Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E. - SEMESTER – II • EXAMINATION – WINTER • 2013

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 terms with respect to security: Integrity, Authorization and non-repudiation.	**07**
	(b)	What do you mean by security attacks? Explain the various passive and active attacks.	**07**
Q.2	**(a)**	Compare the symmetric key and public key encryption with their merits and demerits.	**07**
	(b)	Explain the DES algorithm with steps involved.	**07**
		OR	
	(b)	Describe the RSA algorithm with suitable example.	**07**
Q.3	**(a)**	Give the principles and framework of the public key cryptography.	**07**
	(b)	What is key distribution? Explain one of the key distribution models.	**07**
		OR	
Q.3	**(a)**	What is hash function? What is its use? Give the characteristics of MD5.	**07**
	(b)	Give the working of the Kerberos detail.	**07**
Q.4	**(a)**	Explain any one authentication protocol.	**07**
	(b)	Describe the biometric security and RFID.	**07**
		OR	
Q.4	**(a)**	What is SET? How does it work?	**07**
	(b)	What is the role of firewall in network security? Give the working of a typical firewall.	**07**
Q.5	**(a)**	How does warm and viruses compromise security? How do you prevent them?	**07**
	(b)	What is digital certificate? What are its elements? Give the digital certificate standard.	**07**
		OR	
Q.5	**(a)**	What is digital signature? What is its use in making secured transactions?	**07**
	(b)	Describe the database security issues.	**07**

****