
2. Encoded RSA: Exercise 12.4 in [KL].

3. Public-Key Infrastructures: Exercise 12.13 in [KL]

4. Secure E-mail in Practice: (This is a bonus exercise!) Send and receive PGP-encrypted e-mail. Start from http://www.gnupg.org/ (GnuPG, includes links to Windows/Mac OS), look at http://enigmail.mozdev.org/documentation/quickstart.php.html (Thunderbird), or use whatever software makes sense for you.
   (a) There are several files in http://homepages.cwi.nl/~schaffne/course/pgp-exercise/. What can you tell us about these files?
   (b) Send an e-mail, encrypted and signed by your personal key, to both Joachim and Christian. Ideally, your public key should be on the public keyservers; if you don’t want to upload it, please send it to us (in the same or a separate message.)