K

(Printed Pages 4)

22/134

B.A./B.Sc. (Part-III) Examination, 2022

MATHEMATICS

Fourth Paper

(A,B,C,D,E,F)

BMG - 304

Fourth (A) Paper

(Number Theory and Cryptography)

Time : Three Hours] *[Maximum Marks : 60*

Note : Attempt **all** sections as per instructions.

Section - A

(Very Short Answer Type Questions)

Note : Answer **all** parts of this question. Give answer of each part in about 50 words. Each part carries 1½ marks. Symbols used have their usual meaning.

1½×10=15

P.T.O.

1. (i) Prove that 17 divides $3.5^{2n+1} + 2^{3n+1}$

   (ii) If $(a,b) = (c,b) = 1$, show that $(ac,b)=1$

   (iii) Define perfect number.

   (iv) Define Euler's function.

   (v) Define cryptography and state R.S.A. cryptosystem.

   (vi) Define twin primes by example.

   (vii) Define Signature Schemes.

   (viii) Define rational points on elliptic curves.

   (ix) Explain known attacks.

   (x) Define absolute pseuto-primes with example.

Section - B

(Short Answer Type Questions)

Note : Attempt **all** questions. Give answer of each question in about 200 words. Each question carries 6 marks. 6×5=30

2. State and prove fundamental theorem of Arithmetic.

OR

Show that $5^{38} \equiv 4\,(\mathrm{mod}\,11)$

3. Prove that there are infinitely many primes.

OR

Solve the equation

$X^8 \equiv 17 \pmod{43}$ and

$8x \equiv 7 \pmod{43}$

4. Prove that a cryptosystem has perfect secrecy if p (c=c/p=m) = p (C=c) for all m and c.

OR

Show that the relation of congruency is an equivalence relation.

5. Encrypt the message RETURNHOME using caesar cipher.

OR

Discuss Hash function and Block Ciphers.

6. Discuss Knapsack problem.

OR

Prove that the trace of Frobenius satisfies $|t| \leq 2\sqrt{g}$.

Section - C

(Long Answer Type Questions)

Note : Attempt any **two** questions. Give answer of each question in about 500 words. Each question carries 7½ marks.

7½×2=15

7. State and prove chinese remainder theorem.

8. State and prove Fermate's theorem.

9. Using linear cipher

$C \equiv 5p+11 \pmod{26}$,

encrypt the message Number theory is Easy.

10. If p and q are distinct primes prove that

$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$

11. Prove that the product of two quadratic residues is a quadratic residue.