Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA - SEMESTER–V • EXAMINATION – WINTER • 2014

Subject Code: 650002 Date: 01-12-2014

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)**	1) Explain very briefly: a) Confidentiality b) Authentication c) Authorization d) Data Integrity e) Availability f) Cipher g) Key	**07**
	(b)	1) Write a short note on: Various types of Cryptographic attacks	**04**
		2) Mention two major benefits of using CBC mode compared to the ECB mode for a given cipher. Mention any one major disadvantage of CBC Mode.	**03**
Q.2	**(a)**	1) Mention and briefly explain the reasons why Non Encryption based authentication methods are preferred.	**04**
		2) Mention and briefly explain the application areas of RSA public keyCrypto-system.	**03**
	(b)	1) Explain the process of generating the public and private key in RSA algorithm.	**04**
		2) Briefly explain: Certificate Revocation List (CRL).	**03**
		OR	
	(b)	1) Mention and briefly explain any four environmental differences between Kerberos Version 4 and Version 5.	**04**
		2) Explain with a block diagram how a public key certificate is used.	**03**
Q.3	**(a)**	1) Explain Private Key Ring with reference to PGP.	**04**
		2) Mention and briefly explain any three applications of IPSEC.	**03**
	(b)	1) Explain with the help of a diagram the generic message sending process in PGP.	**04**
		2) Explain the difference between transport mode and tunnel mode operation with respect to IPSEC.	**03**
		OR	
Q.3	**(a)**	1) Mention and very briefly explain the functionality provided by S/MIME.	**04**
		2) Explain the difference between AH and ESP with respect to IPSEC.	**03**
	(b)	1) Explain Public Key Ring with respect to PGP.	**04**
		2) Mention and very briefly explain the various uses of Padding in IPSEC.	**03**
Q.4	**(a)**	1) Mention the various threats experienced on the World Wide Web and their countermeasures.	**04**
		2) Mention and briefly explain various classes of Intruders.	**03**
	(b)	1) Mention and briefly explain Fatal SSL Alerts Messages.	**04**
		2) Briefly Explain: Statistical Anomaly Detection with respect to IDS.	**03**
		OR	
Q.4	**(a)**	1) Mention and briefly explain Non Fatal SSL Alert Messages.	**04**
		2) Briefly Explain: Rule based Detection with respect to IDS.	**03**

(b) 1) Write a short note on: SSLSessionState **04**
2) Briefly explain any three metrics which are useful for profile based Intrusion detection. **03**

Q.5 **(a)** 1) Briefly explain with respect to a firewall : a) Service Control b) Direction Control c) User Control d) Behavior Control **04**
2) Mention and briefly explain any three commonly used techniques for password generation. **03**

(b) 1) Briefly explain the limitations of a firewall. **04**
2) Mention and briefly explain any three rules for creating a good password. **03**

OR

Q.5 **(a)** 1) Mention and briefly explain the criteria/parameters on the basis of which a typical packet filtering firewall filters packets. **04**
2) Mention and briefly explain the reasons why a dictionary based approach for dealing with bad passwords is not practical. **03**

(b) 1) Briefly explain: Bastion Host with respect to a Firewall. **04**
2) Mention and briefly explain any three drawbacks of a packet filtering firewall. **03**

****