Seat No.: _____ Enrolment No._____

# GUJARAT TECHNOLOGICAL UNIVERSITY

**MCA - SEMESTER–V • EXAMINATION – SUMMER 2013**

**Subject Code: 650002 Date: 13-05-2013**

**Subject Name: Network Security**

**Time: 02.30 pm - 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)** | i) | List the security services provided in OSI network model. | **03** |
| | | ii) | Explain giving examples Active Attacks and Passive Attacks. | **04** |
| | **(b)** | i) | Differentiate symmetric and asymmetric encryption | **03** |
| | | ii) | What is digital signature? What are the properties a digital signature should have? | **04** |
| **Q.2** | **(a)** | i) | What is Kerberos? What problem was Kerberos design to address? | **03** |
| | | ii) | How PGP constructs a secure mail? Write the steps involved in the process. | **04** |
| | **(b)** | | List the parameter to be considered while designing symmetric block cipher. Explain single round of DES algorithm. | **07** |
| | | | **OR** | |
| | **(b)** | | Why mode of operation is defined? Explain any three cipher block modes of operations. | **07** |
| **Q.3** | **(a)** | i) | Define the Caesar cipher and encrypt the message “this is my last exam”. | **03** |
| | | ii) | What are the applications of public-key cryptosystems? What requirements must a public key cryptosystems fulfill to be a secure algorithm? | **04** |
| | **(b)** | | Briefly explain Diffie-Hellman key exchange. Justify that Diffie Hellman key exchange is vulnerable to man in the middle attack. | **07** |
| | | | **OR** | |
| **Q.3** | **(a)** | i) | What characteristics are needed in a secure hash function? | **03** |
| | | ii) | In a public key system using RSA, the cipher text intercepted is C=10 which is sent to the user whose public key is e=5, n=35. What is the plaintext M? | **04** |
| | **(b)** | | Explain the different schemes for the distribution of public keys. | **07** |
| **Q.4** | **(a)** | | Draw ESP format for IPSec and describe the need of various fields. | **07** |
| | **(b)** | | What is SET? Explain purchase request and payment authorization processes of SET. | **07** |
| | | | **OR** | |
| **Q.4** | **(a)** | | What is a key ring in PGP? Briefly explain the structure/format indicating the different fields of Private Key Ring in PGP. | **07** |
| | **(b)** | | What protocols comprise SSL? List and briefly define the parameters that define an SSL session state and SSL session connection | **07** |

| | | | | |
|---|---|---|---|---|
| **Q.5** | **(a)** | i) | List and briefly define three classes of intruders. | **03** |
| | | ii) | Just by drawing schematic diagram, show how new password is loaded and existing password is verified in Unix Systems | **04** |
| | **(b)** | | Discuss different types of Firewalls | **07** |

**OR**

| | | | | |
|---|---|---|---|---|
| **Q.5** | **(a)** | i) | What is a dual signature and what is its purpose? | **03** |
| | | ii) | Discus the techniques used by firewalls to control access and enforce a security policy. | **04** |
| | **(b)** | | Discus the common criteria for Information Technology Security Evaluation | **07** |

**********