F 4676 (Pages : 2) Reg. No. 100983d

Name. NASNA

M.Sc. DEGREE (C.S.S.) EXAMINATION, JANUARY 2017

Third Semester

Faculty of Science

Branch : I (A)—Mathematics

MTO 3C 14—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 $(4\ 0\ 1\ 2\ 7\ 7)_7$ by $(1\ 2\ 6)_7$.
2. Express 7 as a linear combination of 1547 and 560.
3. Describe all the solutions of the following congruence $27x \equiv 25 \bmod 256$.
4. Find the quadratic residues mod 11. Also write the non-residues mod 11.
5. What is a public key cryptosystem ?
6. What do you mean by probabilistic encryption ?
7. What is a Carmichael number ?
8. Use Fermat factorization to factor 92296873.

$(5 \times 1 = 5)$

Part B

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

9. Estimate the time required to convert a k-bit integer to its representation in the base 10.
10. Prove that for any prime p, $(p - 1)! \equiv -1 \bmod p$.
11. Factor $3^{12} - 1 = 5\,3\,1\,4\,4\,0$.
12. Prove that $(a + b)^p = a^p + b^p$ in any field of characteristic p.
13. Describe the Massey-Omura cryptosystem for message transmission.
14. Find the discrete log of 28 to the base 2 in $\mathbf{F}_{37}^{*}$ using the Silver-Pohlig-Hellman algorithm.

Turn over

15. Use rho method to factor 7031, where $f(x) = x^2 - 1$, $x_0 = 5$.

16. Prove that $\log n! - (n\log n - n) = 0(\log n)$.

(5 × 2 = 10)

Part C

Answer any **three** *questions.*

Each question has weight 5.

17. (a) State and prove Fermat's little theorem.

    (b) State and prove Chinese remainder theorem.

18. (a) Prove that for any integer b and any positive integer n, $b^n - 1$ is divisible by $b - 1$ with quotient $b^{n-1} + b^{n-2} + \ldots + b^2 + b + 1$.

    (b) Let $m = 2^{24} + 1 = 16777217$:

    (i) Find a Fermat prime which divides m.

    (ii) Prove that any other prime is $\equiv 1 \bmod 48$.

19. State and prove Quadratic reciprocity law.

20. Describe the algorithm for finding discrete logs infinite fields.

21. Explain the encryption and decryption procedure in a RSA cryptosystem.

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)