18P347 (Pages: 2) Name……………………..

Reg. No…………………..

THIRD SEMESTER M.Sc. DEGREE EXAMINATION, NOVEMBER 2019

(Regular/Supplementary/Improvement)

(CUCSS-PG)

CC17P CSS3 E04c - CRYPTOGRAPHY AND NETWORK SECURITY

(Computer Science)

(2017 Admission onwards)

Time: Three Hours Maximum : 36 Weightage

PART A

Answer ***all*** questions. Each question carries 1 weightage.

1. What are basic computer security objectives?
2. What is meant by cryptanalytic attack?
3. Define Masquerade.
4. What are the criteria for a random number?
5. Define the term access control in computer security.
6. What is DDoS attack?
7. Write two specific authentication services defined in X.800.
8. What is spoofing?
9. Define public key encryption.
10. What are the two basic functions used in Encryption algorithm?
11. What is realm, in the context of Kerberos?
12. Write the purpose of SSL Handshake Protocol.

(12 x 1 = 12 Weightage)

PART B

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

13. Write about Triple DES and its drawback.
14. Write the important parameters considered for a Feistel cipher design.
15. Explain RSA Public key encryption algorithm.
16. What is Message Authentication Code? Depict the process of using MAC for authentication of a message.
17. What are the essential properties and requirements needed for a digital signature?
18. Explain symmetric key distribution using asymmetric encryption.
19. What is the difference between an unconditionally secure cipher and a computationally secure cipher?

20. Describe details of the following terms a) IKE b) Replay attack

21. Explain common attacks launched by intruders to compromise the security of computer systems.

(6 x 2 = 12 Weightage)

PART C

Answer any ***three*** questions. Each question carries 4 weightage.

22. Explain AES Encryption process.

23. Explain about Secure Hash function.

24. Compare and contrast four different types of malware in terms of their attacks and appropriate countermeasures.

25. Explain SSL objectives and its architecture.

26. Explain the different cipher block modes of operation with diagram.

27. Define Firewall security. Write about Packet Filtering firewall and Application Proxy firewall.

(3 x 4 = 12 Weightage)

****