T-79.159 Cryptography and Data Security
2005 / Homework 2
Tue 22.3 and Fri 1.4

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. 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 $Kf = Y_{in} = 128$

3. Consider an LFSR with the connection polynomial $f(x) = x^4 + x^3 + x^2 + x + 1$. What are the cycles (periods) of the sequences generated by this LFSR?

4. Consider a threshold generator (Lecture 4) with three LFSRs defined by the connection polynomials and initial states:

$$\begin{aligned} f_1(x) &= x^3 + x^2 + 1, \text{ initial state } \texttt{001} \\ f_2(x) &= x^4 + x^3 + 1, \text{ initial state } \texttt{0011} \\ f_3(x) &= x^5 + x^2 + 1, \text{ initial state } \texttt{00001} \end{aligned}$$

   Compute the 30 first bits of the output sequence of the threshold generator.

   (a) Is the output sequence balanced, that is, has it about equally many zeroes and ones?

   (b) Compare the bits of the output sequence and the corresponding bits of the sequence generated by the third LFSR. For how many bits they are equal?

5. Draw a picture describing the decryption operation of the CBC mode.