DECEMBER 2024 **P/ID 37515/PMA3R**

Time : Three hours Maximum : 80 marks

PART A — ($10 \times 2 = 20$ marks)

Answer any TEN questions.

1. Find $g.c.d.(1547, 560)$.
2. Divide $(HAPPY)_{26}$ by $(SAD)_{26}$.
3. Multiply $(160)_{10}$ and $(199)_{10}$ in the base 7.
4. Define Polynomial time algorithm.
5. Describe all the solutions of $3x \equiv 4 \bmod 7$.
6. Define the Legendre symbol.
7. Define a *generator g* of a finite field F_q.
8. Evaluate the Legendre symbol $\left(\frac{31}{167}\right)$.
9. Define an *enciphering transformation*.
10. Define *Carmichael number*.
11. Define *deciphering key*.
12. Define *Hash function*.

PART B — ($5 \times 6 = 30$ marks)

Answer any FIVE questions.

13. Find an upper bound for the number of bit operations required to compute n!.

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 every finite field has a generator. If g is a generator of F_q^*, then prove that g^j is also a generator if and only if $g.c.d.(j, q-1) = 1$.

17. Find the inverse of the matrix $\begin{pmatrix} 15 & 17 \\ 4 & 9 \end{pmatrix}$ mod 26. Write the entries in the inverse matrix as non-negative integers less than 26.

18. Working in the 26-letter alphabet, find the inverse of the matrix $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_2(Z/26Z)$.

19. Explain *probabilistic encryption* in the public key cryptography.

PART C — ($3 \times 10 = 30$ marks)

Answer any THREE questions.

20. State and prove Fermat's Little Theorem.

21. Suppose that an adversary is using an enciphering matrix A in the 26-letter alphabet. We intercept the ciphertext "WKNCCHSSJH", and we know that the first word is "GIVE." Find the deciphering matrix A^{-1} and read the message.

22. For any two positive odd integers m and n, prove that $\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right)$.

23. Explain the Diffie-Hellman key exchange system.

24. Find the Factor 200819.

———————