1. Exercise sheet
Hand in before Monday, 2005/11/07, 14:30 in b-it 1.22.

Exercise 1.1 (The finite field \( \mathbb{F}_{2^8} \)). (8+4 points)

In the course you learned about the finite field \( \mathbb{F}_{2^8} \) and that its elements are polynomials of degree less than 8 with coefficients in the two-element field \( \mathbb{F}_2 \). Each element is of course given by eight bits, which we can also read as a hexadecimally written byte, so that, for example, 91 corresponds to \( x^7 + x^4 + 1 \).

Addition and multiplication are executed ‘as usual’ but the result is reduced modulo the polynomial \( x^8 + x^4 + x^3 + x + 1 \). Calculate in this field:

(i) Add \( x^5 + x + 1 \) and \( x^7 + x^6 + 1 \).  
(ii) Add 23 and C1.  
(iii) Multiply \( x^5 + x + 1 \) and \( x^7 + x^6 + 1 \).  
(iv) Multiply 23 and C1.  
(v) Calculate the inverse of \( x^5 + x + 1 \).  
(vi) Calculate the inverse of 23.  
(vii*) Describe an algorithm to calculate the inverse of a non-zero element. +4

Exercise 1.2 (The finite ring \( \mathbb{F}_{2^8}[y]/\langle y^4 + 1 \rangle \)). (10 points)

Calculate in the finite ring \( S = \mathbb{F}_{2^8}[y]/\langle y^4 + 1 \rangle \):

(i) Multiply \( c = 02 + 01y + 01y^2 + 03y^3 \) by \( d = 0E + 09y + 0Dy^2 + 0By^3 \).  
(ii) Multiply the column of values 00, 7A, 01, 00 with the polynomial \( c \) and write it again as a column.  
(iii) Try to compute an inverse for \( 01 + 01y^2 \).  
(iv) Try to compute an inverse for \( 11 + 01y^2 \).
Exercise 1.3 (S-box). (2+3 points)

Compute the output of the operation $\text{SubByte}$ (the S-box) and of the polynomial function

$$a \mapsto 05 \cdot a^{254} + 09 \cdot a^{253} + F9 \cdot a^{251} + 25 \cdot a^{247} + F4 \cdot a^{239} + 01 \cdot a^{223} + B5 \cdot a^{191} + 8F \cdot a^{127} + 63$$

(i) at 00,
(ii) at 01, and
(iii) at one further point.

In fact, the two values are always the same. You shall just verify that this is true by a few examples.

You are allowed to use a self-written program for this exercise. In that case, please hand in a printout of your source.

We recommend to use MuPAD; it is available on the b-it computers and can also be downloaded at \url{http://www.mupad.de/}. You can find a MuPAD notebook on our webpage that implements the finite field $\mathbb{F}_{2^8}$ and the ring $\mathbb{F}_2[x]/(x^8 + 1)$ including the translations from and to ‘bytes’.