D 51313 **(Pages : 2)** **Name.....**

Reg. No.....

THIRD SEMESTER M.Sc. (CBCSS) [REGULAR/SUPPLEMENTARY] DEGREE EXAMINATION, NOVEMBER 2023

Mathematics

MTH 3E 02—CRYPTOGRAPHY

(2019 Admission onwards)

Time : Three Hours Maximum : 30 Weightage

Section A

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

1. Define a cryptosystem.
2. Find the number of keys in the Affine Cipher over $\mathbb{Z}_{63}$.
3. Evaluate 7503 mod 81.
4. Define the entropy and the redundancy of a natural language.
5. State Bayes' theorem.
6. What are the different modes of operation of DES ?
7. Find the binary equivalent of hexadecimal 283.
8. Describe a hash family.

(8 × 1 = 8 weightage)

Section B

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

Unit I

9. State Kirchoff's principle.
10. Suppose the plaintext "friday" is encripted using Hill Cipher with $m = 2$. What will be the Ciphertex ?
11. Describe Permutation Cipher with an example.

Unit II

12. State Jensen's inequality.
13. 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 ?

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

Unit III

15. Explain DES (Data Encryption Standard).
16. Write the Merkle-Damgard Algorithm for the construction of a hash function.
17. Describe Message Authentication Codes (MAC).

(6 × 2 = 12 weightage)

Section C

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

18. Encrypt the plaintext "TEACHERS" using Hill cipher encryption with the key $\begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$.
19. Explain the properties of Entropy.
20. State and prove pilling-up lemma.
21. Explain linear attack on a substitution Permutation Network (SPN).

(2 × 5 = 10 weightage)