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

Question Paper Code : 20375

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2018.

Seventh/Eighth Semester

Computer Science and Engineering

CS 6701 — CRYPTOGPAPHY AND NETWORK SECURITY

(Regulations 2013)

(Common to Electronics and Communication Engineering, Information Technology)

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

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Distinguish between attack and threat.
2. Calculate the cipher text for the following using one time pad cipher.
   Plain Text: ROCK & Keyword: BOTS
3. Compare DES and AES.
4. Why is trap door one way function used?
5. Define the term message digest.
6. Contrast various SHA algorithms.
7. List various types of firewall.
8. Discriminate statistical anomaly detection and rule based detection.
9. What are the services provided by PGP?
10. Differentiate transport and tunnel mode in IPSec.

PART B — (5 × 13 = 65 marks)

11. (a) Solve gcd (98, 56) using Extended Euclidean algorithm. Write the algorithm also.

Or

(b) Perform Encryption and decryption using Hill Cipher for the following:
Message PEN and Key: ACTIVATED.

12. (a) Perform encryption and decryption using RSA algorithm for p = 17, q = 11, e = 7 and M = 88.

Or

(b) Find the secret key shared between user A and user B using Diffie Hellman algorithm for the following.

q = 353; α (primitive root) = 3, X_A = 45 and X_B = 50

13. (a) Illustrate SHA2 in detail.

Or

(b) Explain Elgamal digital signature scheme.

14. (a) Analyze various types of virus and its counter measures.

Or

(b) Illustrate the working principle of SET. Relate SET for E-commerce applications.

15. (a) Explain in detail about S/MIME.

Or

(b) Describe in detail about SSL/TLS.

PART C — (1 × 15 = 15 marks)

16. (a) Why ECC is better than RSA? However, why is it not widely used? Defend it.

Or

(b) Evaluate the performance of PGP. Compare it with S/MIME.

———————