# Security on the Internet, summer 2007

MICHAEL NÜSKEN

## 4. Exercise sheet
## Hand in solutions until Thursday, 3 Mai 2007.

Any claim needs a proof or an argument.

**Exercise 4.1** (Polynomials over $\mathbb{F}_2$). (10+4 points)

Let's consider polynomials with coefficients in the field $\mathbb{F}_2$. (Remember that $\mathbb{F}_2 = \mathbb{Z}_2$ since $2$ is prime.)

(i) Take your student id, and write $1234567 + \text{studentid} = \sum_{0 \le k < 24} s_k 2^k$ with $s_k \in \{0, 1\} \subset \mathbb{Z}$. Now interpret $s_k \in \mathbb{F}_2$ and write down the polynomials $\boxed{2}$

$$
\begin{aligned}
a &= \sum_{0 \le k < 8} s_k X^k \in \mathbb{F}_2[X], \\
b &= \sum_{0 \le k < 8} s_{k+8} X^k \in \mathbb{F}_2[X], \\
c &= \sum_{0 \le k < 8} s_{k+16} X^k \in \mathbb{F}_2[X], \\
d &= a + bX^8 = \sum_{0 \le k < 16} s_k X^k \in \mathbb{F}_2[X].
\end{aligned}
$$

If $a = 0$, $b = 0$, or $\deg c < 3$ then add $2345678$ to your real student id.

(ii) Compute $a + b$. $\boxed{1}$

(iii) Compute $a \cdot b$. $\boxed{1}$

(iv) Compute the remainder of the division of $d$ by $c$. $\boxed{3}$

Some polynomials are a proper product of others. Some are not.

(v) Prove that $X^2 + X + 1$ cannot be written as a proper product. We call such a polynomial *irreducible*. $\boxed{1}$

(vi) Write $X^8 + 1$ as a product of irreducible polynomials (that cannot be written as a product). [For verification only: the factors' degrees are all $1$.] $\boxed{2}$

(vii) Write $X^9 + 1$ as a product of irreducible polynomials. [For verification only: the factors' degrees are $1$, $2$, and $6$.] $\boxed{+4}$

**Exercise 4.2** (Touching $\mathbb{F}_4$). (4+4 points)

Consider polynomials of degree less than $2$ over the field $\mathbb{F}_2$. Define addition and multiplication of them modulo the polynomial $X^2 + X + 1$.

$\boxed{1}$ (i) Write down the complete list of elements.

$\boxed{1}$ (ii) Write down the addition table.

$\boxed{2}$ (iii) Write down the multiplication table.

We can now consider polynomials over $\mathbb{F}_4$: $T^2 + T + 1$ is such a polynomial.
$\boxed{+4}$ Factor it (over $\mathbb{F}_4$).

**Exercise 4.3** (Computing inverses). (6 points)

If possible compute the inverse

$\boxed{2}$ (i) …of $89$ in the ring $\mathbb{Z}_{101}$,

$\boxed{2}$ (ii) …of $42$ in the ring $\mathbb{Z}_{1001}$,

$\boxed{2}$ (iii) …of $1817$ in the ring $\mathbb{Z}_{10001}$.

Give a proof if no inverse exists.

**Exercise 4.4** (Computing in $\mathbb{F}_{256}$). (8 points)

Let $M$ be your student id. 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 $\mathbb{F}_{256}$

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

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

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

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