# Security on the Internet, winter 2008

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

## 6. Exercise sheet
## Hand in solutions until
## Monday, 08 December 2008, $11^{59}$am (deadline!).

As usual: Any claim needs a proof or an argument.

**Exercise 6.1** (Remainders). (5+1 points)

Consider rings $\mathbb{Z}_{mn}$ with the following pairs $(m, n)$. In each case make a table with $\mathbb{Z}_m$ on one axis and $\mathbb{Z}_n$ on the other, then write each number $a \in \mathbb{Z}_{mn}$ at position $(a \bmod m, a \bmod n)$ as in this example:

| $\mathbb{Z}_2 \backslash \mathbb{Z}_3$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 4 | 2 |
| 1 | 3 | 1 | 5 |

(i) $(m, n) = (2, 4)$,

(ii) $(m, n) = (3, 5)$,

(iii) $(m, n) = (4, 6)$,

(iv) $(m, n) = (3, 8)$.

(v) In which of the previous cases do the numbers fill the entire table? When do they not collide? $\boxed{1}$

(vi) Give a simple criterion on $(m, n)$ to tell when the numbers fill the table. $\boxed{+1}$

**Exercise 6.2** (Chinese remaindering and Pohlig-Hellman). (4 points)

The goal of this exercise is to understand the algorithm of Pohlig-Hellman. The numbers are deliberately small and the use of MuPAD or any other computer algebra system for this exercise is discouraged.

(i) Let $G = \mathbb{Z}_p^\times$ with $p = 2 \cdot 3 \cdot 5 \cdot 7 + 1$, $g = 2$, $y = 10$. Compute the discrete logarithm of $y$ in base $g$ using the Chinese remainder theorem. $\boxed{2}$

(ii) Let $G = \mathbb{Z}_p^\times$ with $p = 2^4 + 1$, $g = 3$, $y = 7$. Compute the discrete logarithm of $y$ in base $g$ using the idea by Pohlig-Hellman. $\boxed{2}$