DECEMBER 2023 **P/ID 37515/PMA3R**

Time : Three hours Maximum : 80 marks

PART A — (10 × 2 = 20 marks)

Answer any TEN questions.

1. Divide $(HAPPY)_{26}$ by $(SAD)_{26}$.

2. State Fermat's Little Theorem.

3. Define Polynomial time algorithm.

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

5. Define the Legendre symbol.

6. Define a *generator* of a finite field.

7. State the *Law of Quadratic Reciprocity*.

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

9. Define *enciphering*.

10. Define *Carmichael number*.

11. Define *deciphering key*.

12. Define *trapdoor function*.

PART B — ($5 \times 6 = 30$ marks)

Answer any FIVE questions.

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

14. If *g.c.d.* (*a, m*) = 1, then prove that $a^{\varphi(n)} \equiv 1 \bmod m$.

15. Compute $2^{1000000} \bmod 77$.

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

17. If F_q is a field of $q = p^f$ elements, then prove that every element satisfies $X^q - X = 0$ and F_q is precisely the roots of that equation. Prove also time converse.

18. Working in the 26-letter alphabet. use the matrix $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_2(Z/26Z)$ to encipher the message unit "NO"

19. Explain *authentication* in the public key cryptography.

PART C — ($3 \times 10 = 30$ marks)

Answer any THREE questions.

20. State and prove the Chinese Remainder Theorem.

21. Find a formula for the number of different affine enciphering transformations there are with an N-letter alphabet.

22. Prove that
$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if} \quad p \equiv \pm 1 \mod 8 \\ -1 & \text{if} \quad p \equiv \pm 3 \mod 8 \end{cases}.$$

23. Explain RSA cryptosystem.

24. Factor 141467.

———————