



FirstRanker.com

FirstRanker's choice

Code No: 814AT

www.FirstRanker.com

www.FirstRanker.com

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

MCA IV Semester Examinations, August - 2017

INFORMATION SECURITY

Time: 3 Hours

Max. Marks: 60

Note: This question paper contains two parts A and B.

Part A is compulsory which carries 20 marks. Answer all questions in Part A. Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 8 marks and may have a, b, c as sub questions.

PART - A

5 × 4 Marks = 20

- 1.a) Define authentication, confidentiality, Non-repudiation, Availability. [4]
- b) Write a short note on Diffie Hellman Key Exchange Algorithm. [4]
- c) What are the properties of Hash function in cryptography? [4]
- d) Briefly discuss about the concept of combining security associations. [4]
- e) Write short notes on Password selection strategies and their significance. [4]

PART - B

5 × 8 Marks = 40

2. Compare and Contrast between Symmetric and Asymmetric key cryptography. [8]
- OR**
3. With a neat sketch explain the model for inter network security. [8]
4. With a neat diagram explain how does encryption and decryption techniques works for DES. [8]
- OR**
5. Perform encryption and decryption using RSA Alg. for the following. $P=7$; $q=11$; $e=17$; $M=8$. [8]
6. Give a neat sketch to explain the concept of HMAC. [8]
- OR**
7. Client machine C wants to communicate with server S. Explain how it can be achieved through Kerberos protocol? [8]
8. How the messages are generated and transmitted in pretty good privacy (PGP) protocol? Explain with clear diagrams. [8]
- OR**
9. Explain in detail about the various services provided in IPsec. [8]
10. With a neat diagram explain in detail about Secured Electronic Transactions (SET). [8]
- OR**
11. List the characteristics of a good firewall implementation. How is circuit gateway different from application gateway? [8]

---oo0oo---



FirstRanker.com
FirstRanker's choice

www.FirstRanker.com