(Pages : 2) **5829**

Reg. No. : .....

Name : .....

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

Time : 3 Hours Max. Marks : 100

PART – A

Answer **all** questions.

1. Discuss the key generation in SDES.
2. Differentiate unconditionally secure and computationally secure algorithms.
3. Define strict avalanche criterion and bit independence criterion.
4. What is inverse cipher ?
5. What are the requirements of public key cryptography ?
6. What are the different techniques used for distributing public keys ?
7. What are the requirements of hash function ?
8. What is the use of passphrase based key in PGP ?
9. What are the services provided by SSL Record Protocol ?
10. List the functions provided by S/MIME. **(10×4=40 Marks)**

PART – B

Answer **any one** question from **each** Module.

Module – I

11. a) Explain the various substitution techniques in detail. **14**
    b) Write short notes on Rotor machines. **6**

OR

12. a) Explain the cipher feedback mode and output feedback mode. 10

    b) Explain the AES key expansion algorithm with neat sketch. 10

Module – II

13. Explain RSA algorithm and its computational aspects. 20

OR

14. a) Explain MD5 algorithm. 15

    b) Give the differences between MD5 and SHA – 1. 5

Module – III

15. Explain in detail about PGP. 20

OR

16. a) Explain the encapsulation security payload in detail. 10

    b) Explain the operation of SSL Record Protocol. 10