MAY 2023 **P/ID 37515/PMA3R**

Time : Three hours Maximum : 80 marks

SECTION A — ($10 \times 2 = 20$ marks)

Answer any TEN questions.

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

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

3. Convert 10^6 to base 2.

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

5. Describe all the solutions of $3x \equiv 4 \mod 7$.

6. Define Galois extension.

7. Define a generator g of a finite field $\mathbf{F}_q$.

8. Define the Legendre symbol.

9. Define deciphering transformation.

10. Define an enciphering transformation.

11. Define trapdoor function.

12. Define Hash function.

SECTION 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. Suppose that b is prime to m, and a and c are positive integers. If $b^a \equiv 1 \mod m$ and $b^c \equiv 1 \mod m$ and if $d = g.c.d.(a, c)$, then prove that $b^d \equiv 1$ mode m.

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

16. Prove that for any $q = p^f$ the polynomial $X^q - X$ factors in $\mathbf{F}_p[X]$ 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 $g \in \mathbf{F}_p^*$ is a generator approaches zero.

18. Working in the 26-letter alphabet, find the inverse of the matrix.

$$A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_2(\mathbf{Z}/26\mathbf{Z}).$$

19. Explain probabilistic encryption in the pubic key cryptography.

SECTION 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. Factor 200819.

———————