

R15

Code No: 128DH

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

B. Tech IV Year II Semester Examinations, July - 2019

NETWORK SECURITY

(Common to ECE, ETM)

Time: 3 hours

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

(25 Marks)

- 1.a) A bank is performing all its financial transactions over the Internet. What kind of security is required? [2]
- b) Draw the common attacks and vulnerabilities. [3]
- c) What is message authentication? [2]
- d) Give a brief note on HMAC. [3]
- e) What problem was Kerberos designed to address? [2]
- f) How keys are generated in various cryptographic algorithms? [3]
- g) Compare SSL and TLS. [2]
- h) Write brief notes on SET. [3]
- i) How does a trusted system defend from Trojan horse attack? [2]
- j) What are the typical phases of operations of a virus or worm? [3]

PART - B

(50 Marks)

- 2.a) How NIST defines computer security? Give examples of recent computer security attacks which you know.
- b) With the help of neat diagram, explain the model for Internetwork security. [5+5]

OR

3. What are the different RFCs and Internet standards related to security? Logically organize them and explain their contribution. [10]

- 4.a) List and explain the Block Cipher Design Principles and Modes of operation.
- b) Write differences between Block & Stream ciphers. [5+5]

OR

- 5.a) Explain Message Authentication Requirements and What are the attacks related to message communication?

- b) For SHA-512, show the equations for the values of W_{16} , W_{17} , W_{18} , W_{19} and Calculate the hash function for the 48 letter message "I leave 20 million dollars to my friendly cousin bill". [5+5]

- 6.a) Mention three variations of digital signatures and briefly state the purpose of each.
- b) Define Kerberos and name its servers. Briefly explain the duties of each server. [5+5]

OR

AG AG AG AG AG AG AG A

7. List and explain the PGP services and explain how PGP message generation is done with a neat diagram. [10]

AG 8. What are the two levels of alerts? What action is taken by SSL when a fatal level is received? Explain. [10] A

OR

9.a) Explain in detail how payment processing is done in SET.

b) Give a brief note on encapsulating security payload. [5+5]

10.a) What does it mean to say that a system is "trusted"? Do you agree that "only a trusted system can break your security"? Why or why not.

AG b) Give a brief note on SNMPv1 Community facility and SNMPv3. [5+5] A

OR

11. Select any antivirus of your choice and explain it in detail. [10]

---oo0oo---

AG AG AG AG AG AG AG A

AG AG AG AG AG AG AG A

AG AG AG AG AG AG AG A

AG AG AG AG AG AG AG A

AG AG AG AG AG AG AG A