(Pages : 2) **6865**

Reg. No. : .....

Name : .....

Eighth Semester B.Tech. Degree Examination, November 2013
(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 stream cipher and a block cipher.
2. Define an S-box and mention the necessary condition for an S-box to be invertible.
3. Explain differential and linear cryptanalysis.
4. Define a state in AES. How many states are there in each version of AES ?
5. Define Fermat's little theorem and explain its application.
6. Distinguish between message integrity and message authentication.
7. Define a cryptographic hash function.
8. Explain how Bob finds out what cryptographic algorithms Alice has used when he receives a S/MIME message from her.
9. What are security associations ?
10. What is the difference between a firewall and an Intrusion Detection System ?

PART – B

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

MODULE – I

11. a) Discuss about the different substitution techniques used in cryptography.
    b) Explain Fiestel cipher model. **20**

OR

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

P.T.O.

MODULE – II

13. Explain :
    a) Write key exchange algorithm using ECC. 12
    b) Use of modular arithmetic in cryptography. 8

OR

14. a) What are digital signatures ? Write DSA algorithm. 10
    b) Explain MD 5 algorithm. 10

MODULE – III

15. a) What is Secure Electronic Transaction ? What are the key features of SET ? Explain the various categories of SET participants. 12
    b) Write short notes on Dual signature. 8

OR

16. a) Explain IPSec Architecture. 12
    b) Name different protocols in SSL. 8