END TERM EXAMINATION – December 2022

SEMESTER – VII

(B.Tech.-CSE)

Subject Code: CS4019 Duration: 3 hours

Subject: Network Security and Cryptography Max. Marks: 100

Instructions

- All Questions are compulsory
- The Question paper consists of 2 sections - Part A contains 10 questions of 2 marks each. Part B consists of 5 questions of 16 marks each.
- There is no overall choice. Only Part B questions include internal choice.

PART – A

*(2 * 10 = 20 Marks)*

1. Encrypt the "Algorithm" using the Rail fence technique.
2. What is symmetric key cryptography?
3. Give the formula for Euler's Totient function.
4. Richa received an encrypted message sent to him from Sam. Which key should she use to decrypt the message?
5. TSL (Transport Layer Security) is a cryptographic protocol used for securing HTTP/HTTPS-based connections. True/False
6. What do understand by the term TSP (Time stamp protocol)
7. What are the 3 ways of authenticating user identity?
8. Describe 3 main parts of Kerberos?
9. State what do you understand by intrusion detection system?
10. Give a few real-life applications of cryptography?

PART – B

*(16 * 5 = 80 Marks)*

11. a) What are two different techniques used for encrypting data? Explain any one.

OR

b) Explain different principles of security with a diagram or example.

12. a) Describe the Diffie-Hellman key exchange algorithm.

OR

b) Out of two symmetric key algorithms explain any one.

13.a) What is SSL (Secure Socket Layer) and its subprotocols?

OR

b) What do you understand by Digital Signatures?

14. a) Explain the working of Kerberos. What do you understand by biometric authentication?

OR

b) Explain authentication tokens and their types.

15.a) (i) Explain firewall design principles.
(ii) What are trusted systems in Network security?

OR

b) State the difference between IDS (Intrusion Detection System) and firewalls.