Seat No.: ________   Enrolment No.___________

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA – SEMESTER V – EXAMINATION – SUMMER 2015

Subject Code: 650002   **Date: 04/05/2015**

Subject Name: Network Security

Time: 02:30 pm to 05.00 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)** Define the following in brief: **07**

i. Stream Cipher
ii. Active Attack
iii. Non-Repudiation
iv. Digital Signature
v. Link Encryption
vi. Security Association
vii. Honeypot

(b) 1. Explain RC4 Algorithm. **03**

2. Compare encryption techniques DES, 3DES and AES on grounds of Key Size, Block Size, Number of Rounds, Algorithm Used, Security and Overhead. **04**

Q.2 **(a)** 1. How is HMAC different from MAC? **03**

2. Explain the HMAC Algorithm with supporting diagram. **04**

(b) 1. Mention any three Hash-function requirements. **03**

2. Explain the three ways in which Hash-function can be used to authenticate a message being transmitted. **04**

OR

(b) 1. What are the three applications of Public-Key Cryptosystem? **03**

2. Explain the Deffie-Hellman Key Exchange Algorithm. **04**

Q.3 **(a)** Explain the purpose of following in Kerberos Authentication Dialogue: **07**

i. Authentication Server
ii. TGS
iii. Authenticator
iv. Nonce
v. Ticket Flags
vi. Realm
vii. Ticket Lifetime

(b) What is X.509 Certificate? Explain the X.509 Certificate Format with supporting diagram. **07**

OR

Q.3 **(a)** Explain in detail the five services provided by PGP for constructing a secure mail. **07**

(b) 1. How does PGP secure Private Key of a user for storing it in Key Ring? **03**

2. What are the functions provided by S/MIME? **04**

Q.4 **(a)** 1. Explain the Anti-Replay Service of IPSec. **03**

2. Explain the Transport and Tunnel Modes of IPSec for AH and ESP. **04**

(b) 1. Explain any three ISAKMP Payload Types. **03**

2. What are the important features of Oakley? **04**

OR

Q.4 **(a)** Which protocols comprises SSL protocol Stack? Explain the purpose of each protocol. **07**

(b) 1. What are the key features of SET? **03**

2. How is a Dual Signature constructed? **04**

Q.5 **(a)** 1. Differentiate between Statistical Anomaly Detection and Rule-based Intrusion Detection. **03**

2. Discuss the architecture of Distributed Intrusion Detection System. **04**

(b) 1. Explain how No Read Up and No Write Down policies protect system against Trojan Horse Attacks? **03**

2. What is a firewall? Discuss Application-level Gateway with supporting diagram. **04**

OR

Q.5 **(a)** 1. Discuss the two types of password checking scheme. Which scheme is better and why? **03**

2. Name the two ways of protecting password files. Discuss the technique used for loading a new password and verifying a old password in Unix **04**

(b) Discuss the three firewall configurations with supporting diagrams. **07**

****