ANNA UNIVERSITY

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2011.

Seventh Semester

Computer Science and Engineering

IT 2352 – CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Sixth Semester Information Technology)

(Regulation 2008)

Time : Three hours **Maximum : 100 marks**

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Give the types of attack.
2. List out the problems of one time pad?
3. Write down the purpose of the S-Boxes in DES?
4. Define : Diffusion.
5. Define: Replay attack.
6. List out the parameters of AES.
7. Define : Primality test.
8. State the difference between conventional encryption and public-key encryption.
9. Define : Malicious software.
10. Name any two security standards.

PART B — (5 × 16 = 80 marks)

11. (a) Using play fair cipher algorithm encrypt the message using the key "MONARCHY" and explain.

Or

(b) Explain the ceaser cipher and monoalphabetic cipher.

12. (a) Explain the Key Generation, Encryption and Decryption of SDES algorithm in detail.

Or

(b) Write the algorithm of RSA and explain with an example.

13. (a) Illustrate about the SHA algorithm and explain.

Or

(b) Write a detailed note on Digital signatures.

14. (a) Describe the SSL Architecture in detail.
Or
(b) List out the participants of SET system, and explain in detail.

15. (a) Explain the types of Intrustion Detection Systems.
Or
(b) Explain the different types of firewall and its configurations in detail.