Security
Assignment 9, Monday, November 21, 2011

Handing in your answers: There are two options:

1. Put your solutions in Pim's post box (in the white cabinet, lower door, near the printer at the station-side-end of the corridor on the second floor of the Huygens building). Before handing in, make sure:
   - your names and student numbers are written on the document.
2. Send your solutions by e-mail to `pim@cs.ru.nl` with subject '*assignment 9*'. This e-mail should only contain a single PDF document as attachment. Before handing in, make sure:
   - your names and student numbers are included in the document (since it will be printed),
   - your names are part of the filename (example: PimVullers_FlavioGarcia-9.pdf), and
   - the file is a PDF document.

Deadline: Monday, November 28, 8:30 sharp!

Note: Do not forget to perform the modulo operations.

1. **(5 points)** Consider the RSA cryptosystem, see Wikipedia[1]. For each question, give intermediate steps to show how you got your results.
   (a) Bob has chosen primes $p = 5$ and $q = 11$, compute n and $\phi(n)$.
   (b) Take $e = 7$ and compute d such that $d * e = 1 \mod \phi(n)$. Now e and d are Bob's public and private keys.
   (c) Compute Bob's signature on $m = 16$.
   (d) Now Alice wants Bob to sign $m = 16$ **blindly**. Take random $r = 13$ and compute m', i.e., the message that Alice sends to Bob to sign.
   (e) Compute Bob's signature on m'.
   (f) Un-blind the signature from (e) and compare your results with (c).
2. **(5 points)** In this question we ask you to use PGP (Pretty Good Privacy) which allows you to send and receive encrypted and/or signed e-mails. To do this, you need to create your own PGP-identity which is basically your e-mail address and public key signed with your private key. For this purpose we recommend the combination of *Thunderbird*[2] with the extension *Enigmail*[3] which uses *GnuPG*[4]. The latter is an open-source implementation of the OpenPGP standard (RFC4880). You can also use other tools like *PGP Desktop Email*[5], but we only offer support for the *Thunderbird/Enigmail* combination.
   (a) Find out how PGP works by performing the following steps (additional information is available in the Enigmail Quick Start Guide[6]):
      i. Generate a PGP-identity, and submit it to the public key server `subkeys.pgp.net`. This can either be done by using the command line or by using the plugin functionality of *Enigmail*.

[1] `http://en.wikipedia.org/wiki/RSA`
[2] `http://www.getthunderbird.com/`
[3] `http://enigmail.mozdev.org/download/` or `https://addons.mozilla.org/thunderbird/addon/enigmail/`
[4] `http://www.gnupg.org/download/`
[5] `http://www.symantec.com/business/desktop-email`
[6] `http://enigmail.mozdev.org/documentation/quickstart.php.html`

ii. Sign the key of at least one other student, and convince at least one other student to sign your key *on the server*. Remember to upload the signed public key to the key server to make your signature public.

iii. Refresh the public key information from the key server to verify that the keys have been signed. Note that there might be some delay between your upload and actual publication.

(b) Now you have a PGP-identity you can use it to e-mail securely. A convenient way to do this is via the *Enigmail* plugin for *Thunderbird*.

Send an **encrypted** and (digitally) **signed** e-mail with the subject "assignment 9" to `pim@cs.ru.nl` using the public key of key ID `0x021E4C4B`. The message should contain: your **names**, your public **key ID** and, as a PDF attachment, your **answers to the first question** of this assignment.

(It is a good idea to first send this to another student, using her/his public key, and see whether it works. Otherwise we might not be able to grade your work!)