Cryptography, winter 2014/2015

PRIV.-DOZ. DR. ADRIAN SPALKA, DR. DANIEL LOEBENBERGER

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

Exercise 7.1 (The finite field $\mathbb{F}_{256}$). (4 points)

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 hexadecimally 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 $x^7 + x^6 + 1$. [1]

(ii) Multiply `0x23` and `0xC1`. [1]

(iii) Calculate the inverse of `0x23`. [2]

Exercise 7.2 (AES). (19 points)

(i) The ring $S = \mathbb{F}_{256}[y]/\left\langle y^4 + 1\right\rangle$ 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. [3]

(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 [4]

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

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 4×4-matrix $\mathcal{M}$ with entries from $\mathbb{F}_{256}$ to express this multiplication as a matrix-vector product

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = \mathcal{M} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}.$$

2 (iii) Verify that the product of the polynomial $d = \texttt{0B}y^3 + \texttt{0D}y^2 + \texttt{09}y + \texttt{0E}$ and the polynomial $c = \texttt{03}y^3 + \texttt{01}y^2 + \texttt{01}y + \texttt{02}$ is equal to $\texttt{1}$ in the ring S.

4 (iv) Find the inverse of $\texttt{02} + \texttt{01}y + \texttt{01}y^2 + \texttt{03}y^3$ in S.

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

4 (vi) Formulate the AES decryption algorithm.