Reg. No. : □□□□□□□□□□□□

Question Paper Code : 21513

B.E./B.Tech. DEGREE EXAMINATION, MAY/JUNE 2013.

Seventh Semester

Computer Science and Engineering

IT 2352/IT 62/10144 IT 603 – CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Information Technology – Sixth Semester)

(Regulation 2008 / 2010)

Time : Three hours | Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Convert the given text "anna university" into cipher text using rail fence technique.

2. Define steganography.

3. What is the disadvantages with ECB mode of operation?

4. Find GCD (21,300) using Euclid's algorthim.

5. Define discrete logarithm.

6. What is weak collision resistance? What is the use of it?

7. List out the services provided by PGP.

8. Expand and define SPI.

9. Mention the two levels of hackers.

10. What is logic bomb?

PART B — (5 × 16 = 80 marks)

11. (a) Write about any two classical crypto systems (substitution and transposition) with suitable examples.

Or

(b) Write about Fermat and Euler's theoram in detail.

12. (a) Explain briefly about DES in detail.

Or

(b) Explain about RSA with one suitable example.

13. (a) Explain about secure hash algorithm (SHA) in detail.

Or

(b) Explain about Diffie Hellman Key exchange algorithm with one suitable example.

14. (a) Discuss about X.509 authentication service in detail.

Or

(b) Explain about S/MIME in detail.

15. (a) Write about virus and related threats in detail.

Or

(b) Explain briefly about trusted system.

———————