(Pages : 2) **1126**

Reg. No. : .....

Name : .....

Eighth Semester B.Tech. Degree Examination, April 2014
(2008 Scheme)
08.803 : CRYPTOGRAPHY AND NETWORK SECURITY (R)

Time : 3 Hours Max. Marks : 100

PART – A

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

1. Distinguish between a monoalphabetic and a polyalphabetic cipher.
2. Distinguish between diffusion and confusion.
3. What is double DES ? What kind of attack on double DES makes it useless ?
4. List the parameters (block size, key size and the number of rounds) for the three AES versions.
5. Define a trapdoor one way function and explain its use in asymmetric key cryptography.
6. List the security services provided by a digital signature.
7. Compare and contrast existential and selective forgery.
8. Explain how Bob finds out what cryptographic algorithms Alice has used when he receives a PGP message from her.
9. Distinguish between two modes of IPSec.
10. What are encrypted tunnels ? **(10×4=40 Marks)**

PART – B

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

Module – I

11. a) Discuss about the different transposition techniques used in cryptography. **8**
    b) Discuss about the security of AES algorithm. **12**

OR

12. Explain AES Encryption algorithm. **20**

Module – II

13. a) Explain Diffie Hellman Key Exchange algorithm. 10

    b) Discuss about RSA cryptosystem. 10

OR

14. a) Explain Secure Hash Algorithm. 10

    b) Discuss about Digital Signature Standards. 10

Module – III

15. a) Explain Secure Socket Layer protocol. 10

    b) Explain Pretty Good Privacy protocol for email security. 10

OR

16. a) Discuss about the different types of firewalls. 8

    b) Explain the two security protocols defined by IPSec. 12