Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M.E Sem-I Regular Examination January / February 2011

Subject code: 710104N
Subject Name: Information Security

Date: 02 /02 /2011 **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)** Define the following terms and give the real example of each of them : Security attack, Security mechanism and Security service. **07**

(b) What do you mean by packet filtering firewalls? Explain its working and methods. **07**

Q.2 **(a)** What are the criteria to be met by good encryption algorithm? How are they fulfilled by algorithms like DES, AES and IDEA? **07**

(b) Answer following in brief. **07**

1. Write a snote rule that generate alert if mount daemon is accessed?
2. How will you notify that the destination address is class C address?
3. What are the dual homed hosts?

OR

(b) What are the contents of DNS query and reply messages. **07**

Q.3 **(a)** Give the working of Hill cipher with proper example. Give its limitations. **07**

(b) Explain the key generation in DES algorithm. **07**

OR

Q.3 **(a)** What is polyalphabetic Ciphers? How can it be broken? **07**

(b) Give the Feistel cipher structure and give its design criteria. **07**

Q.4 **(a)** Explain the link Vs. end-to-end encryption approach and compare them. **07**

(b) Explain the concept behind the public key cryptography algorithms. **07**

OR

Q.4 **(a)** What do you mean by key distribution? Give at least one method for key distribution with proper illustration. **07**

(b) Answer the following with respect to IDS. **07**

1. Host based Vs. Network based
2. Anomaly detection

Q.5 **(a)** What is message authentication? List the various methods and explain any one of them. **07**

(b) Explain the digital signature algorithm. **07**

OR

Q.5 **(a)** Explain the following terms with proper example. **07**

1. Digital signature
2. Replay attacks

(b) What is Message Digest? What is its significance? Give the methods to generate it. **07**

****