F 5067 (Pages : 2) Reg. No.....

Name.....

M.Sc. DEGREE (C.S.S.) EXAMINATION, JANUARY 2016

Third Semester

Faculty of Science

Branch : I (A)—Mathematics

MT03C14—NUMBER THEORY AND CRYPTOGRAPHY

(2012—Admission onwards)

Time : Three Hours Maximum Weight : 30

Part A

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

1. Divide $(11001001)_2$ by $(100111)_2$ and divide $(HAPPY)_{26}$ by $(SAD)_{26}$.
2. Find the *gcd* (1547, 560).
3. How many divisors does 945 have ? List them all.
4. Evaluate the Legendre symbol $\left(\frac{97}{101}\right)$.
5. Define Hash function.
6. What is the probabilistic encryption ?
7. Find all bases b for which 15 is a pseudoprime.
8. Use Fermat factorisation to factor 4601.

(5 × 1 = 5)

Part B

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

9. Estimate in terms of a simple function of n and N the number of bit operations required to compute N^n.
10. Convert 10^6 to the bases 2, 7 and 26.
11. Prove that n^5-n is always divisible by 30.
12. Determine whether 7411 is a residue module to prime 9283.
13. Explain discrete algorithm problem.
14. Using the Silver-Pohlig-Hellman algorithm, find the discrete log of 153 to the base 2 in F^*_{181}.

Turn over

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. Let $n = 4633$. Use 68, 152 and 153 with a suitable factor-base B to factor 4633. What are the corresponding vectors ?

$(5 \times 2 = 10)$

Part C

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

17. Estimate the time required to convert a K-bit integer to its representation in the base 10.
18. Prove that $\Sigma_{d/n}\phi(d) = n$.
19. Show that for every prime power q there is one and (up to isomorphism) only one finite field with 2 elements.
20. Explain in detail the RSA cryptosystem.
21. Explain the Diffie-Hellman key exchange system.
22. Explain the quadratic sieve method in detail.

$(3 \times 5 = 15)$