T-79.4501 Cryptography and Data Security
2006 / Homework 2
Wed 27.9 and Thu 28.9

1. Consider the DES S-box S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

   (a) For the following 6-bit inputs: `000000, 010011, 101100, 111011`, what are the corresponding outputs?

   (b) Show that the second row of S_4 can be obtained from the first row by means of the following mapping:

$$(y_1, y_2, y_3, y_4) \mapsto (y_2, y_1, y_4, y_3) \oplus (0, 1, 1, 0)$$

2. Let us consider the `mult` operation in IDEA.

   (a) Use the Extended Euclidean Algorithm to compute the inverse of 357 with respect to `mult`.

   (b) What is the inverse of `0` with respect to `mult`?

3. The Mangler function of IDEA takes two 16-bit data inputs Y_{in} and Z_{in} and it produces two 16-bit outputs Y_{out} and Z_{out}, and it is controlled by two 16-bit keys Ke and Ke (see Lecture 3). Compute the outputs with the following keys and inputs:

   (a) $Ke = Kf = 1024$ and $Y_{in} = Z_{in} = 64$

   (b) $Ke = Z_{in} = 512$ and $Kf = Y_{in} = 128$

4. Show that the even round of IDEA with any given round keys Ke and Kf is its own inverse.

5. In the round key expansion procedure Rijndael makes use of eight-bit constants C_i, $i = 1, 2, 3, ..., 30$ that can be computed as

$$C_i = 2^{i-1}$$

   in polynomial arithmetic modulo $m(x) = x^8 + x^4 + x^3 + x + 1$. For example, $C_1 =$ `00000001`, $C_2 = 2 =$ `00000010`, etc. Compute C_{11}, C_{12} and C_{13}.