F 6497 (Pages : 2) Reg. No..............................

Name..................................

M.Sc. DEGREE (CSS) EXAMINATION, JANUARY 2015

Third Semester

Faculty of Science

Branch I (A)—Mathematics

MT 03 C14—NUMBER THEORY AND CRYPTOGRAPHY

(2012 admission onwards)

Time : Three Hours Maximum Weight : 30

Part A

Answer any **five** *questions.*
Each question carries weight 1.

1. Divide $(40122)_7$ by $(126)_7$.
2. Describe all the solutions of $3x = 4 \bmod 12$.
3. Let $m = 2^{24} + 1 = 16777217$. Find a Fermat prime which divides m.
4. For each degree $d \leq 6$, find the number of irreducible polynomials over F_2 of degree d.
5. What is classical cryptosystem ?
6. In F_9^* with α a root of $X^2 - X - 1$, find the discrete logarithm of -1 to the base α.
7. Find all Carmichael numbers of the form $3pq$ (with p and q prime).
8. Use Fermat factorization to factor 4601.

$(5 \times 1 = 5)$

Part B

Answer any **five** *questions.*
Each question carries weight 2.

9. Find an upper bound for the number of bit operations required to compute n !.
10. Prove that $n^5 - n$ is always divisible by 30.
11. For any integer b and any positive integer n, prove that b^{n-1} is divisible by $b - 1$ with quotient $b^{n-1} + b^{n-2} + \ldots + b^2 + b + 1$.
12. Show that the order of any at F_q^* divides $q - 1$, where F_q^* denotes the set of non-zero elements in the finite field F_q.

Turn over

13. Describe the ElGamel cryptosystem.

14. Find the discrete log of 153 to the base 2 in F_{181}^{*}.

15. Factor 4087 using $f(x) = x^2 + x + 1$ and $x_0 = 2$.

16. Use quadratic sieve method to factor 1046603 with P = 50 and A = 500.

(5 × 2 = 10)

Part C

Answer any **three** *questions.*
Each question carries weight 5.

17. State and prove Chinese remainder theorem.

18. Show that the Euclidean algorithm always gives the greatest common divisor in a finite number of steps. Also prove that for $a > b$, Time (finding g.c.d. (a, b) by the Euclidean algorithm) = O $(\log^3(a))$.

19. State and prove the law of quadratic reciprocity.

20. Describe the algorithm for finding discrete logs in finite fields.

21. Explain Diffe–Hallman key exchange system.

22. Prove that if n is a strong pseudoprime to the base b, then it is an Euler pseudoprime to the base b.

(3 × 5 = 15)