H Roll No. ..2192009.......

TBC–504

B. C. A. (FIFTH SEMESTER)

MID SEMESTER

EXAMINATION, Oct., 2023

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 is the difference between mono-alphabetic and polyalphabetic cipher ? Use Caesar cipher with key = 15 to encrypt the message "Hello". (CO1)

OR

(b) What is differential cryptanalysis ? Explain the types of cryptanalysis attacks. (CO1)

P. T. O.

2. (a) What are different security goals ? Distinguish between message integrity and message authentication. (CO1/CO2)

OR

(b) Discuss the design principles of block cipher technique. What are the confusion and diffusion properties of Modern Ciphers ? (CO1/CO2)

3. (a) Explain the Chinese remainder theorem with an example. (CO1/CO2)

OR

(b) Explain Data Encryption Standard (DES) in detail. (CO1/CO2)

4. (a) What is the motivation behind Feistel's cipher ? Explain Feistel's cipher. (CO2)

OR

(b) What are the different block cipher modes of operations ? Explain. (CO2)

5. (a) Differentiate between active and passive attacks with example. (CO1)

OR

(b) Write Euclid's algorithm. How is GCD calculated with Euclid's algorithm ? Calculate the GCD of (270, 192). (CO1)