21000061

21000061

Reg. No..............................

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

M.Sc. DEGREE (C.S.S.) EXAMINATION, FEBRUARY 2021

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 $\gcd(360, 294)$ using Euclidean algorithm.
2. Compute $2^{1000000}$ mod 77.
3. Factor $2^{33} - 1$ and $2^{21} - 1$.
4. Find $\left(\frac{91}{167}\right)$ using quadratic reciprocity.
5. State and explain : Diffie – Hellman assumption.
6. Explain : enciphering key and deciphering key.
7. Find all bases for which 21 is a pseudoprime.
8. Factor 4087 using $f(x) = x^2 + x + 1$ and $u_0 = 2$.

(5 × 1 = 5)

Part B

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

9. Estimate the time required to convert a k-bit integer to its representation in the base 10.
10. State and prove Chinese remainder theorem.
11. Prove : If $\gcd(a,m) = 1$, then $a^{\varphi(m)} \equiv 1 (\bmod m)$.
12. Prove : The order of any $a \in \mathrm{F}_q^*$ divides $q = 1$.

Turn over

13. Find the discrete log of 28 to the base 2 in F_{37}^{*} using the Silver–Pohlig–Hellman algorithm.

14. Describe how RSA works.

15. Prove : A Carmichael number must be the product of at least three distinct prime.

16. Prove that, if n is a strong pseudoprime to the base b, then it is a strong pseudoprime to the base b^k for any integer k.

(5 × 2 = 10)

Part C

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

17. For any prime p, show that $(p-1)! \equiv -1 \bmod p$. Prove that $(n-1)!$ is not congruent to –1 mod n if n is not a prime. Also prove that $\sum_{d/n} \varphi(d) = n$.

18. (a) Explain modular exponentiation by the repeated squaring method.

    (b) Show that $n^5 - n$ is always divisible by 30.

19. Define (i) field ; (ii) vector space ; (iii) polynomial ring ; (iv) isomorphic fields ; and (v) splitting field. Give an example for each.

20. Explain (i) key exchange ; (ii) Hash function ; (iii) Authentication ; (iv) discrete logarithm problem ; and (v) Legendre symbol.

21. Describe the Massey–Omura cryptosystem for message transmission.

22. Use the quadratic sieve method to factor 998771 with p = 50 and A = 500.

(3 × 5 = 15)