

**R18**

**Code No: 157BB**

**JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD**

**B. Tech IV Year I Semester Examinations, February - 2025**

**CRYPTOGRAPHY AND NETWORK SECURITY**

**(Common to CSE, CSE(N))**

**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) What is the need for security? [2]
- b) Compare Substitution and Transposition techniques. [3]
- c) Define block cipher. [2]
- d) Describe the principles of public key cryptosystems. [3]
- e) Define hash function. [2]
- f) What is digital signature? [3]
- g) What is Secure Shell (SSH)? [2]
- h) What are the security challenges in mobile devices? [3]
- i) What are the security services provided by IPSec? [2]
- j) What is Internet Key Exchange? [3]

**PART – B**

**(50 Marks)**

2. Explain about OSI Security architecture model with neat diagram. [10]

**OR**

- 3.a) Describe how steganography is used in providing security in networks. [6+4]
- b) Explain various substitution ciphers in detail. [6+4]

- 4.a) List out the steps of encryption in DES algorithm. [6+4]
- b) Give short note on stream ciphers. [6+4]

**OR**

- 5.a) Using an example, explain the encryption and decryption process in RSA algorithm. [6+4]
- b) Explain knapsack algorithm with an example. [6+4]

- 6.a) How does authentication achieved using Secure Hash Algorithm(SHA – 512)? [6+4]
- b) Explain Elgamal Digital Signature Scheme. [6+4]

**OR**

- 7.a) Discuss about the distribution of Public Keys. [5+5]
- b) In detail explain X.509 Authentication Service. [5+5]

QA QA QA QA QA QA QA QA QA

- 8.a) Explain the web security considerations.
- b) Describe the operational steps of transport layer security. [5+5]

**OR**

QA QA QA QA QA QA QA QA QA QA QA

- 9.a) Explain the requirements of wireless security.
- b) In detail, explain IEEE802.11i wireless LAN security. [5+5]

- 10.a) Explain the mechanism of providing security in E-mails.
- b) Describe the encapsulating security payload in IP Security. [5+5]

**OR**

- 11.a) How does Cross site Scripting Vulnerability occurs?
- b) For the case study: Virtual Elections, discuss the security threats, vulnerabilities and solutions. [4+6]

QA QA QA QA QA QA QA QA QA QA QA

---ooOoo---

QA QA QA QA QA QA QA QA QA QA QA

QA QA QA QA QA QA QA QA QA QA QA

QA QA QA QA QA QA QA QA QA QA QA

QA QA QA QA QA QA QA QA QA QA QA

QA QA QA QA QA QA QA QA QA QA QA