

Code No: 5258AD

R15

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech I Semester Examinations, February - 2017

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) Explain avalanche effect. [5]
- b) Mention the block cipher principles. [5]
- c) How digital signature is different from conventional? [5]
- d) Write an overview of IP security documents. [5]
- e) What is virus? [5]

PART - B

5 × 10 Marks = 50

- 2.a) Explain the security services and mechanisms.
 - b) Explain any two substitution techniques. [5+5]
- OR**
- 3.a) What is meant by Steganography? Explain.
 - b) Explain transposition techniques in detail with examples. [5+5]
- 4.a) Explain in detail the sub key generation and round function of DES algorithm.
 - b) Discuss linear and differential cryptanalysis. [5+5]
- OR**
- 5.a) Discuss about RC4 stream cipher.
 - b) Describe Diffie-Hellman Key exchange algorithm. [5+5]
- 6.a) Explain in detail about Kerberos.
 - b) Explain the knapsack algorithm. [5+5]
- OR**
- 7.a) Write in detail about security of Hash functions and MAC.
 - b) Explain about Whirlpool. [5+5]
- 8.a) Explain authentication header with a neat diagram.
 - b) Discuss about key management. [5+5]
- OR**
- 9.a) Explain PGP message generation and reception.
 - b) What is the need to combine Security Associations? Explain basic combinations of Security Associations. [5+5]
- 10.a) Explain briefly about trusted systems.
 - b) Explain statistical anomaly detection and rule based intrusion detection system. [5+5]
- OR**
11. Write short notes on:
 - a) Firewalls
 - b) Worms
 - c) Web security[10]