Cryptography, winter 2006

PROF. DR. WERNER SCHINDLER, DIPL.-INF. DANIEL LOEBENBERGER

6. Exercise sheet (20.12.2006)
Hand in solutions to the homework exercises on Wednesday, January 17th, in the tutorial/the lecture.

The design of AES uses different rings. The construction starts with the field $\mathbb{F}_2$. Building on that the field $\mathbb{F}_{256} = \mathbb{F}_2[x]/\left\langle x^8 + x^4 + x^3 + x + 1 \right\rangle$ is defined, its elements requiring 8 bits a.k.a. 1 byte. E.g. 23 in decimal, `17` in hexadecimal representation, corresponds to $\overline{x}^4 + \overline{x}^2 + \overline{x} + \overline{1}$. We will omit the bar which we used to illustrate that we are working with remainders (in this case modulo $x^8 + x^4 + x^3 + x + 1$). At some other point in the standard bytes are interpreted as elements of the ring $R = \mathbb{F}_2[z]/\left\langle z^8 + 1 \right\rangle$. Finally, there is also the ring $S = \mathbb{F}_{256}[y]/\left\langle y^4 + 1 \right\rangle$. Let us compute a little with elements of these rings...

Exercise 6.1 (Modular arithmetic).

We want to show that the rings R and S are not fields.

(i) *Show:* $(\overline{z} + \overline{1})^8 = 0$ *in* R.

(ii) *Name a zero divisor in* R.

(iii) *Show that* $\overline{z} + \overline{1}$ *does not have an inverse in* R.

(iv) *Show:* $(\overline{y} + \overline{1})^4 = 0$ *in* S.

(v) *Name a zero divisor in* S.

(vi) *Show that* $\overline{y} + \overline{1}$ *does not have an inverse in* S.

Note*: A zero divisor is an element* a *of a ring that is not zero and for which there is an element* $b \neq 0$ *so that* $ab = 0$.

Exercise 6.2 (Correlation). *The security of a block cipher like AES depends crucially on a sufficient amount of nonlinearity. The following notion is an important measure of nonlinearity.*

Given two functions $f, \ell \colon \mathbb{F}_{256} \to \mathbb{F}_2$ *we define their* correlation

$$\operatorname{corr}(f, \ell) = \sum_{a \in \mathbb{F}_{256}} (-1)^{f(a) + \ell(a)},$$

Thus we add 1 *for every element where* f *and* ℓ *coincide and we subtract* 1 *for every element where they differ. The higher the value, the more* f *and* g *coincide. In fact* $1/256 \operatorname{corr}(f, \ell) = 2 \operatorname{prob}(f(X) = \ell(X)) - 1$*, if* X *is uniformly* *distributed in $\mathbb{F}_{256}$; the correlation of f and ℓ is thus a direct measure for the probability that f and ℓ coincide on a random input.*

A field element $a \in \mathbb{F}_{256}$ can be represented in the form $a = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \pmod{x^8 + x^4 + x^3 + x + 1} \in \mathbb{F}_{256}$.

(i) *A function $\ell\colon \mathbb{F}_{256} \to \mathbb{F}_2$ is* linear *if $\ell(a+b) = \ell(a)+\ell(b)$ for all $a, b \in \mathbb{F}_{256}$. Show that a linear function ℓ is always of the form $\ell(a) = \sum_i \ell_i a_i \in \mathbb{F}_2$ with suitable $\ell_i \in \mathbb{F}_2$.*

(ii) *Compute all possible values of $\mathrm{corr}(f, \ell)$, if f and ℓ are linear.* Hint: *Without loss of generatility you can assume that f is the zero function.*

(iii) *Use* MAPLE *to compute the correlations $\mathrm{corr}(\ell_i \circ f_j, \ell_k)$ of the following functions. Compute a little matrix for each of the f_j.*

- $f_{-1}(a) := a^{-1}$ *for $a \neq 0$ and $f_{-1}(0) = 0$,*
- $f_1(a) := a$,
- $f_2(a) := a^2$,
- $f_3(a) := a^3$,
- $f_*(a) := (a_7 + a_6)x^7 + (a_3 + a_5)x^6 + (a_6 + a_5)x^5 + (a_2 + a_7 + a_4)x^4 + (a_5 + a_7 + a_4 + a_6)x^3 + (a_1 + a_5)x^2 + (a_7 + a_4 + a_6)x + a_6 + a_0 + a_4$.

- $\ell_0(a) := a_0$,
- $\ell_1(a) := a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7$,
- $\ell_2(a) := a_0 + a_4 + a_7$,
- $\ell_3(a) := a_5 + a_7 + 1$,
- $\ell_4(a) := a_5 + a_7$.

Hint: *On our web page you will find a* MAPLE *Worksheet containing the definitions of these functions and some helpful information.*

(iv) *Draw conclusions from the results.*

Exercise 6.3 (Homework: Computing in $\mathbb{F}_{256}$). (8 points)

Let M be your student registration number. Let

$$a = M \bmod 256,\ b = (M \operatorname{div} 256) \bmod 256, \text{ and } c = (a+b) \bmod 256$$

Now interpret a, b and c as elementes of $\mathbb{F}_{256}$, just as in AES. Compute in $\mathbb{F}_{256}$

(i) $a + b$ (Attention! Usually the result will not be c!), $\boxed{2}$

Solution. My student registration number is $M = 1111111$. We have $a = 71$, $b = 244$ and $c = 59$. Interpreted as elements of $\mathbb{F}_{256}$ we have:

$$\begin{aligned} a &= 71_{(10)} = 1000111_{(2)} = x^6 + x^2 + x + 1 \\ b &= 244_{(10)} = 11110100_{(2)} = x^7 + x^6 + x^5 + x^4 + x^2 \end{aligned}$$

Thus we have in $\mathbb{F}_{256}$: $a + b = x^7 + x^5 + x^4 + x + 1 = 10110011_{(2)} = 179_{(10)} \neq c$.

(ii) $a \cdot b$ and $\boxed{2}$

Solution. We have $a \cdot b = x^7 + x^5 + x^4 + x + 1 = 10110011_{(2)} = 179_{(10)}$.

(iii) $1/a$ (or $1/b$ in case $a = 0$). $\boxed{4}$

Solution. We have $1/a = x^6 + x^5 + x^3 + 1$. This was computed using the extended euklidean algorithm.

Note: If $x = x_1 \cdot 256 + x_0$ with $0 \le x_0 < 256$, then $x \operatorname{div} 256 = x_1$ and $x \bmod 256 = x_0$.

Exercise 6.4 (Homework: Encryption and decryption with AES). (12 points)

(i) Given the output of the function ByteSub, how can you find the corresponding input? $\boxed{2}$

Solution. In practice the whole S-Box is stored in a table. So a simple array lookup suffices.

(ii) Compute the inverse of $t_1 = x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_{256}$. $\boxed{2}$

Solution. We have in $\mathbb{F}_{256}$: $1/t_1 = x^7 + x^5 + x^4 + x$.

(iii) Compute the inverse of $t_2 = z^4 + z^3 + z^2 + z + 1 \in \mathbb{F}_2[z]/\langle z^8 + 1 \rangle$. $\boxed{2}$

Solution. We have in $\mathbb{F}_2[z]/\langle z^8+1\rangle$: $1/t_2 = z^6+z^3+z$. ◯

(iv) 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 $\mathbb{F}_{256}[y]/\langle y^4+1\rangle$. $\boxed{6}$

Solution. Staightforward but lengthy calculation. ◯