H Roll No. .....

# TBC–504

## B. C. A. (FIFTH SEMESTER)
## END SEMESTER
## EXAMINATION, Dec., 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 are different security goals ? Distinguish between them example. (CO1)

(b) Differentiate between substitution cipher and transposition cipher. Use vigenere cipher with key HEALTH to encrypt the message "Life is full of surprises". (CO1)

*P. T. O.*

(c) What are different types of cryptanalysis attacks ? Explain in short. (CO1)

2. (a) State the Chinese remainder theorem and fix X for the given set of congruent equations $X \equiv 2 \bmod 3$, $X \equiv 3 \bmod 5$ and $X \equiv 2 \bmod 7$. (CO2)

(b) What is DES ? How is expansion permutation function done in DES ? (CO2)

(c) Explain block cipher modes of operations. (CO2)

3. (a) Write and explain blowfish algorithm with suitable block diagram. (CO3)

(b) Explain the round transformation of IDEA. Also explain the key scheduling of IDEA. (CO3)

(c) Explain the process of symmetric key distribution using asymmetric cryptography. (CO3)

4. (a) Describe RSA algorithm and Estimate the encryption and decryption values for the RSA algorithm parameters. (CO4)



(b) Explain ElGamal crypto system with example. Discuss its security aspects. (CO4)

(c) Describe and explain Fermat's theorem. (CO4)

5. (a) What do you mean by digital signature standard ? Explain the steps involved in digital signature algorithm. (CO5)

(b) What are the requirements of cryptographic hash functions ? (CO5)

(c) Describe the steps in finding the message digest using SHA-512 algorithm. (CO5)