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

Question Paper Code : 80304

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2016.

Seventh Semester

Computer Science and Engineering

CS 6701 — CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Seventh Semester Information Technology)

(Regulations 2013)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Compare active and passive attack.
2. Find gcd (1970, 1066) using Euclid's algorithm.
3. Brief the strengths of triple DES.
4. What is an elliptic curve?
5. State any three requirements for authentication.
6. Differentiate MAC and Hash function.
7. List the three classes of intruders.
8. Define Zombie.
9. List the limitations of SMTP/RFC 822.
10. Define Botnets.

PART B — (5 × 16 = 80 marks)

11. (a) (i) Explain OSI Security Architecture model with neat diagram. (8)

(ii) Describe the various security mechanisms. (8)

Or

(b) (i) State Chinese Remainder theorem and find X for the given set of congruent equations using CRT.

$X = 2 \pmod 3$

$X = 3 \pmod 5$

$X = 2 \pmod 7$. (8)

(ii) State and prove Fermat's theorem. (8)

12. (a) Explain AES algorithm with all its round functions in detail. (16)

Or

(b) Explain RSA algorithm, perform encryption and decryption to the system with $p = 7$; $q = 11$; $e = 17$; $M = 8$. (16)

13. (a) Describe MD5 algorithm in detail. Compare its performance with SHA-1. (16)

Or

(b) Explain digital signature standard with necessary diagrams in detail. (16)

14. (a) Discuss Client Server Mutual authentication, with example flow diagram. (16)

Or

(b) Explain the technical details of firewall and describe any three types of firewall with neat diagram. (16)

15. (a) Discuss the working of SET with neat diagram. (16)

Or

(b) Explain the operational description of PGP. (16)
