Information Assurance and Security (IT352) Laboratory-Program -1

Write a program that should demonstrate that initial permutation and final permutation of DES are inverse of each other. Program should take the input of any size during run time and it can be an alphanumeric/integer/alphabets. If the input size greater than 64 bits, first divide the input into a fixed size block and then demonstrate for the computed fixed size blocks. Assume that no DES rounds exist between initial permutation and final permutation. Print all the intermediate results.

Steps:

a. Consider the run-time input of any size.
b. For each character of the input, take the ASCII value individually, convert the obtained sequence of ASCII values into binary, apply block formation operation.
c. Apply initial permutation operation for each block of size 64 bits individually and display the output of the initial permutation operation.
d. Apply final permutation operation to the output of initial permutation and display the output final permutation.
e. Ensure that output of final permutation is same as respective 64bits input block.

Sample Text Case:

1. Input: NITK Surathkal Mangalore 575025 **(ignore the space)**

Submit program as well as screenshot of the output to it35215b@gmail.com before the deadline.

File name of the program : RegisterNo_IT352_P1

(P1 indicates Program Number-1)

File name of the screenshot : RegisterNo_IT352_P1_S1

(S1 indicates screenshot for the first test case, similarly, for other test cases S2, S3, S4, S5)

Date of Laboratory : 9th January 2019

Dead Line of Submission : 9th January 2019 (on or before 5:30PM).

Note: Kindly clarify the doubt(s) (if any related to the said program) before commencement of the laboratory.