C1003

Total Pages : 3 Roll No. ....

PGDCS-08

Computational Number Theory & Cryptography

(PGDCS-17)

2nd Semester Examination, 2022 (June)

Time : 2 Hours] **Max. Marks : 80**

Note : This paper is of Eighty (80) marks divided into two (02) Sections A and B. Attempt the questions contained in these sections according to the detailed instructions given therein.

SECTION–A

(Long Answer Type Questions)

Note : Section 'A' contains Five (05) long answer type questions of Twenty (20) marks each. Learners are required to answer any Two (02) questions only.

(2×20=40)

1. What is hash in cryptography? Explain SHA hash function in detail.

2. What do you understand by key exchange in crptography? Illustrate any key exchange algorithm with example.

3. State and Prove Chinese Remainder theorem. Find all the solutions of $x^2 = 1 \pmod{144}$.

4. Explain Diffie – Hellman key exchange with algorithm.

5. What do you understand by digital signature and digital certificate? Explain how digital signature are different from authentication protocol.

SECTION–B

(Short Answer Type Questions)

Note : Section 'B' contains Eight (08) short answer type questions of Ten (10) marks each. Learners are required to answer any Four (04) questions only. (4×10=40)

1. What are the principle elements of a public-key cryptosystem?

2. Explain Stream Cipher in crptography.

3. Prove that if AKS algorithm returns Prime then n is prime.

4. What are the various security features of Elliptic curve crptography?

5. Explain time and space complexity with example.

6. Explain in detail the various categories of application of public-key cryptosystems.

7. Define Zero Knowledge proof for Elliptic Curve Discrete Logarithm Problem (ECDLP).

8. Explain Elgamal crptosystem and Massey Omura Cryptosystem.