14

D 91043 (Pages : 2) Name.....

Reg. No.....

THIRD SEMESTER M.A./M.Sc./M.Com. DEGREE (REGULAR) EXAMINATION NOVEMBER 2020

(CBCSS)

Mathematics

MTH 3E 02—CRYPTOGRAPHY

(2019 Admissions)

Time : Three Hours Maximum : 30 Weightag

General Instructions

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

Part A (Short Answer Questions)

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

1. Define the terms Cryptosystem, monoalphabetic cryptosystem, polyalphabetic cryptosystem wi example.
2. Compare between Substitution Cipher and Permutation Cipher.
3. Prove that $a \bmod m = b \bmod m$ if and only if $a = b \pmod m$.
4. State Jensen's inequality.
5. Prove that $H(X/Y) \leq H(X)$, with equality if and only if X and Y are independent.
6. Explain the terms round key mixing and whitening in SPN.
7. Define hash family.
8. Write short note on differential cryptanalysis.

($8 \times 1 = 8$ weighta

Part B (Short Essay)

Answer any **two** *questions.*
Each question has weightage 2.

9. Use Hill Cipher with key $K = \begin{pmatrix} 5 & 3 \\ 2 & 4 \end{pmatrix}$ to encrypt the message GIVE THEM TIME.
10. Define involutory key. Find the number of involutory keys in the Permutation Cipher for $m =$
11. Explain Cryptanalysis of Affine Cipher.

Turn c

12. Prove that if a cryptosystem has perfect secrecy and $|K| = |C| = |P|$, then every cipher text is equally probable.

13. Define unicity distance of a cryptosystem. Calculate it for Substitution Cipher.

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

15. State and prove the Piling-up-lemma.

16. Explain Random Oracle Model Hash functions.

17. Describe Message Authentication code(MAC) and explain HMAC.

(6 × 2 = 12 weightage)

Part C (Essay)

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

18. (a) Define different types of Stream Ciphers and explain the methods of keystream generation.

    (b) How Cryptanalysis done in Stream Cipher.

19. (a) Prove that the Affine Cipher achieves perfect secrecy if every key is used with equal probability 1/312.

    (b) Compute H(K/C) and H(K/P,C) for the Affine Cipher assuming that keys are used equiprobable and plaintexts are equiprobable.

20. Describe and analyse Data Encryption Standard(DES) and Advanced Encryption Standard (AES).

21. Define iterated hash functions and explain the generic construction and the Merkle-Damgård Construction methods of the same.

(2 × 5 = 10 weightage)