D 150348 **(Pages : 3)** **Name.....**

Reg. No.....

THIRD SEMESTER M.Sc. (CBCSS) REGULAR/SUPPLEMENTARY DEGREE EXAMINATION, NOVEMBER 2026

Mathematics

MTH 3E 02—CRYPTOGRAPHY

(2019 Admission onwards)

Time : Three Hours Maximum Weightage : 30

Part A (Short Answer Type Questions)

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

1. Define Cryptosystem.
2. State Jensen's inequality.
3. Describe discrete random variable.
4. State Bayes' theorem.
5. Define unicity distance of a cryptosystem.
6. Describe briefly computational security.
7. Describe conditional entropy.
8. State Piling-up lemma.

(8 × 1 = 8 weightage)

Part B (Paragraph Type Questions)

Answer any **two** *questions from each module.*
Each question carries a weightage 2.

Module I

9. Use exhaustive key search to decrypt the following ciphertext, which was encrypted using a Shift Cipher :

   BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD.

10. Determine the number of involutory keys in the Permutation Cipher for m = 2, 3, 4, 5 and 6.
11. Describe briefly Cryptanalysis of the LFSR Stream Cipher.

Turn over

Module II

12. Suppose X is a random variable having a probability distributin that takes on the values $p_1, p_2, \ldots, p_n$, where $p_i > 0, 1 \le i \le n$. Then prove that $H(X) \le \log_2 n$, with equality if and only if $p_i = 1/n, 1 \le i \le n$.

13. Let $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ be a cryptosystem. Then prove that $H(K|C) = H(K) + H(P) - H(C)$.

14. Prove that $H(X, Y) = H(Y) + H(X|Y)$. Then show as a corollary that $H(X|Y) \le H(X)$, with equality if and only if X and Y are independent.

Module III

15. Let $\varepsilon_{i_1, i_2, \ldots, i_k}$ denote the bias of the random variable $X_{i_1} \oplus \ldots \oplus X_{i_k}$. Then prove that $\varepsilon_{i_1, i_2, \ldots, i_k} = 2^{k-1} \prod_{j=1}^{k} \varepsilon_{i_j}$.

16. For any $X_0 \subseteq \mathcal{X}$ with $|X_0| = Q$, prove that the success probability of "FIND-COLLISION(h, Q)" Algorithm is :

$$\varepsilon = 1 - \left(\frac{M-1}{M}\right)\left(\frac{M-2}{M}\right)\ldots\left(\frac{M-Q+1}{M}\right).$$

17. Suppose $h : \mathcal{X} \to \mathcal{Y}$ is an (N, M)-hash function. For any $y \in \mathcal{Y}$, let $h^{-1}(y) = \{x : h(x) = y\}$ and denote $s_y = |h^{-1}(y)|$. Define $\mathcal{S} = |\{\{x_1, x_2\} : h(x_1) = h(x_2)\}|$. Note that $\mathcal{S}$ counts the number of unordered pairs in $\mathcal{X}$ that collide under h. Prove that $\sum_{y \in \mathcal{Y}} s_y = N$, so the mean of the $s_y's$ is $\bar{s} = \frac{N}{M}$.

(6 × 2 = 12 weightage)

Part C (Essay Type Questions)

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

18. Given below is an example of ciphertext, obtained from an *Affine Cipher*. Determine the plaintext. Give a clearly written description of the steps you followed to decrypt each ciphertext.

Affine Cipher :

KQEREJEBCPPCJCRKIEACUZBKRYPKRBCIBQCARBJCVFCUP
KRIOFKPACUZQEPBKRXPEIIEABDKBPCFCDCCAFIEABDKP
BCPFEQPKAZBKRHAIBKAPCCIBURCCDKDCCJCIDFUIXPAFF
ERBICZDFKABICBBENEFCUPJCVKABPCYDCCDPKBCOCPERK
IVKSCPICBRKIJPKABI

19. Suppose $(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$ is a cryptosystem where $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$. Then prove that the cryptosystem provides perfect secrecy if and only if every key is used with equal probability $1/|\mathcal{K}|$, and for every $x \in \mathcal{P}$ and every $y \in \mathcal{C}$, there is a unique key $\mathcal{K}$ such that $e_{\mathcal{K}}(x) = y$.

20. Prove : H(X, Y) ≤ H(X) + H(Y), with equality if and only if X and Y are independent random variables.

21. Suppose $\text{compress} : \{0,1\}^{m+t} \to \{0,1\}^m$ is a collision resistant compression function, where $t \leq 2$. Then prove that the function $h : \bigcup_{i=m+t+1}^{\infty} \{0,1\}^i \to \{0,1\}^m$, is a collision resistant hash function.

(2 × 5 = 10 weightage)