DECEMBER 2022 **P/ID 37515/PMA3R**

Time : Three hours Maximum : 80 marks

SECTION A — (10 × 2 = 20 marks)

Answer any TEN questions.

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

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

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

4. Define Polynomial time algorithm.

5. Define Galois extension.

6. State the law of quadratic reciprocity.

7. Evaluate the Legendre symbol $\left(\frac{11}{37}\right)$.

8. Define a generator g of finite field F_q.

9. Define and enciphering transformation.

10. Define enciphering.

11. Define Hash function.

12. Define deciphering key.

SECTION B — (5 × 6 = 30 marks)

Answer any FIVE questions.

13. Estimate the time required to convert a $k-$bit integer to its representation in the base 10.

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

$f(X) = X^4 + X^3 + X^2 + 1$, $g(X) = X^2 + 1 \in F_2[X]$. 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 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 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.

SECTION C — (3 × 10 = 30 marks)

Answer any THREE questions.

20. Prove that $\sum_{d|n} \varphi(d) = n$.

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'; "IA'; 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. State and prove the Law of Quadratic Reciprocity.

23. Explain the ElGamal cryptosystem.

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

———————