24P305 (Pages: 2) Name: .....

Reg.No: .....

THIRD SEMESTER M.Sc. DEGREE EXAMINATION, NOVEMBER 2025

(CBCSS - PG)

(Regular/Supplementary/Improvement)

CC19PMTH3E02 - CRYPTOGRAPHY

(Mathematics)

(2019 Admission onwards)

Time : 3 Hours Maximum : 30 Weightage

Part A

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

1. Encrypt "wewillmeetatmidnight" using Shift Cipher with $K = 11$.
2. Determine the number of keys in an Affine Cipher over Z_{100}.
3. What is the difference between mono-alphabetic and poly-alphabetic cryptosystems? Give examples for each.
4. What you mean by spurious keys? What is the entropy (per letter) of a random string of alphabets?
5. Define endomorphic cryptosystem with an example.
6. Explain about two types of permutations used in SPN.
7. Define a Hash family.
8. Explain the algorithm of Merkle-Damgard construction.

(8 × 1 = 8 Weightage)

Part B

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

UNIT - I

9. Prove that the linear congruence $ax \equiv b \ mod \quad m$ has unique solution in $modulo \quad m$ if and only if $gcd(a, m) = 1$.
10. Find the inverse of the matrix $\begin{bmatrix} 1 & 11 & 12 \\ 4 & 23 & 2 \\ 7 & 15 & 9 \end{bmatrix}$ in $modulo \quad 26$.
11. Suppose the plaintext "friday" is encrypted using a Hill Cipher with $m = 2$, to give the ciphertext "PQCFKU". Determine the key used for this encryption.

UNIT - II

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

13. Let $\mathbf{X}$ be a random variable which takes on values on the set $X = \{a, b\}$ with $Pr[a] = \frac{1}{4}$ and $Pr[b] = \frac{3}{4}$. Evaluate $H(\mathbf{X})$.

14. $H(\mathbf{X}|\mathbf{Y}) \leq H(\mathbf{X})$, with equality if and only if $\mathbf{X}$ and $\mathbf{Y}$ are independent.

UNIT - III

15. Suppose that X_1, X_2 and X_3 are independent discrete random variables defined on the set $\{0, 1\}$. Let ε_i denote the bias of X_i, for $i = 1, 2, 3$. Prove that $X_1 \oplus X_2$ and $X_2 \oplus X_3$ are independent if and only if $\varepsilon_1 = 0, \varepsilon_3 = 0$ or $\varepsilon_2 = \pm\frac{1}{2}$.

16. Explain about Advanced Encryption Standard.

17. Explain the algorithms in Random Oracle Model.

(6 × 2 = 12 Weightage)

Part C

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

18. (a) "The Permutation Cipher is a special case of Hill Cipher". Justify this statement.

    (b) Suppose $m = 6$ in Permutation Cipher and the key is the permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 6 & 4 & 2 \end{pmatrix}$. Using this decrypt the ciphertext "EESLSHSALSESLSHBLEHSYEETHRAEOS".

19. (a) How the Vigener Cipher can be defined as a Synchronous Stream Cipher?

    (b) Suppose $m = 3$ and the keyword is "AND" in Vigenere Cipher. Construct the corresponding stream cipher. Hence, encrypt the plaintext "garden" in both the two methods and verify that the resulting ciphertexts are same.

20. (a) Prove that $\mathbf{X}$ and $\mathbf{Y}$ are independent random variables if and only if $Pr[x|y] = Pr[x]$ for all $x \in X$ and $y \in Y$.

    (a) Consider a random throw of a pair of dice. Let $\mathbf{X}$ be the random variable defined on the set $X = \{2, 3, \ldots, 12\}$ obtained by considering the sum of two dice and $\mathbf{Y}$ is a random variable which

    takes on the D if the two dice are the same, and the value N, otherwise. Verify Bayes' Theorem for this pair of random variables.

21. (a) Explain Huffman's algorith.

    (b) Let $\mathbf{X}$ be a random variable which takes on values on the set $X = \{a, b, c, d, e\}$, with the probability distribution $Pr[a] = 0.05, Pr[b] = 0.10, Pr[c] = 0.12, Pr[d] = 0.13$ and $Pr[e] = 0.60$. Using Huffman's algorithm to find the optimal prefix-free encoding of $\mathbf{X}$. Compare the length of this encoding to $H(\mathbf{X})$.

(2 × 5 = 10 Weightage)

****