Cryptography

PROF. DR. JOACHIM VON ZUR GATHEM, KONSTANTIN ZIEGLER

1. Assignment: Arithmetic in $\mathbb{F}_{256}$
(Due: Tuesday, 4 November 2008, 14:40, b-it Rheinsaal)

Exercise 1.1 (The finite field $\mathbb{F}_{256}$). (8 points)

The finite field of 256 elements plays a central role in the description of AES. 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 hexademically written byte, so that, for example, $x^7 + x^4 + 1$ is given by $(10010001)$, which can be read as 91. 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 and document your intermediate steps:

(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 $x^4 + x^3 + x^2 + x + 1$.

(vi) Calculate the inverse of 23.

Exercise 1.2 (The finite ring $\mathbb{F}_{256}[y]/\langle y^4 + 1 \rangle$). (10 points)

The finite ring $\mathbb{F}_{256}[y]/\langle y^4 + 1 \rangle$ consists of polynomials of degree less than 4 in the variable $y$ with coefficients in the field $\mathbb{F}_{256}$.

(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 by 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 (SubBytes and MixColumns).**

(i) Compute the inverse of $z^4 + z^3 + z^2 + z + 1 \in \mathbb{F}_2[z]/\langle z^8 + 1 \rangle$ and compare with your result in exercise 1.1 (v).

(ii) Given the output of the operation SubBytes (S-Box), how can you find the corresponding input? Describe the necessary steps in full detail.

(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 $\mathbb{F}_{256}[y]/\langle y^4 + 1 \rangle$. 