19P305 (Pages : 2) Name: .....
Reg. No.: .....

THIRD SEMESTER M.Sc. DEGREE EXAMINATION, NOVEMBER 2020

(CBCSS - PG)

CC19 MTH3 E02 - CRYPTOGRAPHY

(Mathematics)

(2019 Admission Regular)

Time: 3 hours Maximum: 30 Weightage

PART A

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

1. Given, K = 13, encipher 'bestwishes' using shift cipher.
2. Show that permutation cipher is a special case of the Hill cipher.
3. Determine the number of keys in affine cipher over $\mathbb{Z}_{1225}$.
4. Define Substitution cipher.
5. Define one time pad.
6. Give values for entropy and redundancy of a natural language.
7. Explain encryption and decryption function of iterated cipher
8. Define nested MACs and HMAC.

(8 × 1 = 8 Weightage)

PART B

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

UNIT - I

9. Suppose $K = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$, Encipher 'Nature' using Hill cipher and decipher the same using K.
10. Find the 15 bit keystream generated using linear recurrence with $z_{i+4} = z_i + z_{i+1} \bmod 2$; $i \geq 2$ initialized with vector 1101.

11. Define Kasiski test and Index of coincidence and how it helps in cryptanalysis of Vignere cipher.

UNIT - II

12. Define the term perfect secrecy and show that shift cipher using 26 keys with equal probability $\frac{1}{26}$ has perfect secrecy for any plain text distribution

13. Explain Huffmann Algorithm.

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

UNIT - III

15. Explain Data Encryption standard with necessary deatils.

16. Explain three problems in security of Hash functions.

17. Give Merkle - Damgrad 1 Algorithm.

(6 × 2 = 12 Weightage)

PART C

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

18. (a) Define product cryptosystems and prove that $S \times M = M \times S =$ *Affine Cipher*, where S and M are Shift and multiplicative ciphers respectively.

    (b) Does all cryptosystems commute. Justify? Also prove that if two idempotent cryptosystems commute then thier product cryptosystem is also idempotent.

19. Suppose $(\mathcal{X}, \mathcal{Y}, \mathcal{K}, \mathcal{H})$ is an (N, M) - hash family, Then prove that $Pd_1 = \frac{1}{M}$ if and only if the hash family is strongly universal.

20. (a) Explain unicity distance and spurious keys.

    (b) Prove that $H(X, Y) \leq H(X) + H(Y)$ with equality if and only if X and Y are independent variables.

21. (a) Define Auto key cipher and encipher 'violettulipsaresparkling' using autokey cipher with key k =8.

    (b) Let p be a prime. Prove that the number of 2×2 matrices that are invertible over $\mathbb{Z}_p$ is $(p^2 - 1)(p^2 - p)$.

(2 × 5 = 10 Weightage)

****