure Electronic Transaction with example.	**07**
		OR	
Q.5	**(a)**	Explain the biometric authentication with its applications.	**07**
	(b)	Explain the zero knowledge protocol.	**07**

****