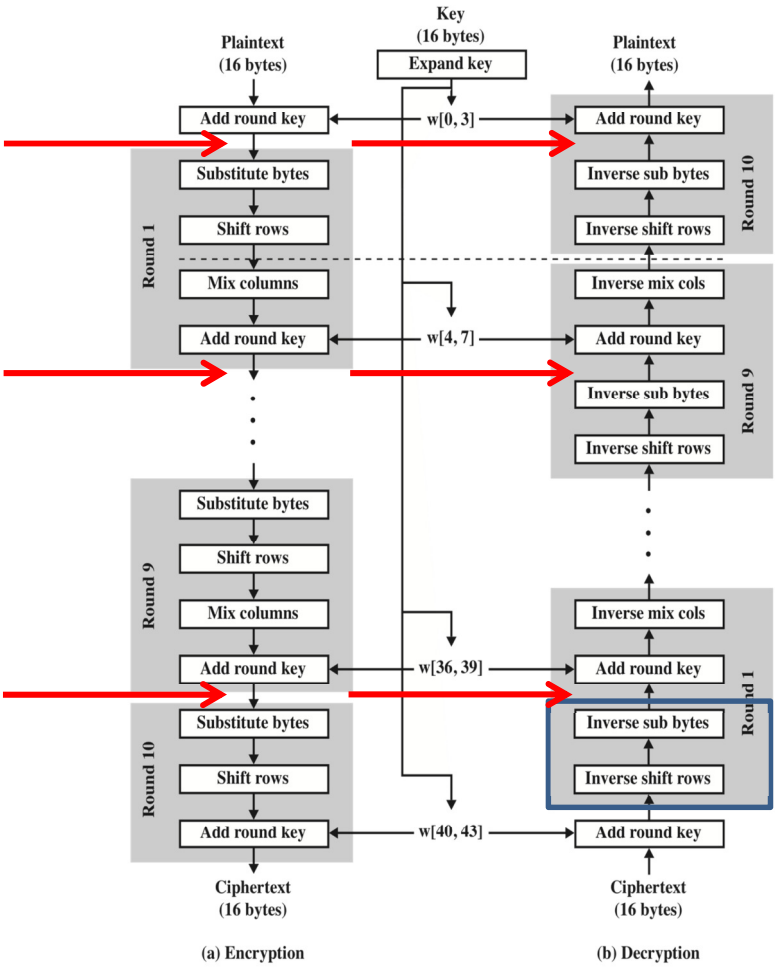
SIL765: Network & System Security: projects

Listed below, you will find a brief description of 3 projects, numbered 0, 1, 2. In groups of 2, you are required to pick the project 0, 1 or 2 as determined by k = A1+A2 mod 3, where
A1 = last_4_digits_of_entry_no_of_first_student, and
A2 = last_4_digits_of_entry_no_of_second_student.

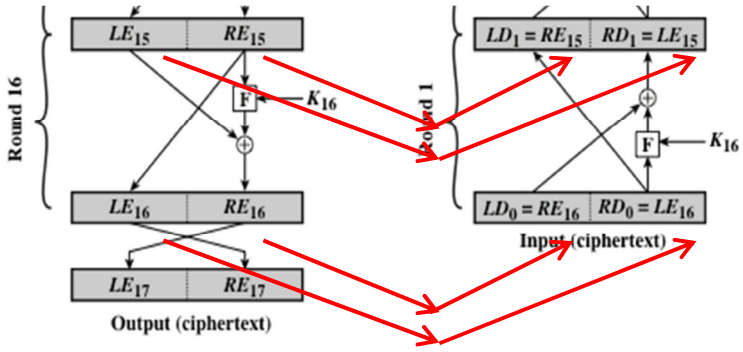
Complete that project and submit a report (with a working system) on or before Monday Feb 13, 5 pm. The submission will consist of a 3 to 4 page document describing the system you have designed and implemented. You will also upload the code as a separate file. You will be evaluated based on a 15 min interaction that will consist of a 5 to 7 slides 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 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/every element of each of the 10 rounds of AES (and that means Substitute bytes, shift-rows, etc, generation of sub-keys, one for round). 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).



Project 1:

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/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 2:

You are required to implement a "key distribution centre" that already has established a "master key" with a known set of client machines (such as A, B, C, …). And program the interactions between a device A that wishes to establish secure communication with another device B. Possibly the 3 systems would be on three different machines. Of course all communications between A, B, the key distribution centre is encrypted as shown below.

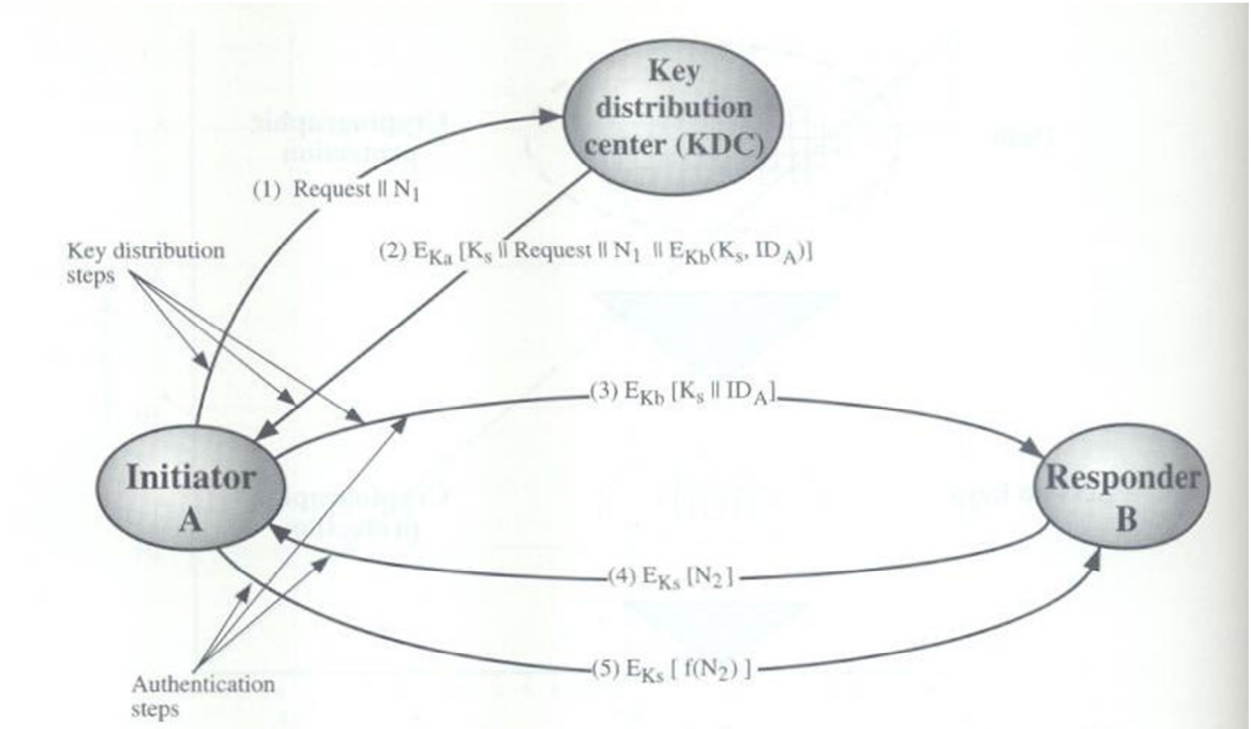


Figure 5.9 Key Distribution Scenario.