20P305 (Pages: 2) Name…….……

Reg. No……..

THIRD SEMESTER M.Sc. DEGREE EXAMINATION, NOVEMBER 2021

(CBCSS-PG)

(Regular/Supplementary/Improvement)

CC19P MTH3 E02 – CRYPTOGRAPHY

(Mathematics)

(2019 Admission onwards)

Time: Three Hours Maximum: 30 Weightage

PART A

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

1. Define Substitution cipher.
2. What is a monoalphabetic cryptosystem?
3. What are the most common types of attack models?
4. Explain Kasiski test.
5. Explain perfect secrecy of a cryptosystem.
6. Give a fundamental relationship that exists among the entropies of components of a cryptosystem.
7. Describe an iterated cipher.
8. Define an unkeyed hash function.

(8 × 1 = 8 Weightage)

PART B

Answer any ***six*** questions. Each question carries 2 weightage.

Unit I

9. Using Shift cipher convert the following plain text to cipher text, where the key K = 11 "**wewillmeetatmidnight"**
10. Explain synchronous stream cipher.
11. Find the key when the plain text **friday** is encrypted using a Hill Cipher with $m = 2$ to give the ciphertext **PQCFKU.**

Unit II

12. Explain different types of approaches for evaluating the security of a cryptosystem
13. Suppose X is a random variable with probability distribution which takes on the values p1, p2, … , pn. Then $H(X) \leq log_2 n$ with equality if and only if $pi = 1/n$, $1 \leq i \leq n$.
14. Explain unicity distance of a cryptosystem and get an estimate for it.

Unit III

15. State and prove Piling - up lemma.
16. Describe DES.
17. Explain the random oracle model for a hash function

(6 × 2 = 12 Weightage)

PART C

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

18. Describe Vigenere Cipher and encrypt the plain text "**thiscryptosystemisnotsecure"** with m = 6 and keyword **CIPHER.**
19. Prove that $H(\mathbf{X}, \mathbf{Y}) \leq H(\mathbf{X}) + H(\mathbf{Y})$, with equality if and only if **X** and **Y** are independent random variables.
20. Explain Substitution- Permutation Networks.
21. Give the Secure Hash Algorithm SHA - 1.

(2 × 5 = 10 Weightage)

****