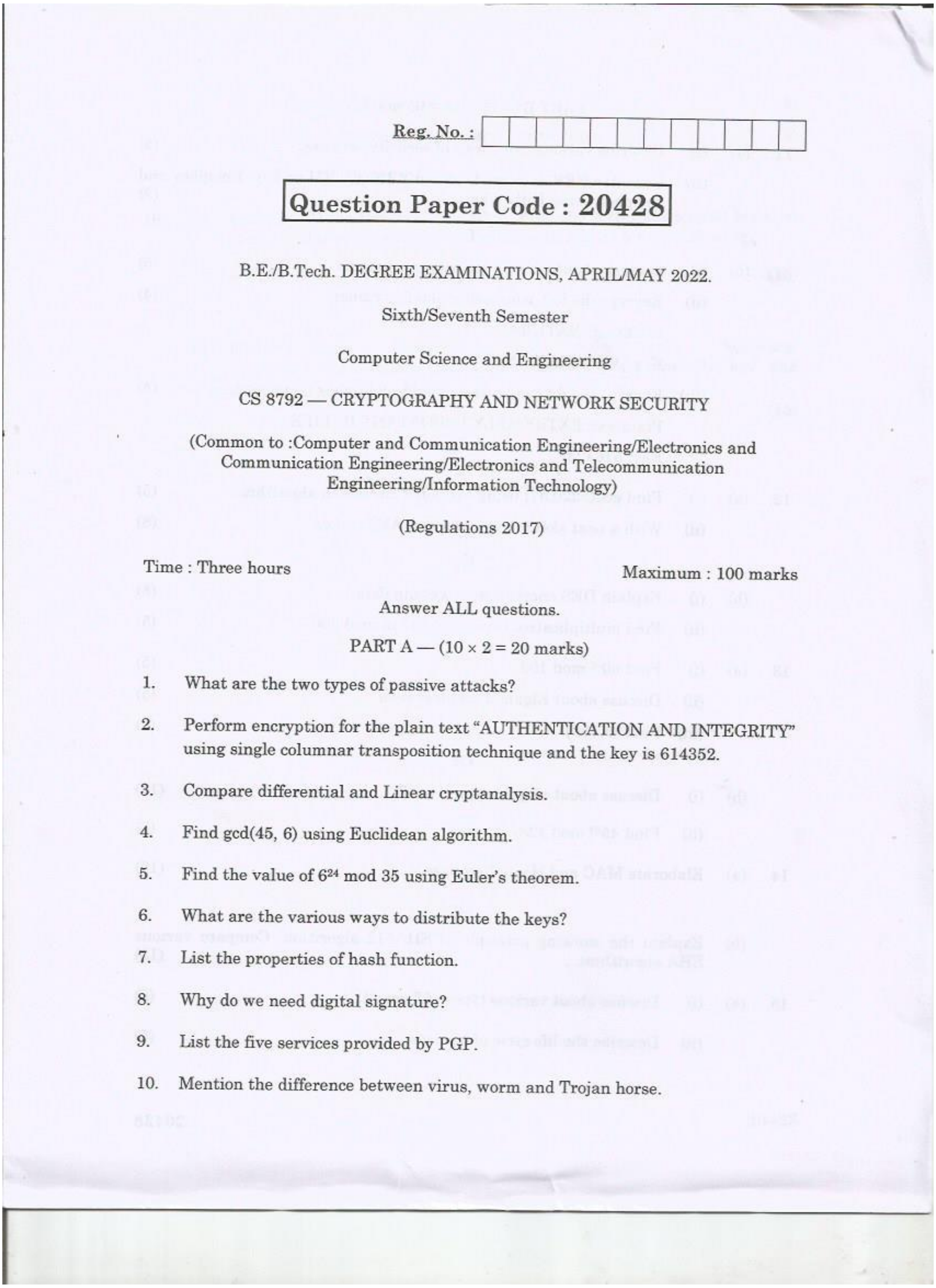

Reg. No. : □□□□□□□□□□□□

Question Paper Code : 20428

B.E./B.Tech. DEGREE EXAMINATIONS, APRIL/MAY 2022.

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. What are the two types of passive attacks?

2. Perform encryption for the plain text "AUTHENTICATION AND INTEGRITY" using single columnar transposition technique and the key is 614352.

3. Compare differential and Linear cryptanalysis.

4. Find gcd(45, 6) using Euclidean algorithm.

5. Find the value of 6^{24} mod 35 using Euler's theorem.

6. What are the various ways to distribute the keys?

7. List the properties of hash function.

8. Why do we need digital signature?

9. List the five services provided by PGP.

10. Mention the difference between virus, worm and Trojan horse.

PART B — (5 × 13 = 65 marks)

11. (a) (i) Describe various categories of security services. (5)

(ii) Consider KEY as plain text and PRFVSUJCJ as key. Encipher and decipher using Hill cipher. (8)

Or

(b) (i) Discuss about various security mechanisms. (5)

(ii) Encrypt the following using playfair cipher. (4)

Plaintext: NATURAL

Key: VEGETATION

(iii) Encrypt the following using double columnar transposition. (4)

Plaintext: EXTREMELY IMPORTANT IN LIFE

Key: 516423

12. (a) (i) Find gcd(5220,57) using extended Euclidean algorithm. (5)

(ii) With a neat sketch explain about AES cipher. (8)

Or

(b) (i) Explain DES encryption process in detail. (8)

(ii) Find multiplicative inverse of 457 in mod 896. (5)

13. (a) (i) Find 60^{-1} mod 103. (5)

(ii) Discuss about Elgamal cryptosystem (5)

(iii) Find $\Phi(458)$. (3)

Or

(b) (i) Discuss about elliptic curve over Z_p. (10)

(ii) Find 45^{67} mod 123. (3)

14. (a) Elaborate MAC and Hash. Compare it. (13)

Or

(b) Explain the working principle of SHA512 algorithm. Compare various SHA algorithms. (13)

15. (a) (i) Discuss about various types of firewall. (8)

(ii) Describe the life cycle of Viruses. (5)

Or

(b) (i) Elaborate various IPSec services. (8)

(ii) Discuss the requirements and key features of SET. (5)

PART C — (1 × 15 = 15 marks)

16. (a) Elaborate Diffie-Heilman algorithm. Find the secret key shared between user A and user B using Diffie-Hellman algorithm for the following.

$q = 257; \alpha = 3, X_A = 256$ and $X_B = 48$ (15)

Or

(b) Write RSA algorithm and Solve the following: $p = 47$; $q = 71$; $e = 79; M = 456$. Find public key and private key and perform encryption and decryption. (15)

———————