Reg. No. : | | | | | | | | | | | | |

Question Paper Code : 60339

B.E./B.Tech. DEGREE EXAMINATION, MAY/JUNE 2012.

Seventh Semester

Computer Science and Engineering

IT 1352/070250033/070230074— CRYPTOGRAPHY AND NETWORK SECURITY/NETWORK PROGRAMMING AND MANAGEMENT

(Common to Sixth Semester Information Technology)

(Regulation 2004)

(Common to B.E. (Part-Time) Sixth Semester Computer Science and Engineering Regulation 2005)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Define : Integrity, Access control.
2. What is the difference between active and passive attack?
3. What are the two problems of one time key pad?
4. Define : Confidentiality.
5. List out the differences between MD4 and MD5 algorithm.
6. List out the authentication protocols.
7. Define : PGP.
8. Define : IP security.
9. What is the use of firewall in system level security?
10. Define : Intrusion detection.

PART B — (5 × 16 = 80 marks)

11. (a) Explain the DES algorithm in detail.

Or

(b) Explain the Hill cipher algorithm with one example.

12. (a) Write elaborate notes on key management in public key cryptography.

Or

(b) Explain the Elliptic curve architecture.

13. (a) Illustrate about the HMAC digital signatures in authentication.

Or

(b) Explain about the RIPMED in detail.

14. (a) Describe the various aspects of Kerberos-X.509 in detail.

Or

(b) Describe the web security in detail.

15. (a) List out the viruses and related threats and explain them in detail.

Or

(b) Explain the password management in system level security.
