D 31127 **(Pages : 2)** **Name.....**

Reg. No.....

THIRD SEMESTER M.Sc. DEGREE (REGULAR/SUPPLEMENTARY) EXAMINATION, NOVEMBER 2022

(CBCSS)

Computer Science

CSS 3E 02 C—CRYPTOGRAPHY AND NETWORK SECURITY

(2019 Admission onwards)

Time : Three Hours Maximum : 30 Weightage

Part A

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

1. What do you mean by cryptanalysis ? Explain.
2. Give the short notes on AES.
3. What are the requirements for message authentication ?
4. Write the principles of public key cryptography.
5. Briefly explain TLS functions and alert codes of Transport Layer Security.
6. What are the different types of viruses ? How do they get into the systems ?
7. List and explain the three classes of intruders.

(4 × 2 = 8 weightage)

Part B

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

8. Discuss the concept of simplified DES.
9. Explain the major design principles of block cipher.
10. What are the major digital signature standards ? Explain.
11. How authentication is performed in Kerberos ?
12. Discuss the concept of IP security architecture.

Turn over

13. Give the taxonomy of malicious programs. Define each one.

14. What are the three common types of firewalls ? Explain.

(4 × 3 = 12 weightage)

Part C

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

15. Define threat and attack. Explain with examples.

16. Describe Hash functions in detail.

17. Explain the authentication services provided by X.509.

18. Discuss the format of an ESP(Encapsulating Security Payload) packet in IP security.

(2 × 5 = 10 weightage)