H

Roll No. .....

TBC–503

B. C. A. (FIFTH SEMESTER)
END SEMESTER EXAMINATION, 2021-22

CRYPTOGRAPHY

Time : Three Hours

Maximum Marks : 100

Note : (i) All questions are compulsory.

(ii) Answer any ***two*** sub-questions among (a), (b) and (c) in each main question.

(iii) Total marks in each main question are **twenty**.

(iv) Each question carries 10 marks.

1. (a) What taxonomy is used for the security goals, security services arid security mechanism of cryptography ? (CO1)

(b) Explain Caesar cipher with numerical example and explain the types of Cryptography. (CO1)

P. T. O.

(c) 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)

2. (a) Explain Data Encryption Standard (DES) in detail. (CO2)

(b) Explain IDEA algorithm in detail with the help of its process diagram. (CO2)

(c) What do you understand by Feistel cipher structure ? Explain with a suitable block diagram. (CO2)

3. (a) Briefly explain Diffie-Hellman key exchange. (CO3)

Users A and B exchange the key using Diffie-Hellman algorithm. Assume $\alpha = 5$, $q = 11$, XA = 2, XB = 3. Find the value of YA, YB and k. (CO3)

(b) Explain placement of encryption function. (CO3)

(c) Explain RC5 with example and symmetric key distribution. (CO3)

4. (a) Explain the RSA algorithm in detail. For the given values trace the sequence of calculation in RSA : P = 7, Q = 13, $e = 5$, M = 10. (CO4)

(b) Explain public key distribution with an example. (CO4)

(c) Explain Fermat and Euler's theorem with numerical example. (CO4)

5. (a) Explain hash cryptography with example. (CO5)

(b) Write short notes on Digital signature and MIME. (CO5)

(c) Explain MD-5 Message Digest Algorithm. (CO5)

370