

Reg. No. :

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Question Paper Code : 10462

B.E./B.Tech. DEGREE EXAMINATIONS, APRIL/MAY 2025.

Sixth/Seventh Semester

Computer Science and Engineering

CS 8792 – CRYPTOGRAPHY AND NETWORK SECURITY

(Common to : Computer and Communication Engineering/Electronics and
Communication Engineering/Electronics and Telecommunication
Engineering/Information Technology)

(Regulations 2017)

Time : Three hours

Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Define masquerade attack.
2. What is steganography?
3. Find GCD(710,90) using Euclidean algorithm.
4. List any two properties of congruences.
5. Find $Q(21)$.
6. Why Fermat's Algorithm is used?
7. Differentiate : MAC and Hash.
8. What is meant by Kerberos Realm?
9. How virus and worms are different?
10. Why firewalls are used?

PART B — (5 × 13 = 65 marks)

11. (a) (i) Let consider that message “university”, key = “btech”, find ciphertext using playfair cipher. (8)
(ii) Describe various security mechanisms. (5)

Or

- (b) (i) Let consider that message = “anna university”, key = 3124576, find ciphertext using Transposition cipher. (8)
(ii) Discuss various type of attacks. (5)
12. (a) With neat diagram, briefly explain the functionality of DES, with the number of bits in each flow of data.

Or

- (b) Discuss the four major key operations in AES with the mathematical and technical factors.
13. (a) (i) Write short notes on elliptic curve cryptography. (6)
(ii) Encrypt using ElGamal: prime number (p) = 3, primitive root (g) = 3, message (m) = 13. (7)

Or

- (b) User X and Y exchange the key using Diffie-Hellmann algorithm, where $q = 11$ and the primitive root (alpha) is 7.
(i) Find A's public key Y_A , if user A has a private key $X_A = 3$? (4)
(ii) Find A's public key Y_A , if user A has a private key $X_B = 6$? (4)
(iii) Explain the process step-by-step with the shared key. (5)

14. (a) Discribe the functionalities of X.509.

Or

- (b) Illustrate : SHA1 with neat diagram.
15. (a) Discuss the seven types of MIME content types.

Or

- (b) Draw IPsec Authentication Header and write short notes on each element of the Header.

PART C — ($1 \times 15 = 15$ marks)

16. (a) A box contains gold coins. If the coins are equally divided among three friends, two coins are left over, if the coins are equally divided among five friends, three coins are left over, if the coins are equally divided among seven friends, two coins are left over. If the box holds smallest number of coins that meets these conditions, how many coins are there? (Hint : Use Chinese Remainder Theorem).

Or

- (b) Perform encryption and decryption using RSA algorithm, where $p = 3$, $q = 11$. Also list out possible threats to RSA algorithm and its countermeasures.
-

