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

**Question Paper Code : 71690**

B.E./B.Tech. DEGREE EXAMINATION, APRIL/MAY 2017.

Seventh/Eighth Semester

Computer Science and Engineering

CS 6701 — CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Electronics and Communication Engineering and Information Technology)

(Regulations 2013)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. State Fermat's theorem.
2. Determine the gcd (24140, 16762) using Euclid's algorithm.
3. State the difference between private key and public key algorithm.
4. Give the five modes of operation of block cipher.
5. What is the role of compression function in hash function?
6. Specify the various types of authentication protocol.
7. Define the roles of firewalls.
8. State the difference between threats and attacks.
9. Draw the ESP packet format.
10. Specify the benefits of IPSec.

PART B — (5 × 16 = 80 marks)

11. (a) State Chinese Remainder theorem and find X for the given set of congruent equations using CRT (16)

$X \equiv 1 \pmod 5$

$X \equiv 2 \pmod 7$

$X \equiv 3 \pmod 9$

$X \equiv 4 \pmod{11}$

Or

(b) Describe :

(i) Playfair cipher

(ii) Railfence cipher

(iii) Vignere cipher. (16)

12. (a) Explain Diffie-Hellman Key exchange algorithm in detail. (16)

Or

(b) Describe DES algorithm with neat diagram and explain the steps. (16)

13. (a) Compare the performance of RIPEMD-160 algorithm and SHA-1 algorithm. (16)

Or

(b) Explain the concepts of Digital signature algorithm with key generation and verification in detail. (16)

14. (a) Discuss the different types of virus in detail. Suggest scenarios for deploying these types in network scenario. (16)

Or

(b) Explain Intrusion Detection System (IDS) in detail with suitable diagram. (16)

15. (a) Explain the architecture of IP security in detail. (16)

Or

(b) Discuss authentication header and ESP in detail with their packet format. (16)

———————