(Pages : 3) **N – 5775**

Reg. No .....

Name : .....

Eighth Semester B.Tech. Degree Examination, April 2022

(2013 Scheme)

13.801 : CRYPTOGRAPHY AND NETWORK SECURITY (R)

Time : 3 Hours Max. Marks : 100

PART – A

Answer **all** questions, each question carries **4** marks.

1. What is *diffusion* in cryptography?
2. Write short note on *caeser* cipher.
3. State Fermat's little Theorem.
4. Explain the term HTTPS.
5. Explain the term S/MIME.

(5 × 4 = 20 Marks)

PART – B

Answer **any one full** questions from **each** Module.

Module – I

6. (a) Explain IDEA algorithm. **10**

   (b) Explain DES algorithm with block diagrams. **10**

OR

7. (a) Explain AES algorithm with block diagrams. **16**

(b) What is 3 DES? Explain. **4**

Module – II

8. (a) Explain RSA algorithm with suitable example. **10**

(b) Explain Diffie Hellman key exchange algorithm. **10**

OR

9. (a) Calculate 3G with respect to elliptic curve crypto system E11(1, 6) (select G as (2, 7)). **12**

(b) Explain Elliptic Curve cryptography. **4**

(c) What are the advantages of elliptic curve cryptography over RSA algorithm? **4**

Module – III

10. (a) Explain different PGP cryptographic functions with diagrams. **12**

(b) Explain transmission and reception of PGP messages using flow charts. **8**

OR

11. (a) What is the difference between transport mode SA and Tunnel mode SA in the context of IP security? **13**

(b) Explain different types of services of IPSec at IP layer. **7**

Module – IV

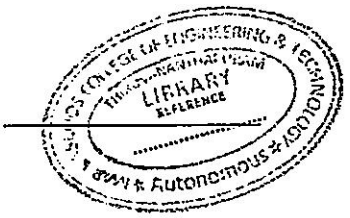
12. (a) Explain different types of firewalls with neat diagrams. **16**

(b) Write short note on secure electronic transactions. **4**

OR

13. (a) Explain TLS function with block diagrams. **8**

(b) Explain SSL hand shake protocol actions with diagram. **12**



(4 × 20 = 80 Marks)