D 31182 (Pages : 3) Name.....

Reg. No.....

THIRD SEMESTER M.Sc. DEGREE (REGULAR/SUPPLEMENTARY) EXAMINATION, NOVEMBER 2022

[November 2021 Session for SDE/Private Students]

(CBCSS)

Mathematics

MTH 3E 02—CRYPTOGRAPHY

(2019 Admission onwards)

Time : Three Hours Maximum : 30 Weightage

Part A (Short Answer Questions)

Answer **all** *questions.*
Each question has weight 1.

1. Define Shift cipher. Encrypt the message "Number Theory" using Shift cipher with K = 9.
2. Define synchronous stream cipher, Periodic stream cipher and non-synchronous stream cipher.
3. Write short note on Cryptanalysis.
4. Explain the term Perfect secrecy.
5. Define concave function and strictly concave function with example.
6. Describe Product cryptosystem .Give an example.
7. Explain iterated block ciphers.
8. Define cryptographic hash functions.

(8 × 1 = 8 weightage)

Part B (Short Essay)

Answer any two questions from each unit.
Each question has weight 2.

Unit 1

9. Define Affine Cipher and involutory key. Prove that K = (a, b) is an involutory key in Affine Cipher over Z_n if and only if $a^{-1} \bmod n = a$ and $b(a + 1) \equiv 0 \pmod n$.

Turn over

10. (a) Let π be the permutation of {1, 2, ...8}. Compute π^{-1} where

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	1	6	2	7	3	8	5

(b) Decrypt the following cipher text which was encrypted using above key π for a perm cipher with $m = 8$. TGEEMNELNNTDROEOAAIIDOETCSHAEIRLM.

11. Explain Cryptanalysis of Vigenere Cipher.

UNIT 2

12. Prove that a cryptosystem has perfect secrecy if and only if H(P/C) = H(P).

13. Let (P, C, K, E, D) be a cryptosystem. Then prove that H(K/C) = H(K) + H(P) – H(C).

14. Explain the cryptosystem One-time Pad. Suppose y and y' are two cipher text elements tuples) in the one time Pad that are obtained by encrypting plaintexts x and x' respectiv the same key K. Then prove that $x + x' = y + y' \pmod 2$.

UNIT 3

15. Describe Substitution-Permutation Networks (SPN).

16. Explain Data Encryption Standard (DES).

17. Explain Nested Message Authentication Codes. How the security of a nested MA ensured ?

$(6 \times 2 = 12$

Part C (Essay)

Answer any **two** *questions.*
Each question has weight 5.

18. (a) Define Hill Cipher. Explain how encryptions and decryptions are done in this Ci example and stating conditions on transformation matrix.

(b) Prove that the number of 2×2 invertible matrices over Z_p is $(p^2 - 1)(p^2 - p)$, wher

(c) If A is a matrix over Z_{26} such that $A^2 = I$. Then prove that $\det A \equiv \pm 1 \pmod{26}$

19. (a) Define entropy and conditional entropy. Prove that in any cryptosystem, H(K/C)

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

20. (a) Explain Linear cryptanalysis.

(b) State and Prove the Piling-up lemma.

(c) Compute the linear approximation table for the S-box given below :

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

21. (a) Compare between keyed and unkeyed hash functions. What are the three problems that should be addressed by a secure hash function ?

(b) Explain Random Oracle Model Hash functions.

(2 × 5 = 10 weightage)