22P305 (Pages: 2) Name: ....

Reg.No: ....

THIRD SEMESTER M.Sc. DEGREE EXAMINATION, NOVEMBER 2023

(CBCSS - PG)

(Regular/Supplementary/Improvement)

CC19P MTH3 E02 - CRYPTOGRAPHY

(Mathematics)

(2019 Admission onwards)

Time : 3 Hours Maximum : 30 Weightage

Part A

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

1. Decrypt "HPHTWWXPPELEXTOYTRSE" using Shift Cipher with key $K = 11$.

2. List all the invertible elements in Z_{35}.

3. Define Permutation Cipher.

4. Define the cryptosystem One-Time Pad.

5. Let $\mathbf{X}$ be a random variable which takes on values on the set X. If $|X| = n$ and $Pr\left[x\right] = \frac{1}{n}$ for all $x \in X$, then prove that $H\left(\mathbf{X}\right) = log_2 n$.

6. State Jensen's inequality.

7. What you mean by round key mixing and whitening in SPN?

8. Define a Hash family.

(8 × 1 = 8 Weightage)

Part B

Answer any ***two*** questions 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. (a) Define Vigenere Cipher.

    (b) Suppose $m = 6$ and the keyword is “CIPHER” in Vigenère Cipher.
    Using this key decrypt the ciphertext “VPXZGIAXIVWPUBTTMJPWIZITWZT”.

11. (a) Suppose $K = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$ be the key used in Hill Cipher with $m = 2$, over Z_{26}. Encrypt the plaintext "july".

    (b) Find the corresponding decryption function.

UNIT - II

12. Explain Huffman's algorithm.

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

14. Suppose M is the Multiplicative Cipher and S is the Shift Cipher. Then verify that $S \times M$ is the Affine Cipher with equiprobable keys.

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 the MIXCOLUMN algorithm in AES.

17. Explain the algorithm of Merkle-Damgard construction.

(6 × 2 = 12 Weightage)

Part C

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

18. (a) Explain the working of Linear Feedback Shift Register.

    (b) Suppose $K = 8$ and the plaintext is "rendezvous" in Auto-key Cipher. Generate the key stream and hence encrypt the given plaintext.

19. (a) What are the most common types of attack models? Explain.

    (b) Explain the cryptanalysis of the Vigenère Cipher.

20. Let $\wp = \{a, b\}$ with $Pr[a] = \frac{1}{4}, Pr[b] = \frac{3}{4}$ and $\kappa = \{K_1, K_2, K_3\}$ with $Pr[K_1] = \frac{1}{2}, Pr[K_2] = \frac{1}{4}, Pr[K_3] = \frac{1}{4}$. Let $C = \{1, 2, 3, 4\}$ be the set of all possible ciphertexts and suppose the encryption functions are defined to be $e_{K_1}(a) = 1, e_{K_1}(b) = 2, e_{K_2}(a) = 2, e_{K_2}(b) = 3, e_{K_3}(a) = 3, e_{K_3}(b) = 4$. Compute the conditional probabilities $Pr[x|y]$ and $Pr[y|x]$ for all $x \in X$ and $y \in Y$.

21. (a) Explain the security of Hash functions using Preimage, Second Preimage and Collision problems.

    (b) Explain the algorithms in Random Oracle Model.

(2 × 5 = 10 Weightage)

****