Roll No. | | | | | | | | | | | | **Total No. of Pages : 02**

Total No. of Questions : 07

B.Sc. (Cyber Security) (Sem.–3)

MATHEMATICAL FOUNDATIONS FOR CRYPTOGRAPHY

Subject Code : UGCA1987

M.Code : 92751

Date of Examination : 14-12-22

Time : 3 Hrs. **Max. Marks : 60**

INSTRUCTIONS TO CANDIDATES :

1. **SECTION-A is COMPULSORY consisting of TEN questions carrying TWO marks each.**
2. **SECTION-B contains SIX questions carrying TEN marks each and students have to attempt any FOUR questions.**

SECTION-A

1. Write briefly :

a) What are Abelian groups?

b) What is modular polynomial arithmetic?

c) Discuss bitwise OR.

d) What is Shift left operation?

e) Define Cryptography.

f) Write about block and stream ciphers.

g) What is malware? How it differs from virus?

h) Differentiate between Confidentiality End Privacy.

i) Write about Chinese Remainder Theorem.

j) Write about importance of keys on Encryption.

SECTION-B

2. What are logarithms for modular arithmetic?

3. Write about linear congruence. What are properties of congruence?

4. Write about pseudorandom number generators? Discuss their principles.

5. Discuss substitution and transposition ciphers.

6. Write about following :

   a. Intrusion

   b. Vulnerability

   c. Privacy

7. Why are shift operators used in cryptography? Discuss any two.

NOTE : Disclosure of Identity by writing Mobile No. or Marking of passing request on any paper of Answer Sheet will lead to UMC against the Student.