Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E. - SEMESTER – II • EXAMINATION – WINTER • 2013

Subject code: 725104 Date: 21-12-2013

Subject Name: PKI and Biometrics

Time: 10.30 am – 01.00 pm Total Marks: 70

Instructions:

1. Attempt question 1, which is compulsory and answer any five from the rest questions.
2. Make suitable assumptions wherever necessary.
3. Figures to the right hand indicate the marks.

Q. No. 1 [2 Marks X 10 = 20 Marks]

a. What is transposition cipher?
b. What is the purpose of the S-boxes in DES?
c. What is triple encryption and how many keys are used in it?
d. What is steganography?
e. What is one way function? Where is it used in Cryptography?
f. What is the difference between passive and active security attacks?
g. What is interruption and interception?
h. What are the properties a digital signature should have?
i. What is replay and masquerading attack?
j. What is false positive and false negative?

Q. No. 2

a. For a user workstation in a typical business environment, list potential location for confidential attacks. [5 Marks]
b. What are the ways in which secret keys can be distributed to two communicating parties? [5 Marks]

Q. No. 3

a. What types of information might be derived from a traffic analysis attack? [5 Marks]
b. What requirements must a public key cryptosystem fulfil to be a secure algorithm? [5 Marks]

Q. No. 4

a. List approaches to dealing with replay attack. [5 Marks]
b. What is the difference between message authentication code and one way hash function? [5 Marks]

Q. No. 5

a. Explain Iris scan and Retina scan. [6 Marks]
b. Write a short notes on key distribution. [4 Marks]

Q. No. 6

a. Explain known plaintext attack and chosen plaint text attack. [6 Marks]
b. Explain CMAC with diagram. [4 Marks]

Q. No. 7

Explain Diffie-Hellman algorithm. [10 Marks]

Q. No. 8

Explain Rijndael algorithm. [10 Marks]

****