21P305 (Pages: 2) Name: .....

Reg.No: .....

THIRD SEMESTER M.Sc. DEGREE EXAMINATION, NOVEMBER 2022

(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. Define Shift Cipher. Encrypt "wednesday" using Caesar Ciher.
2. Evaluate $(-7503)\ mod\ 81$ and $7503\ mod\ 81$
3. Define Affine functions. Do all Affine functions used in Affine Cipher? Justify.
4. Verify that One-Time Pad provides perfect secrecy.
5. Define entropy of random variable. What is the entropy of n independent coin tosses?
6. What you mean by spurious keys? What is the entropy (per letter) of a random string of alphabets?
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. (a) Define Vigenere Cipher.
   (b) Suppose $m = 6$ and the keyword is “CIPHER” in Vigenère Cipher.
   Using this key encrypt the plaintext “thiscryptosystemisnotsecure”.
10. 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 "seeyousoon".
11. Explain the cryptanalysis of Hill Cipher.

UNIT - II

12. 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 $\mathbf{X}$.

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 $S \times M$ is the Affine Cipher with equiprobable keys.

UNIT - III

15. Explain the algorithm of SPN.

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 MIXCOLUMN algorithm in AES.

(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. 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)

****