Seat No.: ________ Enrolment No.______________

# GUJARAT TECHNOLOGICAL UNIVERSITY

**M.E –IIst SEMESTER–EXAMINATION – JULY- 2012**

**Subject code: 725103** **Date: 10/07/2012**

**Subject Name: Information System and Network Security**

**Time: 10:30 am – 13:00 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) Define the terms threat and attack. List and briefly define categories of security attacks. **04**

(ii) List and briefly define the security services. **03**

**(b)** (i) Briefly explain the building blocks of information security. **04**

(ii) Discuss security policies and measures in mobile computing. **03**

**Q.2** **(a)** Define the terms diffusion and confusion. What is the purpose of S-box in DES? Explain the avalanche effect in DES. **07**

**(b)** Explain monoalphabetic cipher and polyalphabetic cipher by giving an example. **07**

**OR**

**(b)** What is cryptography? Briefly explain the model of Asymmetric Cryptosystem. **07**

**Q.3** **(a)** (i) Discuss the possible approaches to attacking the RSA algorithm. **04**

(ii) Perform encryption and decryption using the RSA algorithm for p=3,q=11, e=7, M=5. **03**

**(b)** Why mode of operation is defined? Explain the block cipher modes of operation? **07**

**OR**

**Q.3** **(a)** (i) Compare conventional encryption with public key encryption. **04**

(ii) What is a trap-door one-way function? What is its importance in public key cryptography? **03**

**(b)** The Miller-Rabin test can determine if a number is not prime but cannot determine if a number is prime. How can such an algorithm be used to test for primality? Write two properties of prime numbers that is needed for Miller-Rabin algorithm. **07**

**Q.4** **(a)** Briefly explain Diffie-Hellman key exchange. Is it vulnerable to man in the middle attack? Justify. **07**

**(b)** (i) What characteristics are needed in a secure hash function? **04**

(ii) What is the difference between weak and strong collision resistance? **03**

**OR**

**Q.4** **(a)** Discus the ways in which public keys can be distributed to two communication parties. **07**

**(b)** (i) Write the Euclid’s algorithm and show the steps of Euclid’s algorithm to find gcd(1970,1066). **04**

(ii) What is Fermat’s theorem and what is its importance in public-key cryptography. **03**

**Q.5** **(a)** List the security services provided by digital signature. Write and explain the Digital Signature Algorithm. **07**

**(b)** What is MAC? Why it is required? Explain HMAC algorithm. **07**

**OR**

**Q.5** **(a)** What problem was Kerberos designed to address? Briefly explain how session key is distributed in Kerberos. **07**

**(b)** What is the purpose of X.509 standard? Discuss the elements of X.509 certificate format. **07**

*************