7. Exercise sheet
Hand in solutions until
Wednesday, 17 December 2014, 23:59:59

Exercise 7.1 (The finite field $\mathbb{F}_{256}$).

The finite field of 256 elements plays a central role in cryptography. 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 hexadically written byte, so that, for example, $x^7 + x^4 + 1$ is given by $(10010001)_2$, which can be read as 0x91. Addition and multiplication in the field are the usual addition and multiplication of polynomials, apart from the rule that the result is reduced modulo the polynomial $x^8 + x^4 + x^3 + x + 1$. Carry out the following computations:

(i) Add $x^5 + x + 1$ and $x^7 + x^6 + 1$.

(ii) Multiply 0x23 and 0xC1.

(iii) Calculate the inverse of 0x23.

Exercise 7.2 (AES).

(i) The ring $S = \mathbb{F}_{256}[y]/ \langle y^4 + 1 \rangle$ is not a field. In particular, there are nonzero elements in $S$ without a multiplicative inverse. Give an example and explain how you could check that property.

(ii) The output $b_3, b_2, b_1$ and $b_0$ of the MixColumns-step for a column with entries $a_3, a_2, a_1$ and $a_0$ is determined by the product

$$b_3y^3 + b_2y^2 + b_1y + b_0 = (02 + 01y + 01y^2 + 03y^3) \cdot (a_3y^3 + a_2y^2 + a_1y + a_0).$$

Expand the product over $\mathbb{F}_{256}[y]$, reduce it modulo $y^4 + 1$ and collect the terms with equal powers of $y$ to obtain equations for $b_3, b_2, b_1$ and $b_0$. Find a $4 \times 4$-matrix $M$ with entries from $\mathbb{F}_{256}$ to express this multiplication as a matrix-vector product

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = M \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}.$$
(iii) Verify that the product of the polynomial $d = 0By^3 + 0Dy^2 + 09y + 0E$ and the polynomial $c = 03y^3 + 01y^2 + 01y + 02$ is equal to 1 in the ring $S$.

(iv) Find the inverse of $02 + 01y + 01y^2 + 03y^3$ in $S$.

(v) Given the output of the function SubBytes, how can you find the corresponding input?

(vi) Formulate the AES decryption algorithm.