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

Question Paper Code : 71763

B.E./B.Tech. DEGREE EXAMINATION, APRIL/MAY 2015.

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)

(Common to PTIT 2352 – Cryptography and Network Security for B.E. (Part-Time) Seventh Semester – Computer Science and Engineering – Regulation 2009)

Time : Three hours Maximum : 100 marks

(Codes/Tables/Charts to be permitted, if any, may be indicated)

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Differentiate between active attacks and passive attacks.
2. Find 11^7 mod 13.
3. Differentiate between stream ciphers and block ciphers.
4. State few applications of RC4 algorithm.
5. What is primitive root?
6. What is digital Signature?
7. When are the certificates revoked in X.509?
8. What is tunnel mode in IP Security?
9. Define Worm.
10. What is the advantage of Intrusion detection system over firewall?

PART B — (5 × 16 = 80 marks)

11. (a) Explain the Substitution encryption techniques in detail. (16)

Or

(b) State and derive

(i) Fermat's theorem (8)

(ii) Euler's theorem. (8)

12. (a) Explain Data Encryption Standard (DES) in detail. (16)

Or

(b) Explain the RSA algorithm in detail. For the given values, trace the sequence of calculations in RSA. P=7, q=13, e=5 and M=10. (16)

13. (a) Explain ElGamal public key cryptosystems with an example (16)

Or

(b) Explain Secure Hash in detail. (16)

14. (a) Explain Kerberos Version 4 in detail. (16)

Or

(b) Explain Secure Socket Layer (SSL) in detail. (16)

15. (a) Write brief notes on the following :

(i) Classification of viruses (8)

(ii) Worm Counter measures. (8)

Or

(b) Explain the characteristics and types of firewalls. (16)

———————