The electronic health card, summer 2008

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

1. Exercise sheet
Hand in solutions until Tuesday, 15 April 2008.

For future exercises it might be important to use b-it computers. So please register an account for the b-it. (Ask at the infodesk for the procedure.)

A word on the exercises. They are important. Of course, you know that. Just as an additional motivation, you will get a bonus for the final exam if you earn more than 60% or even more than 80% of the credits.

Exercise 1.1 (Secure email). (6 points)

(i) Send a digitally signed email with the subject "`[08ss-ehc] hello`" to us at `08ss-ehc@bit.uni-bonn.de` from your personal account. The signature must be verifiable and correct. [It is a good idea to verify this by sending a blind carbon copy (Bcc) to oneself.] [4]

With Thunderbird I recommend using `enigmail` and `gpg`. In any case make sure to register your key eg. at `http://wwwkeys.de.pgp.net/`.

Choose yourself among this and possible other solutions. In any case use a pgp key pair.

Note: Future exercise hand-ins will only be accepted via signed email. Then a bonus point will be awarded for a correct signature and a malus for a missing or invalid signature.

(ii) Send a second email with the subject "`[08ss-ehc] student id`" containing your student identification number. (How should that be secured?) You have only one trial here! [If you need testing then test with yourself or with a friend.] [2]

Deadline for earning these credits: Monday, 14 April 2008, 23:59:59 (valid timestamp of your emails).

Exercise 1.2 (Trust). (4 points)

2 (i) Find the fingerprint of your own PGP key. Bring 10 printouts of it to the next tutorial. (Do not send me an email with it. Guess, why!)

2 (ii) Sign all your collegues' public keys and our two keys: The corresponding fingerprints of our PGP keys are

```
F753 FA1F 70C8 0B4A 0181 8B50 B6EF 9CA3 B967 0465
```

and

```
FC11 51FB 995E 58A0 186B B701 306A DAFE 965F 1E54
```

Find our keys in your key management tool, after verification give it some or full trust, sign and submit your decision to the key server. (Make sure that things *are* visible on the server! Join with your fellow students to synchronize you.)

The deadline for this part is Monday, 21 April.

Exercise 1.3 (Magic). (4 points)

4 Verify, using the square-and-multiply algorithm that we have the following equations:

$$3^{2^{160}} = 3^{76} \text{ in } \mathbb{Z}_{101}$$

and

$$3^{3^{160}} = 3 \text{ in } \mathbb{Z}_{101}$$

You may use any programming language of your choice to check that. Hand in the source code.

Exercise 1.4 (Tool: Groups). (0+7 points)

In this exercise you will get comfortable with the concept of a group. Always remember: Don't PANIC. Which of the following sets, together with the given operation form a group? Check for each property (Proper, Associative, Neutral, Inverse, Commutative) if it is well-defined, and if so if it is fulfilled or not:

(i) $(\mathbb{Z}, -)$: The integers $\mathbb{Z}$ with subtraction. +1

(ii) $(\mathbb{N} \setminus \{0\}, \hat{})$: The positive integers $\mathbb{N} \setminus \{0\}$ with exponentiation. +1

(iii) $(\mathbb{B}, \vee)$: The set $\mathbb{B} := \{\top, \bot\}$ with operation $\vee$ (the logical OR), defined as: +1

$\vee$	$\top$	$\bot$
$\top$	$\top$	$\top$
$\bot$	$\top$	$\bot$

(iv) $(\mathbb{B}, \oplus)$: The set $\mathbb{B}$ with operation $\oplus$ (the logical XOR), defined as: +1

$\oplus$	$\top$	$\bot$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\bot$

(v) $(4\mathbb{Z}+1, \cdot)$: The set $4\mathbb{Z}+1 := \{z \in \mathbb{Z} \mid z = 1 \text{ in } \mathbb{Z}_4\}$ with multiplication. +1

(vi) $(\{\mathbb{Z}_7 \to \mathbb{Z}_7\}, \circ)$: The set $\{\mathbb{Z}_7 \to \mathbb{Z}_7\} := \{f : \mathbb{Z}_7 \to \mathbb{Z}_7\}$ with concatenation $\circ$ of functions. An example: If $g_1, g_2 : \mathbb{Z}_7 \to \mathbb{Z}_7$ are two functions then $(g_1 \circ g_2)(x) := g_1(g_2(x))$ for all $x \in \mathbb{Z}_7$.

(vii) $(\mathcal{S}(\mathbb{Z}_{13}), \circ)$: The set $\mathcal{S}(\mathbb{Z}_{13}) := \{f : \mathbb{Z}_{13} \to \mathbb{Z}_{13} \mid f \text{ bijective}\}$ with concatenation $\circ$. +1

(viii) $(\mathbb{Z}_3^2, \square)$: The set $\mathbb{Z}_3^2 := \{(a, b) \mid a \in \mathbb{Z}_3, b \in \mathbb{Z}_3\}$ with the following operation $\square$: +1

$$\square: \begin{array}{rcl} \mathbb{Z}_3^2 \times \mathbb{Z}_3^2 & \longrightarrow & \mathbb{Z}_3^2, \\ (a,b),(c,d) & \longmapsto & (ac+bd, ad+bc) \end{array}$$