Security on the Internet, summer 2006

MICHAEL NÜSKEN

1. Exercise sheet
Hand in solutions to Exercise 1.2
on Tuesday, 25th of April, 14:00 in 1.22 (or nearby).

Exercise 1.1 (Secure email). (4 points)

Send a verifiable digitally signed email to me at `nuesken@bit.uni-bonn.de` from your personal account. [4]

- I recommend using `enigmail` and `gpg`, in that case make sure to register your key eg. at `http://wwwkeys.de.pgp.net/`.
- Or you can get an email certificate at some trustcenter, eg. `http://www.thawte.com/`.

Choose yourself among these and possible other solutions.

Deadline for earning the credits: Monday, 24th April 2006, 23:59 (valid time of your mail).

Exercise 1.2 (PKCS #7). (6 points)

(i) Get a (printed) copy of the standard PKCS #7 and read it briefly. [2]

Examine the standard with respect to protection from modification:

(ii) What does it require about the signature algorithm? [2]

(iii) Does it make a statement about the used (pseudo) random number generator? [2]