MAY 2024 **P/ID 37515/PMA3R**

Time : Three hours Maximum : 80 marks

PART A — (10 × 2 = 20 marks)

Answer any TEN questions.

1. Multiply $(160)_{10}$ and $(199)_{10}$ in the base 7.

2. Find *g.c.d.* (1547, 560).

3. Define deciphering.

4. Define digraphs.

5. Determine all the solutions of $103x \equiv 612 \bmod 676$.

6. Define Galois extension.

7. Evaluate the Legendre symbol $\left(\frac{11}{37}\right)$.

8. Define a generator g of a finite field F_q .

9. Define the discrete logarithm.

10. Define Carmichael number

11. Define trapdoor function.

12. Define deciphering key.

PART B — (5 × 6 = 30 marks)

Answer any FIVE questions.

13. Estimate the time required to convert a k-bit integer to its representation in the base 10.

14. Find an upper bound for the number of bit operations it takes to compute the binomial coefficient $\binom{n}{m}$.

15. For any integer b and any positive integer n, prove that $b^n - 1$ is divisible by $b-1$ with quotient $b^{n-1} + b^{n-2} \cdots + b + 1$.

16. Prove that the order of any $a \in F_q^*$ divides $q-1$.

17. Prove that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$.

18. Solve the following system of congruences:

$2x + 3y \equiv 1 \bmod 26$

$7x + 8y \equiv 2 \bmod 26$

19. Explain authentication in the public key cryptography.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

20. State and prove Fermat's Little Theorem.

21. An adversary is using a cryptosystem with a 27-letter alphabet, in which the letters A-Z have numerical equivalents 0–25, and blank = 26. Each digraph then corresponds to an integer between 0 and $728 = 27^2 - 1$ according to the rule that, if the two letters in the digraph have numerical equivalents x and y. then the digraph has numerical equivalent $27x + y$. Suppose that a study of a large sample of ciphertext reveals that the most frequently occurring digraphs are (in order) "ZA"; "IA"; and "IW". Suppose that the most common digraphs in the English language (for text written in our 27-letter alphabet) are "E" (i.e. , "E blank') "S", "T". The cryptosystem uses an affine enciphering transformation modulo 729. Find the deciphering key, and read the message "NDXBHO". Also find the enciphering key.

22. State and prove the Law of Quadratic Reciprocity.

23. Explain the ElGamal cryptosystem.

24. Find the type of $y^2 = x^3 - x$, over $\mathbb{F}_{71}$.
