L4

86109

D 11680 (Pages : 3) Name.....

Reg. No.....

THIRD SEMESTER M.Sc. DEGREE (REGULAR/SUPPLEMENTARY) EXAMINATION, NOVEMBER 2021

[November 2020 for SDE/Private Students]

(CBCSS)

Mathematics

MTH 3E 02—CRYPTOGRAPHY

(2019 Admission onwards)

Time : Three Hours Maximum : 30 Weightage

General Instructions (Not applicable to SDE/Private Students)

1. *In cases where choices are provided, students can attend* **all** *questions in each section.*
2. *The minimum number of questions to be attended from the Section / Part shall remain the same.*
3. *The instruction if any, to attend a minimum number of questions from each sub section / sub part / sub division may be ignored.*
4. *There will be an overall ceiling for each Section / Part that is equivalent to the maximum weightage of the Section / Part.*

Part A (Short Answer Questions)

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

1. Define Euler phi-function and Affine Cipher. Find the number of keys in the Affine Cipher over Z_{30}.
2. Prove that $-a \bmod m = m - (a \bmod m)$ where $a, m > 0$ and $a \neq 0 \pmod m$.
3. Decrypt the message XHPEN BDYQ which was produced with Auto key Cipher having key K = 16.
4. Define concave function and show that the function $f(x) = x^2$ is concave in the interval $(-\infty, \infty)$.
5. Explain entropy and redundancy of a natural language.
6. Describe block ciphers with example.
7. State the Piling up Lemma.

Turn over

8. Define Strongly Universal Hash Families. Prove that for such a (N, M) hash family

$$(X, Y, \kappa, H),\ \left|\{K \in \kappa : h_\kappa(x) = y\}\right| = \frac{|\kappa|}{M},\ \forall x \in X, y \in Y.$$

$(8 \times 1 = 8$ we

Part B (Short Essays)

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

Unit 1

9. List all invertible elements in Z_m for $m = 28, 35$.

10. Define involutory key. Find the number of involutory keys in the Hill Cipher over Z_{26} $m = 2$.

11. Explain Cryptanalysis of LFSR Stream Cipher.

Unit 2

12. Let S is a random variable representing the sum of a pair of dice. Compute H (S).

13. Prove that the Shift Cipher achieves perfect secrecy if every key is used probability 1/26.

14. Define unicity distance of a cryptosystem. Calculate it for Hill Cipher with $m \times m$ matrix.

Unit 3

15. Define balanced S-box. Prove that for a balanced S-box

$$N_L(0, b) = 2^{n-1},\ \forall \text{ integers } b \text{ such that } 0 < b \leq 2^n - 1.$$

16. Describe Data Encryption Standard (DES).

17. Compare keyed and unkeyed hash functions. Define (N, M) hash family. What problems that should be addressed by a secure

Part C (Essays)

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

18. (a) Define Vigenere Cipher. Encrypt the message ATTACK AT ONCE using keyword READY.

(b) Define Hill Cipher. Prove that t the number of 2×2 invertible matrices over Z_p is :

$(p^2 - 1)(p^2 - p)$, where p prime.

19. (a) Suppose (P, C, K, E, D) is a cryptosystem where $|C| = |P|$ and keys are chosen equiprobably. Let R_L be the redundancy of the language. Then prove that given a string of cipher text of length n, the expected number of spurious keys $\bar{s}_n \geq \frac{|K|}{|P|^{nR_L}} - 1$.

(b) Consider a cryptosystem in which P = {a, b, c}, K = {K_1, K_2, K_3} and C = {1, 2, 3, 4}. The encryption matrix is as follows :

		a	b	c
K_1	...	1	2	3
K_2	...	2	3	4
K_3	...	3	4	1

Given that the keys are chosen equiprobably and the plaintext probability distribution is Pr [a] = 1/2 , Pr [b] = 1/3, Pr [c] = 1/6. Then compute H (P), H (C), H (K), H (K/C), H (P/C).

20. Explain Linear cryptanalysis and Differential cryptanalysis.

21. Describe Message Authentication Codes (MAC) and explain the construction of Nested MAC, HMAC.

($2 \times 5 = 10$ weightage)