

Programming assignment no. 2 (due date TUE, Feb 20, 2024)

Listed below, you will find brief description of 2 projects, numbered 0 through 1. In groups of 2 you are required to:

- pick one project (see algorithm below for you to pick a project),
- complete that project, and
- submit a report (with a working system) on or before **TUE, Feb 20, 2024**. The outcome will be evaluated by me and the TAs in an oral presentation that you will make using Google Meet.

Further:

- You may use any programming language that you are comfortable with, including C, C++, Java, Python, etc., and
- Do not copy your assignment from another group, or allow others to copy your assignment – be aware it is easy for us to find out (it will also show up in the oral presentation you will make).

Algorithm to pick a project: pick project numbered 0 or 1 as determined by $k = (A1 + A2) \bmod 2$, where

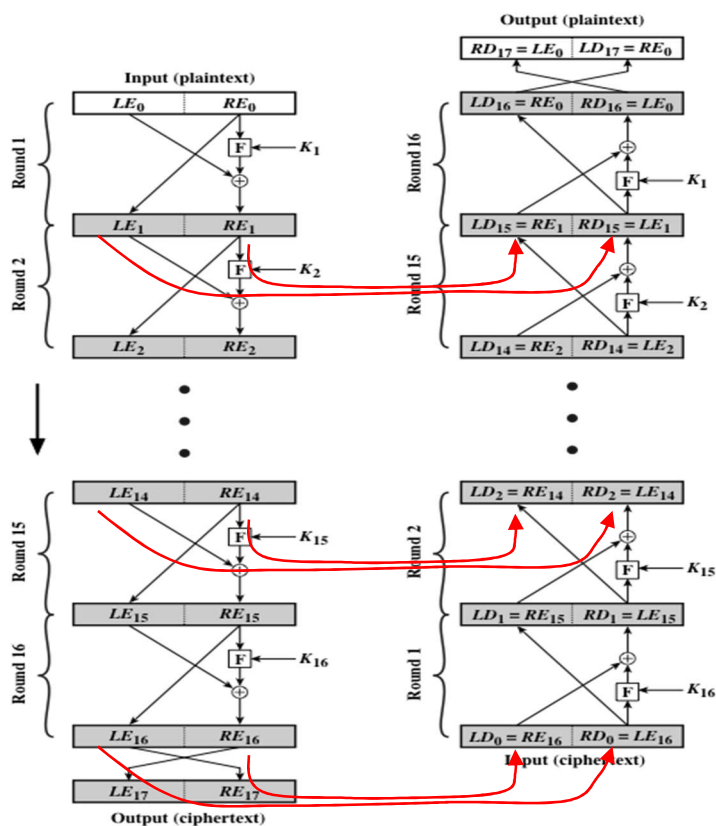
$A1$ = last_4_digits_of_entry_no_of_first_student, and $A2$ = last_4_digits_of_entry_no_of_second_student.

The submission will consist of three parts:

- a 2 to 4-page document describing system you have designed, together with sample inputs/outputs from the code,
- the code itself as a separate file, and
- 5 to 8 slides that you will use to present your work.

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, etc.). Then, with at least THREE pairs of < plaintext, ciphertext>:

- Verify that the ciphertext when decrypted will yield the original plaintext,
- Verify that output of the 1st encryption round is same as output of the 15th decryption round as illustrated below, and
- Verify that output of the 14th encryption round is same as the output of the 2nd decryption round as illustrated below.



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 (repeat, 10 rounds). Instead of using an available library, ***I insist that you program each and every element of each of the 10 rounds of AES*** (and that means Substitute bytes, shift-rows, etc., etc., and generation of sub-keys, etc.). Having done that, with at least THREE pairs of <plaintext, ciphertext>:

- Verify that the ciphertext when decrypted will yield the original plaintext,
- Verify that the output of 1st encryption round is same as output of the 9th decryption round as illustrated below, and
- Verify that the output of 9th encryption round is same as output of the 1st decryption round as illustrated below.

