23P305 (Pages: 2) Name: .....

Reg.No: .....

THIRD SEMESTER M.Sc. DEGREE EXAMINATION, NOVEMBER 2024

(CBCSS - PG)

(Regular/Supplementary/Improvement)

CC19P MTH3 E02 - CRYPTOGRAPHY

(Mathematics)

(2019 Admission onwards)

Time : 3 Hours Maximum : 30 Weightage

Part A

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

1. Define Shift Cipher. Which shift key is known as "Caesar Ciher"?
2. Define Vigenere Cipher.
3. Explain the working of Linear Feedback Shift Register.
4. Show that One-Time Pad is vulnerable to a known-plaintext attack.
5. Prove that $H(\mathbf{X}) = 0$ if and only if $Pr[x_0] = 1$ for some $x_0 \in X$ and $Pr[x] = 0$ for all $x \neq x_0$.
6. Define unicity distance of a cryptosystem.Give a formula for estimating unicity distance.
7. Define a Hash family.
8. What is the Collision problem in the security of Hash functions?

(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. Suppose that $K = (7, 3)$ is a key in an Affine Cipher over Z_{26}. Decrypt the ciphertext "AXG" with this key.
11. Find the inverse of the matrix $\begin{bmatrix} 10 & 5 & 12 \\ 3 & 14 & 21 \\ 8 & 9 & 11 \end{bmatrix}$ in $modulo \quad 26$.

UNIT - II

12. 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.

13. Prove that $H(\mathbf{X}, \mathbf{Y}) = H(\mathbf{Y}) + H(\mathbf{X}|\mathbf{Y})$.

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

UNIT - III

15. Suppose that $l = m = N_r = 4$ in SPN. Let π_s is defined as follows: where the input and output are written in hexadecimal notation.

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_s(z)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

Let π_p be defined as follows:

z	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\pi_p(z)$	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

Let $K = 0011 \quad 1010 \quad 1001 \quad 0100 \quad 1101 \quad 0110 \quad 0011 \quad 1111$

For $1 \leq r \leq 5$, define K^r to consist of 16 consecutive bits of K, beginning with K_{4r-3}. Find W^2 for the plaintext $0010 \quad 0110 \quad 1011 \quad 0111$ using this system.

16. 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 $\varepsilon_2 = \pm\frac{1}{2}$.

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) "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) 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.
(b) Explain the cryptanalysis of the Vigenère Cipher.

20. (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 $Pr[a] = 0.32, Pr[b] = 0.23, Pr[c] = 0.20, Pr[d] = 0.15$ and $Pr[e] = 0.10$. Using Huffman's algorithm to find the optimal prefix-free encoding of $\mathbf{X}$. Compare the length of this encoding to $H(\mathbf{X})$.

21. Explain about DES and AES.

(2 × 5 = 10 Weightage)

****