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

Question Paper Code : Q 2284

B.E/B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2009.

Sixth Semester

Information Technology

IT 1352 — CRYPTOGRAPHY AND NETWORK SECURITY

(Regulation 2004)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What are the types of security attacks?

2. What are the strengths of DES algorithm?

3. List out the ingredients of Public key encryption scheme.

4. Write down the difference between conventional encryption and public key encryption.

5. What is Message Authentication Code (MAC)?

6. What are the requirements of Hash functions?

7. What is S/MIME?

8. What are the applications of IP Security?

9. Define Honeypots.

10. List out the types of Viruses.

PART B — (5 × 16 = 80 marks)

11. (a) With the help of the block diagram, explain the AES encryption and decryption processes in detail.

Or

(b) Write about the

(i) Triple DES and its applications (10)

(ii) Placement of Encryption Function. (6)

12. (a) What is public key cryptography and when is it preferred? Describe in detail the RSA algorithm with computational aspects.

Or

(b) Discuss the importance of key management? Describe in detail the Diffie-Hellman key exchange algorithm and the Man-in-the-middle attack.

13. (a) Where Hash functions are used? What characteristics are needed in secure hash function? Write about the Security of Hash Functions and MACs.

Or

(b) What are the basic arithmetic and logical functions used in SHA. Discuss in detail.

14. (a) Explain the functions of Kerberos authentication server and differentiate Kerberos version 4 and Kerberos version 5.

Or

(b) What is Secure Electronic Transaction? List and briefly define the categories of SET participants.

15. (a) What is the role of Intrusion Detection System? What are the three benefits that can be provided by the Intrusion Detection System? What are the differences between the statistical anomaly detection and rule based intrusion detection system?

Or

(b) What are the demerits of not using Firewall? List the design goals of firewall. Explain the types of the firewalls with design principles.
