(Pages : 2) **2022**

Reg. No. : .....

Name : .....

Eighth Semester B.Tech Degree Examination, May 2013
(2008 Scheme)
08.803 : CRYPTOGRAPHY AND NETWORKS SECURITY (R)

Time : 3 Hours Max. Marks : 100

PART – A

Answer **all** questions. **Each** question carries **4** marks. **(10×4=40 Marks)**

1. Encrypt the message 'she is listening music', using Vigenere cipher with 'PASCAL' as the initial secret key.
2. Explain computationally secure cipher and unconditionally secure cipher.
3. What is steganography ?
4. Compare cipher feedback mode and output feedback mode.
5. What are the basic requirements that should be possessed by a digital signature ?
6. How is authentication achieved in public-key cryptography ?
7. Give examples of replay attacks.
8. What are the different applications of IPSec ?
9. What is the difference between SSL connection and SSL session ?
10. What are the basic approaches in bundling security associations ?

P.T.O.

PART – B

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

Module – I

11. Explain the following :
    i) One-time pad
    ii) Auto key cipher
    iii) Hill cipher
    iv) Keyed transposition cipher
    v) Caesar cipher **20**

OR

12. a) Explain IDEA algorithm. **10**
    b) Explain the different steps in Fiestal Encryption with a classical Fiestal network. **10**

Module – II

13. a) Explain Direct Digital Signature and Arbitrated Digital signature. **10**
    b) Explain the following schemes used in distribution of public keys.
    i) Public-key authority and ii) Public-key certificate. **10**

OR

14. a) Explain the Diffic-Helman Key exchange algorithm. **10**
    b) Explain Digital Signature algorithm. **10**

Module – III

15. a) Explain the working of packet filtering router. **10**
    b) Give the different attacks possible on packet filtering router and the appropriate counter measures taken. **5**
    c) What is the difference between a packet filtering router and a stateful inspection firewall ? **5**

OR

16. a) What is PGP ? Briefly explain the general format of a PGP message. **10**
    b) What are the limitations of SMTP ? How does MIME overcome the limitations of SMTP ? **10**