CSE350/550: Network Security: Programming Exercise 1

Listed below, you will find a brief description of 2 projects, numbered 0 and 1. In groups of 2, you are required to pick project 0 or 1 as determined by k = A1+A2 mod 2, where
A1 = last_4_digits_of_entry_no_of_first_student, and
A2 = last_4_digits_of_entry_no_of_second_student.

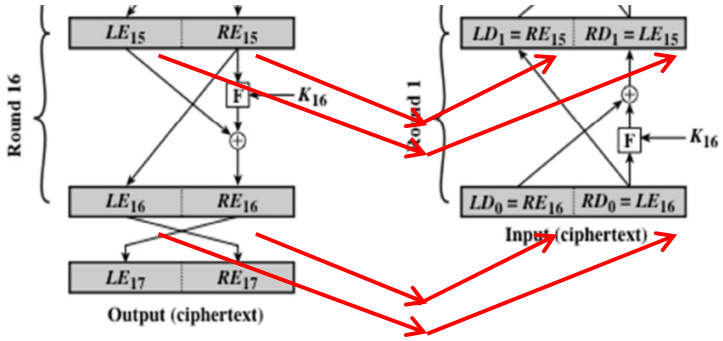
Complete that project and submit a report (with a working system) on or before Thursday Jan 30, 11.55 pm. The submission will consist of:

1. a 3 to 4 page document describing the system you have designed and implemented,
2. the code as a separate file, and
3. a brief 6 to 8 slides presentation that you will use to present as part of evaluation.

You will be evaluated based on a 15 min interaction that will consist of the above presentation and demonstration on your laptop connected to an overhead projector.

Project 0:

You are required to develop a program to encrypt (and similarly decrypt) a 64-bit plaintext using DES. Instead of using an available library, ***I insist that you program any and every element of each of the 16 rounds of DES*** (and that means F-box, 32-bit exchanges, generation of sub-key required in each round). Having done that, with one or more 64-bit plaintext(s), verify that indeed the output of the J^{th} encryption round is identical to the output of the $(16\text{-}J)^{th}$ decryption round. (This is illustrated below for round 16 of encryption).



Project 1:

You are required to develop a program to encrypt (and similarly decrypt) a 128-bit plaintext using AES that uses keys of size 128 bit, and 10 rounds. Instead of using an available library, ***I insist that you program any and every element of each of the 10 rounds of AES*** (and that means Substitute bytes, shift-rows, etc., generation of sub-keys, etc.). Having done that, and for a one or more input plaintext(s), verify that indeed the output of the 1st and 9th encryption round is identical to the output of the corresponding decryption rounds. (This is illustrated below).