THIRD SEMESTER M.Sc. DEGREE EXAMINATION, NOVEMBER 2022

(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. Describe symmetric encryption principles.

2. Describe RSA Algorithm.

3. Explain Ticket granting service exchange in Kerberos Version 4.

4. Describe Federated Identity Management.

5. Discuss Security Policy Database.

6. Explain packet filtering firewall.

7. Explain VPN.

(4×2 = 8 Weightage)

Part-B

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

8. Illustrate model for network security.

9. Explain Triple DES.

10. Illustrate One -Way hash function.

11. Illustrate HMAC structure.

12. Explain SSH Protocol Stack.

13. Explain Top-Level format and Substructure of payload used in ESP.

14. Discuss any three types of malicious software.

(4×3 = 12 Weightage)

Part-C

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

15. Discuss Cipher Block modes of operation.

16. Describe X.509 Certificates with figure.

17. Describe SSL Handshake Protocol with figure.

18. Explain any three intrusion detection techniques.

(2 × 5 = 10 Weightage)

****