Crypto and Comm Security **Homework 2**
CS 6750 Fall 2009 (Pucella) **Due: Oct 1, 2009**

Note on integrity: You may discuss problems with fellow students, but all written work must be entirely your own, and should not be from any other course, present or past. If you use a solution from another source you must cite it, including from other people who help you.

Questions

(1) Code, in whatever programming language you want, the full 16 rounds DES algorithm for encryption and for decryption. I do not care about efficiency, but I care about clarity—your code must be understandable.

Your code should behave as follows. For encryption, it should accept as input a 64-bits plaintext expressed as a string of 16 hexadecimal characters, and a 64-bits key also expressed as a string of 16 hexadecimal characters.

Your code should print the following as it computes: for each round, the round number, the key used in that round, and the string produced by that round. (The result of the last round is not the final ciphertext, because of the final permutation that DES prescribes.) Your code should print out the final ciphertext as well. Every bit string should be printed out in hexadecimal.

For decryption, something similar. Your decryption code should accept as input a string of ciphertext as a string of 16 hexadecimal characters (giving you 64 bits, which is what DES can handle) and a key as a string of 16 hexadecimal characters (giving you 64 bits). Your code should as befoer print at each round the round number, the key used in that round, and the string produced by that round.

Make sure that if you decrypt what you encrypted using the same key, the result is the original plaintext...

Please hand-in your source code for both encryption and decryption, as well as sample outputs showing inputs (text and key), and all the information produced by your programs.

(2) Modify your code from question (1) so that in each round, the permutation is done *before* the S-boxes are applied. There are a few ways to do that, so just pick one and describe how you do encryption and decryption. Again, hand-in your source code for both encryption and decryption, as well as sample outputs showing inputs (text and key), and all the information produced by your programs.