D 132043 **(Pages : 3)** **Name..................................**

Reg. No..............................

THIRD SEMESTER M.Sc. DEGREE [REGULAR/SUPPLEMENTARY] EXAMINATION, NOVEMBER 2025

(CBCSS)

Mathematics

MTH3E02—CRYPTOGRAPHY

(2019 Admission onwards)

Time : Three Hours Maximum : 30 Weightage

Section A

Answer **all** *questions.*

Each question carries 1 *weightage.*

1. Define Shift Cipher.
2. Find the number of keys in the Affine Cipher over $\mathbb{Z}_{60}$.
3. Evaluate – 7503 mod 81.
4. Define perfect secrecy of a cryptosystem ?
5. Define the entropy and the redundancy of a natural language.
6. What is ECB (Electronic Codebook) mode for DES ?
7. Write the binary equivalent of hexadecimal 153.
8. What is a collision resistant hash function ?

(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. Suppose the key for a Shift Cipher is K = 13 and the planetext is MATHEMATICS. What is the cypher text ?

Turn over

10. Define a synchronous stream cipher.

11. Find the inverse of $A = \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix} \in M_2 \left(\mathbb{Z} / 26\mathbb{Z}\right)$.

Unit II

12. Suppose that in the Shift Cipher, 26 keys are used with equal probability $\frac{1}{26}$. Show that the Shift Cipher has perfect secrecy for any plaintext probability distribution.

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

14. Suppose X is a random variable having a probability distribution that takes on the values $p_1, p_2, ..., p_n$. where $p_i > 0$. Show that $H(X) \leq \log_2 n$, and equality holds if and only if $p_i = \frac{1}{n}$.

Unit III

15. Explain Differential Cryptanalysis.

16. Let p be prime. For $a, b \in \mathbb{Z}_p$ define $f_{(a,b)} : \mathbb{Z}_p \to \mathbb{Z}_p$ by the rule $f_{(a,b)} = ax + b \bmod p$. Show that $\left(\mathbb{Z}_p, \mathbb{Z}_p, \mathbb{Z}_p \times \mathbb{Z}_p, \left\{f_{(a,b)} : a, b \in \mathbb{Z}_p\right\}\right)$ is a strongly universal (p, p)- hash family.

17. Explain the secure Hash Algorithm.

(6 × 2 = 12 weightage)

Section C

Answer any **two** *questions.*

Each question carries 5 *weightage.*

18. Encrypt the plaintext "BEAUTIFUL" using Hill cipher encryption with the key

$$\begin{bmatrix} 11 & 8 & 2 \\ 3 & 7 & 1 \\ 3 & 2 & 7 \end{bmatrix}.$$

19. Explain Huffman Encodings.

20. State and prove piling-up lemma.

21. Discuss Substitution-Permutation Network (SPN).

(2 × 5 = 10 weightage)