DEPARTMENT OF COMPUTER SCIENCE AND ENGG.
NATIONAL INSTITUTE OF TECHNOLOGY, TIRUCHIRAPPALLI.
B.Tech(C.S.E) SIXTH SEMESTER

CYCLE TEST I

CSPC63 Principles of Cryptography

13/02/25 Time: 60 mins

ANSWER ALL THE QUESTIONS

MAX:5 * 4 = 20 Marks

1. What are the different types of attacks? Explain each one of them with examples. (4)

2. With a neat block diagram, explain the working of a round in DES. (4)

3. Alice often needs to encipher a plain text made of both letters (a to z) and digits (0 to 9). Find out the key domain and the modulus if she uses a

   (a)a multiplicative cipher (2)

   (b)an affine cipher (2)

4. A transposition cipher is used to produce the following ciphertext:

   X 2! H M E S S S E 2 Y T A 2 I I A

   The key used was: 5 2 6 3 4 1

   What is the plaintext? (4)

5. Using EEA, find the multiplicative inverse of 23 in Z_{100} (4)

****