(Pages : 2) **5612**

Reg. No. : .....

Name : .....

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

Time : 3 Hours Max. Marks : 100

PART – A

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

1. What is absolute security ?
2. Define key equivocation.
3. What is chi test ?
4. Define generating function.
5. What is the purpose of S-boxes in DES ?
6. Differentiate weak and semi-weak keys.
7. Write important aspects of public key systems.
8. What is birthday attack ?
9. In what ways can a hash value be secured so as to provide message authentication ?
10. Compare Link encryption with End-to-End encryption. **(10×4=40 Marks)**

P.T.O.

PART – B

Answer **any one full** question from **each** Module. **All** questions carry **20** marks.

Module – I

11. Write short notes on :

    a) Vigenere cipher

    b) Kasiski test

    c) Pure cipher

    d) Coincidence Index. **20**

OR

12. a) Summarize the differences between stream and block cipher systems. **10**

    b) Discuss about information measure and practical security. **10**

Module – II

13. a) Give analysis of DES. **10**

    b) Explain working of IDEA. **10**

OR

14. Write notes on :

    a) Euclidean algorithm

    b) Jacobi symbol. **20**

Module – III

15. Discuss about key distribution for symmetrical algorithms. **20**

OR

16. a) Explain working of fair crypto systems. **10**

    b) Write advantages and disadvantages of digital signature algorithms. **10**
