D 111191 **(Pages : 2)** **Name.....**

Reg. No.....

THIRD SEMESTER M.Sc. DEGREE (REGULAR/SUPPLEMENTARY) EXAMINATION, NOVEMBER 2024

(CBCSS)

Mathematics

MTH 3E 02—CRYPTOGRAPHY

(2019 Admission onwards)

Time : Three Hours Maximum : 30 Weightage

Section A

Answer **all** *questions.*
Each question carries 1 *weightage.*

1. Describe Substitution Cipher.
2. Find the number of keys in the Affine Cipher over $\mathbb{Z}_{97}$.
3. Evaluate – 7503 mod 81.
4. Define the unicity distance of a cryptosystem.
5. Define the entropy and the redundancy of a natural language.
6. Find the binary equivalent of hexadecimal 987.
7. What are the main criterian for the suitability of AES candidates ?
8. What is round key mixing ?

(8 × 1 = 8 weightage)

Section B

Answer any **two** *questions from each of the following three units.*
Each question carries 2 weightage.

UNIT I

9. Determine the inverse of the matrix over $\begin{bmatrix} 2 & 5 \\ 9 & 5 \end{bmatrix}$ over $\mathbb{Z}_{26}$.
10. Describe Hill Cipher with an example.

Turn over

11. Encrypt the plaintext "“MUSIC” using the encryption funtion $e_K(x) = 9x + 4$.

UNIT II

12. Describe Product Cryptosystems with an example.

13. Show that $H(X, Y) \leq H(X) + H(Y)$, and equality hold if and only if X and Y are independent random variables.

14. Consider three fair coins : two will result in heads with a probability of 0.50, while the third will result in heads with a probability of 0.75. What is the chance that the biased coin is the one that is chosen at random and tossed three times, generating three heads ?

UNIT III

15. Explain AES (Advanced Encryption Standard).

16. Suppose that $(\mathcal{X}, \mathcal{Y}, \mathcal{K}, \mathcal{H})$ is a strongly universal (N, M)-hash family. Show that $(\mathcal{X}, \mathcal{Y}, \mathcal{K}, \mathcal{H})$ is an authentication code with $Pd_0 = Pd_1 = \frac{1}{M}$.

17. Explain Huffman Encodings.

(6 × 2 = 12 weightage)

Section C

Answer any **two** *questions.*
Each question carries 5 *weightage.*

18. Find the encrypted plain text “WONDERFUL” using the encryption function $e_K(x) = 7x + 3$.

19. Suppose $(\mathcal{X}, \mathcal{Y}, \mathcal{K}, \mathcal{H})$ is an (N, M)-hash family. Show that $Pd_1 = \frac{1}{M}$ if and only if the hash family is strongly universal.

20. State and prove piling-up lemma.

21. Discuss Substitution-Permutation Network (SPN).

(2 × 5 = 10 weightage)