827

Total pages : 03 Roll No. .....

MIT (CS)-204/PGDCS-08

Computational Number Theory & Cryptography

(MSCCS-18/PGDCS-17)

Examination 2021 (Winter)

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 x 20=40)

Q.1. Define cyclic group? Explain discrete logarithm in cryptography with suitable example.

Q.2 What are the principle elements of a public-key cryptosystem? Explain in detail the three broad categories of application of public-key crpytosystems.

P.T.O.

Q.3 What do you understand by digital signature and digital certificate? Explain how digital signature are different from authentication protocol.

Q.4 Explain RSA and attacks on RSA public key Cryptosystem.

Q.5 What do you understand by key exchange in cryptography? Illustrate any key exchange algorithm with example.

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 x 10=40)

Q.1 Explain time and space complexity with example.

Q.2 What is SHA hash function?

Q.3 Define Zero Knowledge proof for Elliptic Curve Discrete Logarithm Problem(ECDLP).

Q.4 Explain elementary number theory in cryptography.

Q.5 What are the various security features of Elliptic curve cryptography?

Q.6 State and prove Chinese Remainder theorem.

Q.7 What do you understand by Sub groups? Explain the properties of Sub Groups.

Q.8 Explain Quadratic-sieve Factoring algorithm.

****