Cryptographic passports & biometrics, summer 2009

MICHAEL NÜSKEN, KONSTANTIN ZIEGLER

1. Exercise sheet
Hand in solutions until Monday, 20 April 2009.

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. The bonus does not help passing the exam, but if you pass the bonus will increase your mark by up to two thirds.

Exercise 1.1 (Secure email). (6 points)

(i) Send a digitally signed email with the subject "`[09ss-cpb-handin] hello`" (without the quotation marks) to us at [4]

`09ss-cpb-handin@lists.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.]

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.

(ii) Find the fingerprint of your own PGP key. Bring two printouts of it to the next tutorial. (Do not send us an email with it. Guess, why!) [2]

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.

Exercise 1.2 (Electronic passports around the world). (6 points)

Pick an interesting country, as follows. If you are born outside europe and north-america, take the country you were born in. Otherwise choose a country outside europe and north-america.

[1] (i) Find out whether the chosen country issues passport with an electronic chip and/or with biometrics.

[1] (ii) Does the country participate in the U.S. visa waiver program?

[1] (iii) Does the passport specification follow the ICAO guidelines?

[1] (iv) When was or will it be introduced?

[1] (v) How is the identification number composed? (Is it a random number? Or is there a part for the town and a serial and…?) How many possible numbers are there? How many if you know the town? …the issuing date?

[1] (vi) Apart from a digital face image and data that is also written in the passport, is there further information stored electronically? (Eg. one or more fingerprints…)

Exercise 1.3 (Tool: The Extended Euclidean Algorithm). (4 points)

Integers: We can add, subtract and multiply them. And there is a division with remainder: Given any $a, b \in \mathbb{Z}$ with $b \neq 0$ there is a quotient $q \in \mathbb{Z}$ and a remainder $r \in \mathbb{Z}$ such that $a = q \cdot b + r$ and $0 \leq r < |b|$. (We write $a \operatorname{quo} b := q$, $a \operatorname{rem} b := r \in \mathbb{Z}$. If we want to calculate with the remainder in its natural domain we write $a \bmod b := r \in \mathbb{Z}_b$.) Using that we give an answer to the problem to find $s, t \in \mathbb{Z}$ with $sa + tb = 1$. Allowed answers are: "There is no solution." or "A solution is $s = ...$ and $t = ...$" Any answer needs a proof.

[2] (i) Find $s, t \in \mathbb{Z}$ such that $s \cdot 17 + t \cdot 21 = 1$.

[2] (ii) Find $s, t \in \mathbb{Z}$ such that $s \cdot 15 + t \cdot 21 = 1$.

PS: Guessing or trying all possibilities is not allowed here!