D 91658 (Pages : 2) Nark.....

Reg. No.....

THIRD SEMESTER M.Sc. DEGREE EXAMINATION, DECEMBER 2015

(CUCSS)

Computer Science

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

(2014 Admissions)

Time : Three Hours Maximum : 36 Weightage

Part A

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

1. Define replay attack.
2. Define diffussion.
3. What are the two problems with the one time pad ?
4. List the authentication requirements.
5. What is honey pots ?
6. State the difference between convential encryption and public key encryption.
7. Define malicious software.
8. Name any *two* security standards.
9. What is the purpose of the X.509 standards ?
10. What protocol comprise SSL ?
11. List three classes of Intruders.
12. What is DDOS ?

(12 x 1 = 12 weightage)

Part B

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

13. List and briefly define types of cryptanalytic attacks.
14. What is the purpose of the S-boxes in DES ?
15. Explain the avalanche effect.
16. List the important features of Kerberos.
17. What steps are involved in the SSL record protocol ?

Turn over

18. What is the difference between direct and arbitrated digital signature ?

19. What is circuit level gateway ?

20. What is the difference between statistical anomaly detection and rule based intrusion detection ?

21. With a neat block diagram, explain the network security model and important parameters associated with it.

(6 × 2 = **12** weightage)

Part C

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

22. Explain key generation, encryption and decryption **of DES algorithm in detail.**

23. **With the steps involved, explain** Diffie-Hellman **key exchange algorithm in detail with example.**

24. **Write the algorithm of RSA and explain with an example.**

25. **Write a detailed note on digital signature.**

26. **Explain the different types of** firewall **and its configurations in detail.**

27. (a) **Differentiate transport mode and tunnel mode encryption in IP** Sec.

(b) With a neat diagram, explain handshake protocol in SSL.

(3 **x 4 = 12** Weightage)