CS

(Pages : 2) 905

Reg. No. : .....

Name : .....

First Semester M.Tech. Degree Examination, March 2014
(2013 Scheme)
Computer Science Engineering And Information Security
RIC1001 : FOUNDATIONS OF INFORMATION SECURITY

Time : 3 Hours Max. Marks : 60

MODULE – I

Answer **any two** questions :

I. Write an algorithm to attack

a) Weak collision resistance of cryptographic hash function. Derive an expression for time complexity of the algorithm. 4

b) Strong collision resistance of cryptographic hash function. Derive an expression for time complexity of the algorithm. 4

c) Explain Diffie Hellman key exchange protocol with an example. 2

II. a) Explain small subgroup attack against Diffie Hellman key exchange. 2

b) State windows access control algorithm show how the order of ACEs in a DACL can lead to incorrect results. 5

c) Explain with an example how Hasse diagram can be used to represent multi level security. 3

III. a) Explain Biba model and Bell La Padula model of security policies. Can they both exist in a system simultaneously ? Defend your answer. 5

b) Which is the most appropriate term email worm or email virus ? Explain. 2

c) Define i) Steganography ii) Water marking. How do they differ ? 3

P.T.O.

MODULE – II

Answer **any two** questions :

IV. a) Explain Kerberos protocol. 7

b) In a triometric authentication system is it possible to decrease the fraud rate without simultaneously increasing the insult rate and vice versa. Why ? Why not ? 3

V. Explain how Needham Schroder protocol prevents

i) Man in the middle attack

ii) Replay attack 10

VI. a) Explain SSL hand shake protocol.

b) Explain SYN flooding. 10

MODULE – III

Answer **any two** questions :

VII. Compare and contrast the security policies. 10

VIII. Explain the features of any two security tools. 10

IX. What is ethical hacking ? Why is it needed ? 10