CSE350/550: Network Security (Jan-May 2025)

Programming assignment no. 2 (due date FRI, Feb 21, 2025)

Listed below, you will find brief description of 2 projects, numbered 0 through 1. In groups of 2 you are required to: a. pick one project (see algorithm below for you to pick a project),

b. complete that project, and

c. submit a report (with a working system) on or before FRI, Feb 21, 2025. The outcome will be evaluated by me and the TAs in an oral presentation that you will make.

Further:

a. You may use any programming language that you are comfortable with, including C, C++, Java, Python, etc. on any platform, Linux, MS Windows, etc., and

b. 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, 1, or 2 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.

The submission will consist of four parts:

1. a 2- to 4-page Word or pdf document describing the system you have designed,
2. sample inputs and/or outputs from running the code you have written,
3. the code itself as a separate file, and
4. 5 to 8 slides that you will use to present your work during your presentation to me & TAs.

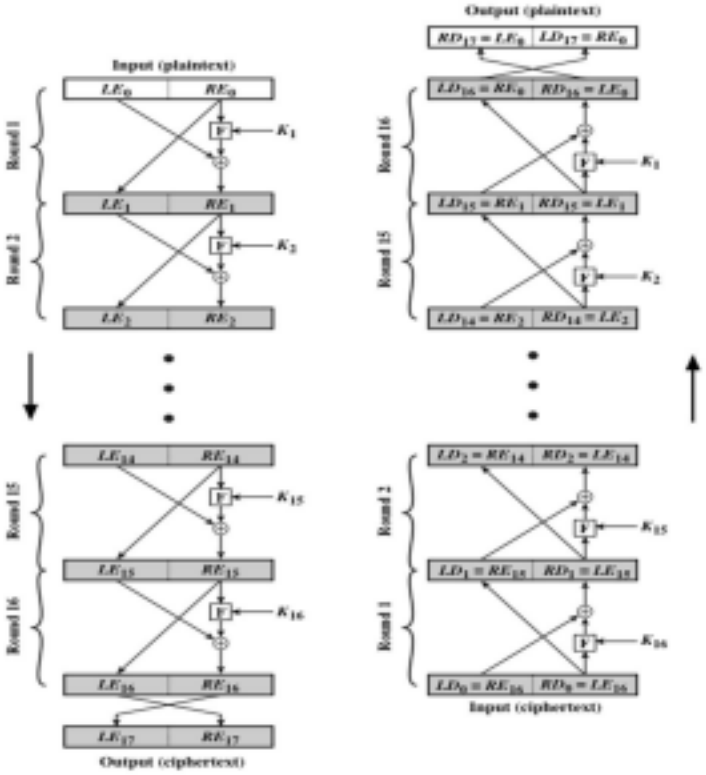
Continued on next 2 pages

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

a. Verify that the ciphertext when decrypted will yield the original plaintext,

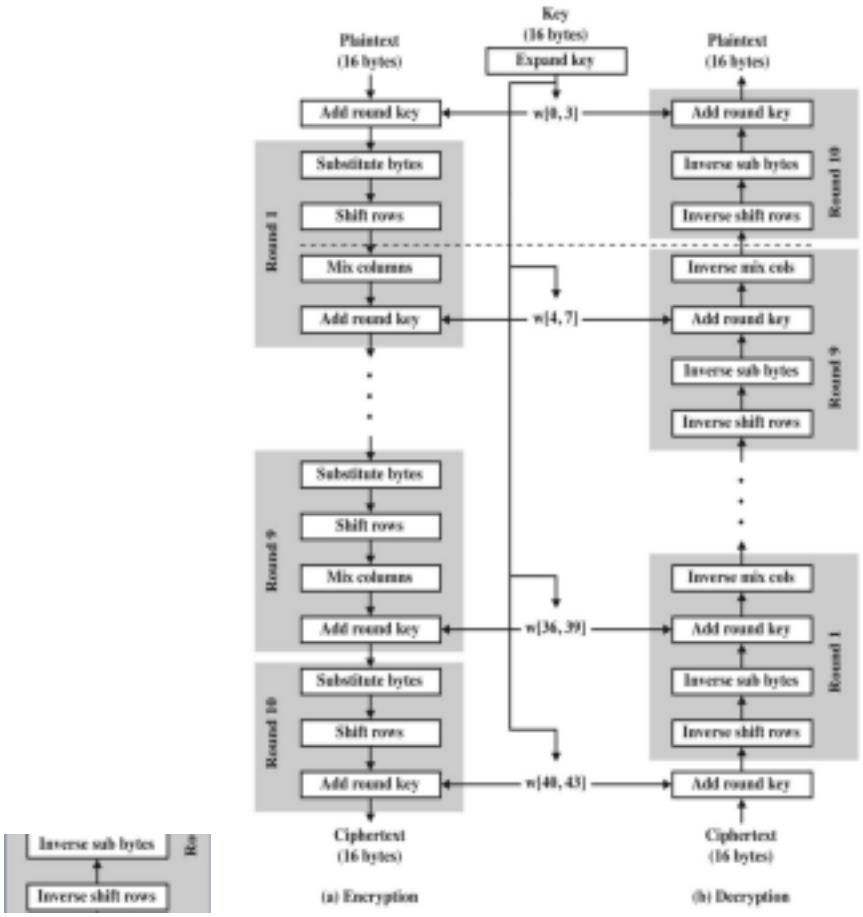
b. Verify that output of the 1st encryption round is same as output of the 15th decryption round as illustrated below, and

c. 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>:

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


Key
(16 bytes)
Expand key
Plaintext
(16 bytes)
Add round key
w[0, 3]
Substitute bytes
Shift rows
Mix columns
Add round key
w[4, 7]
Round 1
Substitute bytes
Shift rows
Mix columns
Add round key
w[36, 39]
Round 9
Substitute bytes
Shift rows
Add round key
w[40, 43]
Round 10
Ciphertext
(16 bytes)
(a) Encryption
Plaintext
(16 bytes)
Add round key
Inverse sub bytes
Inverse shift rows
Round 10
Inverse mix cols
Add round key
Inverse sub bytes
Inverse shift rows
Round 9
Inverse mix cols
Add round key
Inverse sub bytes
Inverse shift rows
Round 1
Add round key
Ciphertext
(16 bytes)
(b) Decryption
Inverse sub bytes
Inverse shift rows