H

Roll No. .....

TBC–503

B. C. A. (FIFTH SEMESTER)

MID SEMESTER EXAMINATION, 2022

CRYPTOGRAPHY

Time : 1½ Hours

Maximum Marks : 50

Note : (i) Answer all the questions by choosing any ***one*** of the sub-questions.

(ii) Each question carries 10 marks.

1. (a) What do you mean by attacks ? Differentiate between active and passive attack. (CO1)

OR

(b) What are the different types of Cryptography ? Using the Vigenère cipher, encrypt the word "explanation' using the key leg. (CO1)

P. T. O.

2. (a) (i) Explain Caesar cipher with numerical example.

(ii) Encrypt the word "diamond" using affine cipher having key pair (5, 2). (CO2)

OR

(b) Explain *five* security services and eight security mechanisms in details. (CO1)

3. (a) Explain the Hill Cipher in detail. Use a Hill Cipher to encrypt the message" We live in an insecure world" by using following key : [03 02 05 07] (CO1)

OR

(b) (i) What is the Mono-Alphabetic and Poly-Alphabetic Substitution Cipher.

(ii) Using Playfair cipher encrypt the message 'the platinum is precious than gold". Ignore the white spaces between words. The key used for encryption is GUIDANCE. (CO1)

4. (a) What is IDEA algorithm in cryptography ? Explain in detail. (CO1)

OR

(b) Explain DES structure. If the key with parity bit (64 bits) is 0123 ABCD 2562 1456, find the first round key. (CO1)

5. (a) (i) Explain Diffie-Hellman key Exchange/Agreement Algorithm.

(ii) What is the rail fence cipher ? If the plaintext is "Meet me at the park" then what will be the equivalent rail fence cipher text (CO2)

OR

(b) Write short notes on the following : (CO2)

(i) Steganography

(ii) Security Goals

(iii) Diffusion and Confusion