MAY 2022 **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. Find g.c.d. (1547, 560).

4. Define Polynomial time algorithm.

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

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

7. State the *Law of Quadratic Reciprocity*.

8. Define the *Legendre symbol.*

9. Define an *enciphering transformation.*

10. Define *Carmichael number.*

11. Define *trapdoor function.*

12. Define *deciphering key.*

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 $a^{\varphi(n)} \equiv 1 \mod m$.

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

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 nonnegative integers less than 26.

18. Solve the following system of congruences :

$$2x + 3y \equiv 1 \mod 26$$
$$7x + 8y \equiv 2 \mod 26$$

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

23. Explain the Diffie-hellman key exchange system.

24. Find the type of $y^2 = x^3 - x$.