GUJARAT TECHNOLOGICAL UNIVERSITY
M. E. - SEMESTER – II • EXAMINATION – SUMMER • 2013

Subject code: 1720205   **Date: 05-06-2013**
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)**	What is digital certificate? What information does it contain? Give its use in present day applications.	**07**
	(b)	Explain the Authorization and Authentication in depth with the help of examples.	**07**
Q.2	**(a)**	Compare the following.	**07**
		1. Active and passive attacks	
		2. Worms and viruses	
		3. Symmetric and asymmetric cryptography	
	(b)	Explain the working of the DES algorithm.	**07**
		OR	
	(b)	Discuss the RSA algorithm with example.	**07**
Q.3	**(a)**	Discuss any one of the key distribution method in depth.	**07**
	(b)	Discuss role of the certification authorities.	**07**
		OR	
Q.3	**(a)**	What is hash function? What is its use? Give its working with example.	**07**
	(b)	Discuss the various attacks that are possible on public key algorithms.	**07**
Q.4	**(a)**	What is Authentication protocol? List them and explain any one with proper illustration.	**07**
	(b)	Discuss following with suitable example.	**07**
		Message Integrity, Biometric Authentication	
		OR	
Q.4	**(a)**	Discuss the working of the Virtual Private Networks to create the secured channel on the Internet.	**07**
	(b)	Discuss following in brief.	**07**
		IP security, Database Access Control	
Q.5	**(a)**	What is RFID? Discuss the privacy and security issues regarding the RFID.	**07**
	(b)	What is role of firewall in network security? List the different types of firewalls and give the functioning of any one of them.	**07**
		OR	
Q.5	**(a)**	Explain the Enterprise Application security issues.	**07**
	(b)	What is SSL? How does it provide security in Web? Give the examples.	**07**

****