MAY 2025 **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. Multiply $(160)_{10}$ and $(199)_{10}$ in the base 7.

3. Define Polynomial time algorithm.

4. Describe all the solutions of $103x \equiv 612 \mod 676$.

5. Define Galois *extension*.

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

7. State the Law of Quadratic Reciprocity.

8. Define the Legendre symbol.

9. Define deciphering transformation.

10. Define enciphering.

11. Define Hash function.

12. Define trapdoor function.

PART B — (5 × 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. Estimate the time required to convert a k-bit integer n to its representation in the base b, where b might be very large.

15. Let $f(X) = X^4 + X^3 + X^2 + 1$, $g = X^3 + 1 \in F_2$ [X]. find $g.c.d(f, g)$ using Euclidean algorithm for polynomials and express the g.c.d. in the form $u(X)f(X) + v(X)g(X)$.

16. Prove that for any $q = p^f$ the polynomial $X^q - X$ factors in F_p [X] into the product of all monic irreducible polynomials of degrees d dividing f.

17. Prove that there exists a sequence of primes p such that the probability that a random $g \in F_p^*$ is a generator approaches zero.

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 × 10 = 30 marks)

Answer any THREE questions

20. Sate and prove the Chinese Remainder Theorem.

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

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

23. Explain RSA cryptosystem.

24. Factor 141467.

———————