Seat No.: __________ **Enrolment No.**_____________

GUJARAT TECHNOLOGICAL UNIVERSITY

ME Semester –I Examination Feb. - 2012

Subject code: 710104N **Date: 21/02/2012**
Subject Name: Information Security
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) For the group G=<Z_4,+>: **04**
a. Is it an abelian group? Justify answer.
b. Show the result of 3+2 and 3-2.
(ii) What is URL encoding and HTML encoding? For what purpose it is used? **03**

(b) (i) For what purpose pattern based intrusion detection is used? For ping, TTL count is set to 24. Show the ping time out with state based analysis. **04**
(ii) Which three actions are available in Snort? **03**

Q.2 **(a)** Compare the substitution, permutations and round keys in DES(Data encryption standard) and AES(Advanced encryption standard). Why there is only one substitution table(S-box) in AES and several in DES? **07**

(b) (i) If DNS(Domain name system) contains following, What is the interpretation? **04**
Type: A (Host address)
Class: IN (0x0001) What other Type and class it can have?
(ii) What is authoritative and Non-authoritative answer in DNS(Domain name system)? **03**

OR

(b) (i) Give examples of replay attacks. **04**
(ii) How traceroute(tracert command) can help in finding out ICMP error? **03**

Q.3 **(a)** Is playfair a stream cipher or block cipher? Justify. In case of playfair, what is the maximum number of characters that will be changed in the ciphertext if only one character is changed in plaintext? Use the playfair cipher to encipher the message “enjoy the balloon ride” and the key is “ticket”. **07**

(b) Write the Euclid and extended Euclid algorithm and find multiplicative inverse of 550 mod 1769. **07**

OR

Q.3 **(a)** Encrypt the message “the house being sold tonight” using one of the following ciphers. **07**
(i) Vignere cipher with key:”bad”.
(ii) Autokey cipher with key:”hide”
Are the above schemes vulnerable to cryptanalysis?

(b) Which weakness is found in all direct digital signature schemes? Explain how these problems are addressed by using arbiter? Explain Arbitrated Digital signature. **07**

Q.4 **(a)** (i) Write Fermat's theorem and with its use. Find 3^{201} mod 11. **04**
(ii) What is the difference between link and end to end encryption? **03**

(b) Describe the domain level threats. **07**

OR

Q.4 **(a)** (i) Write Miller-Rabin algorithm. How can this algorithm be used to test for primality? **04**
(ii) What is the difference between a session key and a master key? **03**

(b) Explain the server level E-mail threats. **07**

Q.5 **(a)** Write the four possible approaches of attacking RSA algorithm. Discuss the timing attack in detail and show the countermeasures that can be used. **07**

(b) Explain three different types of firewalls. **07**

OR

Q.5 **(a)** What is message authentication code? What is the difference between a message authentication code and a one-way hash function? Write the basic uses of Message authentication code. **07**

(b) Explain dual homed host, bastion host and screened host. Explain split screened subnet. **07**

****