20/2914-20/2919

20/2914

B.A./B.Sc. (Third Year) Examination, 2020

MATHEMATICS

Fourth Paper (Optional)

(A) Number Theory and Cryptography

Time : Three Hours ***Maximum Marks : 75***

Note: Answer **five** questions in **all**. Question **No.1** is **compulsory**. Answer **one** question from each unit. Marks allotted to each question are indicated in the right-hand margin.

Note: The answers to short answer type questions should not exceed 200 words and the answers to long answer type questions should not exceed 500 words.

P.T.O.

20/2914 - 20/2919

1. Answer the following short answer questions $3.5 \times 10 = 35$

   (a) Evaluate (3 4 5 6 7, 8 9 0).

   (b) Define Euler functions. Evaluate $\phi(121)$.

   (c) Using Fermat's theorem, evaluate $(365)^{13}$ congruence modulo 7.

   (d) Define Smooth functions.

   (e) What is security encryption?

   (f) Define cryptography.

   (g) Write Diffe-Hellman Key-exchange protocol.

   (h) Evaluate the value of floor and ceiling functions at point x=2.5.

   (i) Write down the general equation of elliptic curve.

   (j) List all the divisors of 945.

Unit - I

2. State and prove Chinese-remainder theorem. Also find the g.c.d. of 130, 156 and 24. 10

OR

3. Prove that every natural number greater than 1 can be expressed as product of prime numbers. Also prove that there are infinitely many primes. 10

Unit - II

4. Describe Pollard's method for factorization. Illustrate it by means of an example. 10

OR

5. What is cryptanalysis? Explain any classical technique by an example. 10

Unit - III

6. Write short notes on the following : 5×2=10

   (a) Data Encryption Standard (DES)

   (b) Public Key Cryptography

OR

7. Describe RSA algorithm of public key encryption. Illustrate it by means of an example. 10

Unit - IV

8. Explain digital signature algorithm. Also illustrate Key distribution problem. 10

OR

9. Write short notes on the following : 5×2=10

   (a) Elliptic curve cryptography

   (b) Knapsack problem