Seat No.: _____ Enrolment No.______

GUJARAT TECHNOLOGICAL UNIVERSITY

B E Sem-VI Examination May 2011

Subject code: 160702

Subject Name: Information Security

Date: 17/05/2011 **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)** (i) Explain the various types of cryptanalytic attack, based on the amount of information known to the cryptanalyst. **04**

(ii) Explain the terms diffusion and confusion. **03**

(b) (i) Which two criteria are used to validate that a sequence of numbers is random? Explain the linear congruential method to generate pseudorandom numbers. **04**

(ii) Write the key distribution scenario in which each user shares a unique master key with key distribution center **03**

Q.2 **(a)** (i) Why mode of operation is defined? Explain the simplest mode for block cipher modes of operation? **04**

(ii) What is the purpose of S-boxes in DES? Explain the avalanche effect. **03**

(b) (i) In a public key system using RSA, the ciphertext intercepted is C=10 which is sent to the user whose public key is e=5, n=35. What is the plaintext M? **04**

(ii) Write the differences between conventional encryption and public key encryption. **03**

OR

(b) (i) Briefly explain the Diffie-Hellman key exchange. **04**

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

Q.3 **(a)** (i) How key exchange using elliptic curves can be done? **04**

(ii) Construct a playfair matrix with the key "occurrence". Generate the cipher text for the plaintext "Tall trees" **03**

(b) Explain how subkeys are generated in blowfish algorithm and also explain the encryption in blowfish algorithm. How does the key-size in blowfish differ from cast-128? **07**

OR

Q.3 **(a)** (i) Write the Euclid's algorithm and show the steps of Euclid's algorithm to find gcd(1970,1066). **04**

(ii) Encrypt the message "Good morning" using the Hill Cipher with the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$. **03**

(b) Which parameters affect RC5 encryption algorithm. Explain RC5 encryption and decryption process. **07**

Q.4 **(a)** Illustrate variety of ways in which hash code can be used to provide message authentication. **07**

(b) (i) Why is the segmentation and reassembly function in PGP(Pretty Good Privacy) needed? **04**

(ii)What are the security threats to E-commerce transactions? **03**

OR

Q.4 **(a)** What is cryptographic checksum or message authentication code? Describe the three situations in which message authentication code is used. **07**

(b) (i) What is the difference between transport mode and tunnel mode? **04**

(ii) What parameters characterize the nature of a particular security association in IPSec. **03**

Q.5 **(a)** Write the Digital Signature Algorithm. **07**

(b) Explain the following properties of hash function

(i) One way property **02**

(ii) Weak collision resistance **02**

(iii) Compression function in hash algorithm. **03**

OR

Q.5 **(a)** List and define the parameters that define secure socket layer connection state. **07**

(b) What is dual signature and explain construction of dual signature. **07**

****