1. Exercise sheet

Hand in solutions until Thursday, 12 April 2007.

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 “[07ss-soti] hello” to me at nuesken@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.

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 “[07ss-soti] 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.]

Deadline for earning these credits: Thursday, 12 April 2007, 23:59:59 (valid timestamp of your emails).
Exercise 1.2 (Trust).  

(i) Find the fingerprint of your own PGP key. Bring 20 printouts of it to the next tutorial. (Do not send me an email with it. Guess, why!) 

(ii) Sign all your colleagues’ public keys and mine: The fingerprint of my PGP key is 

E49D 218D B622 51E0 DE04 DF1E 7142 20BB A085 1EB4

Find my key 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 Thursday, 19 April.