Reg. No. : .....

Name : .....

(Pages : 2)

H – 3411

Eighth Semester B.Tech. Degree Examination, November 2019

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. Compare transposition and substitution techniques.
2. Explain the purpose of S-boxes in the design of DES.
3. Explain the key expansion algorithm used in AES algorithm.
4. What is the difference between modular arithmetic and ordinary arithmetic?
5. Give two applications of public key cryptosystems.
6. What is the difference between weak and strong collision resistance?
7. What requirements should a digital signature scheme satisfy?
8. What are security associations?
9. Explain transport mode of IPSec operation.
10. What is an application level gateway?

(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. (a) Discuss the security of AES algorithm.

(b) Explain linear and differential cryptanalysis.

OR

12. Explain IDEA encryption algorithm.

Module – II

13. (a) Explain Diffie-Hellman key exchange algorithm.

(b) Explain Digital Signature Standards.

OR

14. (a) Explain RSA algorithm.

(b) Discuss Secure Hash Algorithm.

Module – III

15. (a) Describe S/MIME protocol used for providing email security.

(b) What are secure electronic transactions?

OR

16. (a) Explain SSL protocol.

(b) What are dual signatures?

(3 × 20 = 60 Marks)