

22P340

(Pages: 2)

Name:

Reg.No:

THIRD SEMESTER M.Sc. DEGREE EXAMINATION, NOVEMBER 2023

(CBCSS - PG)

(Regular/Supplementary/Improvement)

CC19P CSS3 E02c - CRYPTOGRAPHY AND NETWORK SECURITY

(Computer Science)

(2019 Admission onwards)

Time : 3 Hours

Maximum : 30 Weightage

Part-A

Answer any *four* questions. Each question carries 2 weightage.

1. Explain the Triple DES algorithm.
2. Explain encryption with private key and public key.
3. Describe Public-Key Certificates.
4. Describe Federated Identity Management.
5. Explain TLS Alert Codes.
6. Discuss the different classes of intruders.
7. Explain Digital Immune System.

(4 × 2 = 8 Weightage)

Part-B

Answer any *four* questions. Each question carries 3 weightage.

8. Describe security attacks with neat figures.
9. Illustrate Fiestel cipher structure.
10. Illustrate One -Way hash function.
11. Explain Diffie-Hellman Key Exchange.
12. Explain applications, services and benefits of IPsec .
13. Describe Top-Level format and Substructure of payload used in ESP.
14. Discuss the need and characteristics of firewalls. Also Explain packet filtering firewall.

(4 × 3 = 12 Weightage)

Part-C

Answer any *two* questions. Each question carries 5 weightage.

15. Discuss Cipher Block modes of operation.

16. Discuss Kerberos version 4 in detail.
17. Describe SSL Protocol Stack and Handshake Protocol with figure.
18. Discuss DMZ and VPN.

(2 × 5 = 10 Weightage)
