Reg. No. : ☐☐☐☐☐☐☐☐☐☐☐☐

C 3342

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2008.

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. The given cipher text is "ybpq lc irzh". Find the plain text when the key is "monoalphabetic cipher" with $x = x + 3$.

2. Write down the evaluation criteria for AES.

3. Elliptic curve system use what formula to determine the relationship between public and private keys within the universe created by an elliptic curve.

4. Write down the principle behind RSA's secure model.

5. Blow fish algorithm is specially employed for maintaining what?

6. The TKIP – The temporal key integrity protocol is implemented on what principles.

7. Internet – Engineering Task Force defines IP security as what? and in what two modes it is operated?

8. List the benefits of Kerberos.

9. How is a worm different from a virus? and state what is a macrovirus.

10. "Host based IDS are in some way better than NIDs". Justify.

PART B — (5 × 16 = 80 marks)

11. (a) From the first principles derive how Triple DES generates and distributes key choosing suitable environment and data.

Or

(b) Summarise the salient features of various classical Encryption techniques.

12. (a) Show how Diffie-Hellman key exchange is used for key management schemes.

Or

(b) Explain the process of generation of an RSA key pair assuming suitable data.

13. (a) Discuss about the security of Hash functions and MAC's.

Or

(b) Brief on the requirements of Authentication and Enlist the features of various Authentication protocols.

14. (a) Enumerate the X.509 Authentication Services.

Or

(b) (i) How do you provide Electronic Mail Security?

(ii) What are known as cookies, Honey pots and sniffer dogs? In which part of the network are they placed?

15. (a) Briefly give a note on the various viruses and related threats affecting the security of networks and the counter measures employed in handling them.

Or

(b) What are the limitations of firewall?

(i) Is firewall the ultimate solution? How can this be cracked?

(ii) How is a firewall designed?

———————

C 3342