

**R18**

**Code No: 157CR**

**JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD**

**B. Tech IV Year I Semester Examinations, December-2023/January-2024**

**NETWORK SECURITY AND CRYPTOGRAPHY**

**(Electronics and Communication Engineering)**

**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) Explain Active and Passive Security attacks. [2]
- b) What are the various Security Services? [3]
- c) Why Random numbers are used in Cryptography? [2]
- d) Discuss about the placement of Encryption function. [3]
- e) Enumerate the differences between Private key and Public key. [2]
- f) Explain Euler's theorem. [3]
- g) What is Message Authentication Code? [2]
- h) Explain the security of Hash functions. [3]
- i) What is a Malicious code? [2]
- j) What are the limitations of Firewalls? [3]

**PART – B**

**(50 Marks)**

- 2.a) Explain in detail about various types of security mechanisms with neat diagrams.
- b) With a neat diagram explain the model for Network Security? [5+5]

**OR**

- 3.a) Explain the Block Cipher design principles.
- b) Explain the features and strength of DES algorithm. [5+5]

4. With a neat block diagram, explain the Blowfish encryption algorithm. [10]

**OR**

- 5.a) Explain the characteristics of Advanced Symmetric Block Ciphers.
- b) Describe a scenario of secret key distribution in cryptography. [5+5]

- 6.a) Explain the steps of RSA algorithm.
- b) Given two prime numbers  $p = 5$  and  $q = 11$ , and encryption key  $e = 7$  derive the decryption key  $d$ . Let the message be  $x = 24$ . Perform the encryption and decryption using R.S.A algorithm. [5+5]

**OR**

- 7.a) What are the principal elements of a Public Key Cryptosystems?
- b) Explain the Diffie - Hellman key Exchange algorithm. [5+5]

QA QA QA QA QA QA QA G

- 8.a) Explain the general format of a PGP message with a pictorial representation.
- b) Describe the working of Kerberos.

[5+5]

QA QA QA QA QA QA QA QA QA QA G

- 9. Give a neat sketch to explain the concept of Secured Hash Algorithm (SHA).

[10]

- 10. Describe the working of Secure Electronic Transaction (SET).

[10]

**OR**

- 11.a) List and explain the types of firewalls.
- b) Explain the generations of Antivirus techniques.

[5+5]

QA QA QA QA QA QA QA QA QA QA G

---ooOoo---

QA QA QA QA QA QA QA QA QA QA G

QA QA QA QA QA QA QA QA QA QA G

QA QA QA QA QA QA QA QA QA QA G

QA QA QA QA QA QA QA QA QA QA G

QA QA QA QA QA QA QA QA QA QA G