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

Question Paper Code : 51560

B.E./B.Tech. DEGREE EXAMINATION, MAY/JUNE 2014.

Seventh Semester

Computer Science and Engineering

IT 2352/IT 62/10144 IT 603/10144 CSE 46 — CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Sixth Semester – Information Technology)

(Regulation 2008/2010)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What are active and passive attacks that compromise information security?

2. Why random numbers are used in network security?

3. State Euler's theorem.

4. What is Optimal Asymmetric Encryption Padding?

5. What is discrete logarithm problem?

6. State whether symmetric and asymmetric cryptographic algorithms need Key Exchange.

7. List the authentication requirements.

8. What are birthday attacks?

9. Differentiate spyware and virus.

10. What are zombies?

PART B — (5 × 16 = 80 marks)

11. (a) Explain any two classical ciphers and also describe their security limitations.

Or

(b) Describe Linear Feedback Shift Registers Sequences and Finite Fields with their application in cryptography.

12. (a) Describe the working principle of Simple DES with an example.

Or

(b) (i) Explain RSA algorithm. (8)

(ii) Demonstrate encryption and decryption for the RSA algorithm parameters: p = 3, q = 11, e = 7, d = ?, M = 5. (8)

13. (a) Explain Digital Signature Standard.

Or

(b) (i) Briefly explain Diffie-Hellman Key Exchange. (8)

(ii) Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root α=7. If user A has private key $X_A = 5$, what is A's public key Y_A? (8)

14. (a) Elaborately explain Kerberos authentication mechanism with suitable diagrams.

Or

(b) Explain Pretty Good Privacy in detail.

15. (a) Explain statistical anomaly detection and rule based intrusion detection.

Or

(b) Describe any two advanced anti-virus techniques in detail.