D 90999 (Pages : 2) Name.....

Reg. No.....

THIRD SEMESTER M.A./M.Sc./M.Com. DEGREE (REGULAR) EXAMINATION, NOVEMBER 2020

(CBCSS)

Computer Science

CSS 3E 02 C—CRYPTOGRAPHY AND NETWORK SECURITY

(2019 Admissions)

Time : Three Hours Maximum : 30 Weightage

General Instructions

1. *In cases where choices are provided, students can attend* **all** *questions in each Section / Part.*
2. *The minimum number of questions to be attended from the Section / Part shall remain same.*
3. *There will be an overall ceiling for each Section / Part that is equivalent to maximum weightage of the Section / Part.*

Section A

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

1. Briefly explain about DES.
2. Define security mechanism.
3. Specify the components of encryption algorithm.
4. Define the classes of message authentication function.
5. Write the network security applications.
6. What is the need to combine Security Associations ?
7. Mention about Password management.

(4 × 2 = 8 weightage)

Section B

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

8. Describe about evaluation criteria for AES.
9. Explain transposition techniques.

Turn over

10. Distinguish between direct and arbitrated digital signature ?

11. Specify the applications of the public key cryptosystem.

12. What is Kerberos ? Explain how it provides authentic services.

13. Why Internet Key Exchange is used ? Explain header and payload formats of it.

14. Summarize the three classes of intruders.

(4 × 3 = 12 weightage)

Section C

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

15. Compare all the features of stream and block ciphers.

16. Explain MACs based hash function with its design objectives and structure of the algorithm.

17. Explain in detail the operation of Secure Socket Layer in detail.

18. What is a firewall ? What is the need for firewalls ? What is the role of firewalls in protecting networks ?

(2 × 5 = 10 weightage)