H Roll No. .....

TBC–503

B. C. A. (FIFTH SEMESTER)
END SEMESTER
EXAMINATION, Jan., 2023

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 sub-question carries 10 marks.

1. (a) What is cryptography ? Explain the security Goals. (CO1)

(b) What is Ceaser Cipher Method ? Using Ceaser Cipher encrypt (CO1)

Text : ATTACKATONCE

Shift : 4

P. T. O.

(c) What is the difference between Block Cipher and Stream Cipher ? (CO1)

2. (a) What is AES ? Describe with the help of diagram. (CO2)

(b) What is DES ? What is the difference between Double DES and Triple DES ? (CO2)

(c) What is fiestal Structure ? Explain different modes of operations that are use in Block Cipher. (CO2)

3. (a) What are different types of keys in cryptography ? Also mention the advantage and disadvantage of each.(CO3)

(b) Explain IDEA Algorithm with diagram. (CO3)

(c) What is Blowfish Algorithm with diagram ? (CO3)

4. (a) Describe the RSA algorithm. Encrypt plaintext 9 using the RSA public-key encryption algorithm. This example uses prime numbers 7 and 11 to generate the public and private keys. (CO4)

(b) What is public-key infrastructure ? What are the roles of the public and private key ? (CO4)

(c) Explain Elgamal cryptosystem. Also explain the difference between symmetric key and asymmetric key. (CO4)

5. (a) Explain Digital Signature with help of diagram. (CO5)

(b) Explain the following : (CO5)

(i) SHA-512

(ii) MD-5 Message Digest Algorithm

(c) What is message authentication ? Explain the ways of Message Authentication. (CO5)

400