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

Question Paper Code : 52874

B.E./B.Tech. DEGREE EXAMINATIONS, APRIL/MAY 2019.

Seventh/Eighth Semester

Computer Science and Engineering

CS 6701 — CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Electronics and Communication Engineering/Information Technology)

(Regulation 2013)

(Also common to PTCS 6701 — Cryptography and Network Security for B.E. (Part-Time) — Sixth Semester – Computer Science and Engineering – Regulation 2014))

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Differentiate active and passive attacks.
2. Specify the components of encryption algorithm.
3. Give the applications of the public key cryptosystem.
4. What are primitive operations used in RC5?
5. What are the requirements for message authentication?
6. Show how SHA is more secure than MD5.
7. List the design goals of firewalls.
8. List the three classes of intruders.
9. Mention the five header fields defined in MIME.
10. What are the benefits of IP Security?

PART B — (5 × 13 = 65 marks)

11. (a) (i) What is steganography? Describe the various techniques used in steganography. (7)

(ii) What is monoalphabetic cipher? Examine how it differs from Caesar cipher. (6)

Or

(b) Explain the network security model and its important parameters with a neat block diagram.

12. (a) (i) Describe in detail the key generation in AES algorithm and its expansion format. (7)

(ii) Describe triple DES and its applications. (6)

Or

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

(ii) Perform encryption and decryption using RSA algorithm for the following : $p = 7$, $q = 11$, $e = 7$, $M = 9$. (5)

13. (a) Describe digital signature algorithm and show how signing and verification is done using DSS.

Or

(b) Describe the MD5 message digest algorithm with necessary block diagrams.

14. (a) (i) What is Kerberos? Explain how it provides authenticated service. (7)

(ii) Explain the format of the X.509 certificate. (6)

Or

(b) Explain the various types of firewalls with neat diagrams.

15. (a) Explain PGP cryptographic functions in detail with suitable block diagrams.

Or

(b) Explain the architecture of IPsec in detail with a neat block diagram.

PART C — (1 × 15 = 15 marks)

16. (a) (i) Explain briefly about Diffie Hellman key exchange algorithm with its merits and demerits. (10)

(ii) Explain public key cryptography and when it is preferred? (5)

Or

(b) Solve using playfair cipher method. Encrypt the word "Semester Result" with the keyword "Examination". Discuss the roles to be followed.