Homework Assignment # 3

Due Date: Wednesday, September 27

1. There are two reading assignments related to DES:
   (a) Section 3.3 in the textbook,
   (b) Sections 1.1–3.5 from Gustavus Simmons' book. Copies of these pages are distributed in class.

2. As stated in Section 3.3 of the textbook, one important property which makes DES secure is that the S-boxes are non-linear. In this problem we are going to verify this property by computing the output of S_1 for several pairs of inputs.

   Show that $S_1(x_1) \oplus S_1(x_2) \neq S_1(x_1 \oplus x_2)$, where "$\oplus$" denotes bitwise XOR, for:
   (a) $x_1 = 000000$, $x_2 = 000001$
   (b) $x_1 = 111111$, $x_2 = 100000$
   (c) $x_1 = 101010$, $x_2 = 010101$

3. We want to verify that $\mathrm{IP}(\cdot)$ and $\mathrm{IP}^{-1}(\cdot)$ are truly inverse operations. We consider a vector $x = (x_1, x_2, \ldots, x_{64})$ of 64 bits. Show that $\mathrm{IP}^{-1}(\mathrm{IP}(x)) = x$ for the first five bits of x, i.e. for $x_i, i = 1, 2, 3, 4, 5$.

4. What is the output of the first iteration of the DES algorithm when the plaintext and the key are both all zero?

5. Remember that it is desirable for good block ciphers that a change in one input bit effects many output bits (diffusion or avalanche effect). We try now to get a feeling for the diffusion property of DES. We apply an input word that has a "1" at bit position 57 and all other bits and the key are all zero? (Note that the input word has to run through the initial permutation.)
   (a) How many S-boxes get different inputs compared to the case considered in the previous problem?
   (b) What is the minimum number of output bits of the S-boxes that will change according to the S-box design criteria?
   (c) What is the output after the first round?
   (d) How many output bits have actually changed compared to the case when the plaintext was all zero. (Observe that we only consider a single round here. There will be more and more output differences after every new round. Hence the term *avalanche effect*).

6. As shown in the lecture, for the decryption process a reversed key schedule is needed. Design a fast scheme which generates the 16 sub keys in the order $k_{16}, k_{15}, \cdots, k_1$. Use only modules which perform cyclic right shifts and permutations. (Hint: Consider the fact that $C_0 = C_{16}$ and $D_0 = D_{16}$.) — The solution to this problem is in the lecture notes. *I would like to ask you not to look at the notes for this problem.*

7. DES has a somewhat surprising property related to bitwise complements of its inputs and output. We will investigate the property in this problem.

   We denote the bitwise complement of a number A (that is, all bits are "flipped") by A'. Let "$\oplus$" denote bitwise XOR. We want to show that if

   $$y = \mathrm{DES}_k(x)$$

   then

   $$y' = \mathrm{DES}_{k'}(x'). \tag{1}$$

   This states that if we complement the cleartext and the key, then the ciphertext output will also be the complement of the original ciphertext. Your task is to **prove** this property.

8. Assume we perform a known-plaintext attack against DES with one pair of plain and ciphertext. How many keys do we have to test in a worst-case scenario if we apply an exhaustive key search in a straightforward way? How many on average?