FirstRanker.com
Firstranker's choice
www.FirstRanker.com www.FirstRanker.com

Code No: 824AE **R15**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
MCA IV Semester Examinations, August - 2017
INFORMATION SECURITY

Time: 3hrs **Max.Marks:75**

Note: This question paper contains two parts A and B.
Part A is compulsory which carries 25 marks. Answer all questions in Part A. Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 10 marks and may have a, b, c as sub questions.

PART - A

5 × 5 Marks = 25

1.a) Explain the need for computer security and describe various nature of attacks. [5]
b) Write a short note on the weaknesses of DES algorithm. [5]
c) Explain in detail the 0/1 Knapsack problem. [5]
d) Write a short note on the functions provided by S/MIME. [5]
e) State and explain the various kinds of Firewalls. [5]

PART - B

5 × 10 Marks = 50

2. Explain in detail various principles of security. [10]

OR

3.a) Distinguish between symmetric and asymmetric encryption.
b) Demonstrate substitution and transposition techniques with examples. [5+5]

4. Explain in detail about Advanced Encryption Standard (AES) algorithm. [10]

OR

5.a) Discuss the procedure involved in RSA public-key encryption algorithm along with its security issues.
b) Illustrate Diffi-Hellman key exchange scheme with an example. [5+5]

6. Explain the X.509 authentication services with a neat structure diagram. [10]

OR

7. Explain in detail the Secure Hash Algorithm. [10]

8. Define PGP and explain in detail the five principal services provided by PGP. [10]

OR

9. Explain the scenario of IP Security with a neat diagram and list out the services provided by the IPSec at IP layer. [10]

10. Explain in detail about various kinds of Viruses and Worms. [10]

OR

11. List out the three categories of Intruders and with the help of a neat diagram explains the architecture of Distributed Intrusion Detection. [10]

---oo0oo---

www.FirstRanker.com