(Pages : 2)

K – 5397

Reg. No. : ....

Name : ....

Eighth Semester B.Tech. Degree Examination, February 2021

08.803 – CRYPTOGRAPHY AND NETWORKS SECURITY (R)

(2008 Scheme)

Time : 3 Hours

Max. Marks : 100

PART – A

Answer **all** questions. **Each** question carries **4** marks.

1. Explain the difference between a unconditionally secure cipher and computationally secure cipher.

2. Explain the parameters and design choices that determine the actual algorithm of Fiestel cipher.

3. What is the difference between confusion and diffusion?

4. Prove that [(a modn) - (b modn)]mod n =(a-b)mod n.

5. What is a trapdoor one way function?

6. Explain elliptic curve cryptography.

7. What are the properties of a digital signature?

8. Why is the segmentation and reassembly function in PGP needed?

9. What are the services provided by IPSec?

10. What is a dual signature and what is its purpose?

(10 × 4 = 40 Marks)

P.T.O.

PART – B

Answer **one** full Question from each module. Each full question carries **20** marks.

Module - I

11. Explain AES Encryption algorithm.

OR

12. (a) Explain the different substitution techniques used in cryptography.

    (b) Discuss about the strength of DES.

Module - II

13. (a) Explain about public key cryptosystems. What are its applications?

    (b) Discuss MD5 hash algorithm.

OR

14. (a) Discuss the applications of message authentication codes and hash functions.

    (b) Explain elliptic curve cryptography.

Module - III

15. (a) Discuss about any three types of firewalls.

    (b) What do you mean by transport layer security?

OR

16. (a) Explain the different modes of IPSec operation.

    (b) What are encrypted tunnels?

(3 × 20 = 60 Marks)