

Code No: 5258AD

R15

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech I Semester Examinations, February - 2016

NETWORK SECURITY

(Computer Science and Engineering)

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) Write about transportation techniques. [5]
- b) Discuss the strengths of DES. [5]
- c) What problem was Kerberos designed to address? [5]
- d) Give the format of PGP message and mention the purpose of each field. [5]
- e) Explain the role of encryption in the operation of virus. [5]

PART - B

5 × 10 Marks = 50

2. List and explain categories of Security Services and Mechanisms. [10]
OR
3. Discuss various types of security attaches. [10]
4. Explain different crypto algorithms where public key cryptosystems are used. [10]
OR
- 5.a) What are the differences between symmetric and asymmetric cryptography?
b) What is the significance of key distribution? How keys are distributed in classical cryptography? [4+6]
6. Write a short note on the following:
a) CMAC b) Whirlpool [5+5]
OR
- 7.a) How confidentiality and authentication are provided for a message?
b) Give a brief note on secure hash algorithm. [3+7]
8. Explain the web of trust made from certificates in PGP. [10]
OR
- 9.a) For the Oakley aggressive key exchange, indicate which parameters in each message go in which ISAKMP payload type.
b) Explain encapsulating security payload protocol. [5+5]
10. Where would you place a web server in an organization assuming that you can use a network firewall and why? Describe the limitations of firewall. [10]
OR
- 11.a) Discuss the services provided by SSL and TLS
b) Write a short note on virtual elections. [5+5]