D 70930 (Pages : 2) Name.......................................

Reg. No.......................................

THIRD SEMESTER M.Sc. DEGREE (REGULAR) EXAMINATION NOVEMBER 2019

Computer Science

CSS 3E 04 (C)—CRYPTOGRAPHY AND NETWORK SECURITY

Time : Three Hours Maximum : 36 Weightage

Part A

Answer **all** *questions.*

1. What do you mean by "security service" ?
2. Draw block diagram of a Model for Network security.
3. What are the two requirements for secure use of symmetric encryption.
4. What is a digital signature ?
5. What is a Message Authentication Code ?
6. List any three uses of public key cryptosystems.
7. What do you mean by "Public key infrastructure".
8. What is a nonce ?
9. Give examples of application of IPsec.
10. What is the purpose of HTTPS.
11. What is a firewall ?
12. List and briefly explain three classes of intruders.

(12 × 1 = 12 weightage)

Part B

Answer any **six** *questions.*

13. Explain the structure of DES. What are the strengths of DES ?
14. Discuss the challenges of Computer Security.
15. Write and explain HMAC algorithm.

Turn over

16. Give a digital signature scheme based on public key cryptography. Explain Digital signature Standard.

17. List the principal elements of an Identity Management System.

18. Explain how symmetric keys are distributed using symmetric encryption.

19. Write a note on SSH.

20. Explain Security Association database.

21. Discuss password selection strategies.

(6 × 2 = 12 weightage)

Part C

Answer any **three** *questions.*

22. (i) Discuss the criteria used to validate that a sequence of numbers is random. Explain TRNG. PRNG and PRF.

    (ii) Briefly explain the four stages used in an AES round.

23. Explain in detail cipher modes of operations.

24. (i) Give an overview of RSA algorithm.

    (ii) Discuss Hash function requirements.

25. Give a detailed account of Kerberos.

26. Discuss SSL architecture and SSL record protocol.

27. Give a detailed account of characteristics of computer viruses and counter measures to virus attacks.

(3 × 4 = 12 weightage)