Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA - SEMESTER–V • EXAMINATION – SUMMER • 2014

Subject Code: 650002 Date: 26-05-2014

Subject Name: 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)**	Answer the following in brief (Any Seven) 1. List software attacks. 2. What is a difference between a block cipher & a stream cipher? 3. What is message authentication code? 4. What do you mean by certificate revocation? 5. What is detached signature? 6. What do you mean by replay attack? 7. Difference between transport and tunnel mode 8. Why are biometrics used for authentication? 9. Define: firewall	**07**
	(b)	Answer the following in brief (Any Seven) 1. List X.800 Security Services. 2. Define: Session Key & Master Key 3. How is MAC different from HMAC? 4. What do you mean by signature field in X.509 format? 5. Why is r-64 conversion useful for an e-mail application? 6. List different fields of Authentication Header. 7. List key features of SET. 8. Define subject & object with respect to Trusted System. 9. Which are the benefits of IDS?	**07**
Q.2	**(a)**	Explain Active and Passive attacks in detail.	**07**
	(b)	Explain Security Mechanisms in detail.	**07**
		OR	
	(b)	1. What is the difference between link & end-to-end encryption? (4) 2. Explain Key Distribution (3)	**07**
Q.3	**(a)**	1. Explain types of attacks on encrypted message (4) 2. Compare DES, 3DES & AES (3)	**07**
	(b)	Explain three approaches to Message Authentication.	**07**
		OR	
Q.3	**(a)**	Explain Kerberos version 4 in detail.	**07**
	(b)	Explain PGP Services.	**07**
Q.4	**(a)**	1. Explain public key encryption structure. (5) 2. Mention the applications for public key cryptosystem.(2)	**07**
	(b)	Explain X.509 Authentication Procedures.	**07**
		OR	
Q.4	**(a)**	Explain ESP protocol in IPSec in detail.	**07**
Q.4	**(b)**	Explain SSL Architecture & SSL record protocol.	**07**

Q.5	**(a)**	1. Explain IPSec Services. (4) 2. Explain Security Association(3)	**07**
	(b)	1. Explain two rules of multilevel security.(2) 2. Explain Trojan Horse Defense. (5)	**07**
		OR	
Q.5	**(a)**	Explain password selection strategies.	**07**
	(b)	1. List types of firewall. (1) 2. Explain firewall configuration. (6)	**07**

****