19002010

19002010

Reg. No.....

Name.....

M.Sc. DEGREE (C.S.S.) EXAMINATION, NOVEMBER 2019

Third Semester

Faculty of Science

Branch I (A) : Mathematics

MT 03 C 14—NUMBER THEORY AND CRYPTOGRAPHY

(2012–2018 Admissions)

Time : Three Hours Maximum Weight : 30

Part A

Answer any **five** *questions.*
Each has weight 1.

1. Find the last base-7 digit in $2^{1000000}$.
2. Factor $3^{1^2} - 1 = 531440$.
3. Describe all solutions of $9x \equiv 12 \pmod{21}$.
4. State the properties of Legendre symbol.
5. Define discrete logarithm with an example.
6. Compare deterministic and probabilistic encryptions.
7. Find the smallest pseudoprime to the base 5.
8. Use Fermat factorisation to factor 8633.

$(5 \times 1 = 5)$

Part B

Answer any **five** *questions.*
Each has weight 2.

9. Estimate the time required to convert a K-bit integer n to its representation in the base b, where b might be very large.
10. State and prove Fermat's Little Theorem.
11. Show that the Euler phi-function is "multiplicative" meaning that $\varphi(m\,n) = \varphi(m)\,\varphi(n)$ whenever $g\,c\;\;d\,(m, n) = 1$
12. Prove : There exists a sequence of prime p such that the probability that a random $g \in F_p^*$ is a generator approaches zero.

Turn over

13. Describe how RSA works.

14. Explain how Digital Signature standard works.

15. Show that p^2 (with p prime) is a pseudoprime to the base b if and only if $b^{p-1} \equiv 1 \bmod p^2$.

16. Prove that 561 is the smallest Carmichael number.

(5 × 2 = 10)

Part C

Answer any **three** *questions.*
Each has weight 5.

17. Find a 3-digit (decimal) number which leaves a remainder of 4 when divided by 7, 9, or 11. Also express 7 as a linear combination of 1547 and 560.

18. (a) State the properties of Congruences.

    (b) Establish Euclidean algorithm.

19. Explain with examples :

    (a) finite field.

    (b) Characteristic of a field.

    (c) Irreducible polynomial.

    (d) Extension field.

    (e) Polynomial ring.

20. Discuss, in detail, the idea of public key cryptography.

21. Describe the EI Gamal cryptosystem in detail.

22. State the necessary lemmas and prove :

    If n is an odd composite integer, then n is a strong pseudoprime to the base b for at most 25% of all $0 < b < n$.

(3 × 5 = 15)