

R16

Code No: 136AW

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

B. Tech III Year II Semester Examinations, July - 2023

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to CSE, IT)

Time: 3 Hours

Max. Marks: 75

Note: i) Question paper consists of Part A, Part B.

ii) Part A is compulsory, which carries 25 marks. In Part A, Answer all questions.

iii) In Part B, Answer any one question from each unit. Each question carries 10 marks and may have a, b as sub questions.

PART - A

(25 Marks)

- 1.a) Discuss the need of security. [2]
- b) What is steganography? [3]
- c) Write about cipher block chaining mode of operation. [2]
- d) List out the advantages of RC5 algorithm. [3]
- e) Define CMAC. [2]
- f) Explain Kerberos. [3]
- g) Discuss the functions of SSH protocol. [2]
- h) Discuss about the importance of security in mobile devices. [3]
- i) What is transport mode and tunnel mode in IP sec? [2]
- j) What is authentication header? [3]

PART - B

(50 Marks)

- 2.a) List and briefly define categories of Security Services and attacks. [5+5]
- b) Discuss about Brute force attack in detail. [5+5]

OR

- 3.a) Demonstrate the terminologies used in Encryption. [5+5]
- b) Discuss about model for Network Security. [5+5]

- 4.a) Critically analyze the security of RSA. [5+5]
- b) Enumerate in detail about the steps in Blow Fish Algorithm and explain the process of each round with a neat diagram. [5+5]

OR

- 5.a) Differentiate between RC5 and blowfish. [5+5]
- b) Write a short note on knapsack algorithm. [5+5]

- 6.a) Discuss about Secure Hash algorithm. [5+5]
- b) Explain about Digital Signature Scheme. [5+5]

OR

- 7.a) Discuss about the message exchange mechanism in Kerberos version 4. [5+5]
- b) Explain about X.509 authentication service. [5+5]

QA QA QA QA QA QA QA G

- 8.a) List and briefly define the parameters that define an SSL session state.
b) Discuss briefly about HTTPS.

[5+5]

QA QA QA QA QA QA QA G

- 9.a) Discuss the IEEE 802.11i Wireless LAN Security.
b) What are web security consideration? Explain.

[5+5]

- 10.a) Describe the functionalities of Internet Key Exchange Protocol.
b) What is a firewall? State the design goals of firewalls. Also discuss in detail different types of firewalls.

[5+5]

QA QA QA QA QA QA QA G

- 11.a) How inter branch payment transactions are performed?
b) Explain in detail about the mechanism of security associations and IP Security in IPSec.

[5+5]

QA QA QA QA QA QA QA G

---ooOoo---

QA QA QA QA QA QA QA G

QA QA QA QA QA QA QA G

QA QA QA QA QA QA QA G

QA QA QA QA QA QA QA G