Cryptography I, winter 2005/06

Joachim von zur Gathen, Michael Nüsken

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, $\mathtt{91}$ 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 $x^7 + x^6 + 1$. $\boxed{1}$

(ii) Add $\mathtt{23}$ and $\mathtt{C1}$. $\boxed{1}$

(iii) Multiply $x^5 + x + 1$ and $x^7 + x^6 + 1$. $\boxed{1}$

(iv) Multiply $\mathtt{23}$ and $\mathtt{C1}$. $\boxed{1}$

(v) Calculate the inverse of $x^5 + x + 1$. $\boxed{2}$

(vi) Calculate the inverse of $\mathtt{23}$. $\boxed{2}$

(vii*) Describe an algorithm to calculate the inverse of a non-zero element. $\boxed{+4}$

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 $c = \mathtt{02} + \mathtt{01}y + \mathtt{01}y^2 + \mathtt{03}y^3$ by $d = \mathtt{0E} + \mathtt{09}y + \mathtt{0D}y^2 + \mathtt{0B}y^3$. $\boxed{4}$

(ii) Multiply the column of values $\mathtt{00}$, $\mathtt{7A}$, $\mathtt{01}$, $\mathtt{00}$ with the polynomial c and write it again as a column. $\boxed{2}$

(iii) Try to compute an inverse for $\mathtt{01} + \mathtt{01}y^2$. $\boxed{2}$

(iv) Try to compute an inverse for $\mathtt{11} + \mathtt{01}y^2$. $\boxed{2}$

Exercise 1.3 (S-box). (2+3 points)

Compute the output of the operation `SubByte` (the S-box) and of the polynomial function

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

$\boxed{1}$ (i) at `00`,

$\boxed{1}$ (ii) at `01`, and

$\boxed{+3}$ (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 `http://www.mupad.de/`. You can find a MuPAD note book on our webpage that implements the finite field $\mathbb{F}_{2^8}$ and the ring $\mathbb{F}_2[x]/\langle x^8+1\rangle$ including the translations from and to 'bytes'.