(Pages : 2) **1928**

Reg. No. : ....

Name : ....

Seventh Semester B.Tech. Degree Examination, May 2014
(2008 Scheme)
08.703 : CRYPTOGRAPHY (F)

Time: 3 Hours Max. Marks: 100

PART – A

Answer **all** questions :

1. Explain the various cryptanalytic attacks based on the amount of information known to cryptanalyst.

2. Encrypt the message "TO BE OR NOT TO BE" using Vigenere cipher with keyword "HAMLET".

3. What do you mean by absolute security ?

4. What is a fair cryptosystem ?

5. What is the need for link encipherment and how it is used ?

6. What are the random properties of shift register sequences ?

7. What is the purpose of S-boxes in DES ?

8. What do you mean by zero knowledge techniques ?

9. Discuss the characteristics of a good message authentication code.

10. Define block enciphering. **(10×4=40 Marks)**

P.T.O.

PART – B

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

Module – I

11. a) Explain how Hagelin machine works.

    b) Discuss error probability and security.

    c) What is unicity distance ? Explain.

OR

12. a) Explain the different aspects of security.

    b) Explain the various substitution ciphers. Give examples of each.

Module – II

13. a) Explain how DES works.

    b) Discuss the structure and working of IDEA.

OR

14. a) Explain RSA algorithm with a suitable example.

    b) Explain in detail about the public key systems with elliptical curves.

Module – III

15. a) Discuss message authentication with MAC.

    b) What are the advantages and disadvantages of digital signature algorithm ?

OR

16. a) What is birthday attack ? Explain.

    b) Explain how key management is done for network security. **(3×20=60 Marks)**

———————