Security on the Internet, summer 2007

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

7. Exercise sheet
Hand in solutions until Thursday, 24 Mai 2007.

Any claim needs a proof or an argument.

Exercise 7.1 (Close the gap). (5 points)

In the first proof of the correctness of RSA we restricted to invertible elements in $\mathbb{Z}_{pq}$.

Fill the gap and proof $x^{ed} = x$ for $x = sp$ $(0 < s < q)$, for $x = tq$ $(0 < t < p)$, and for $x = 0$. [Do not use the Chinese Remainder Theorem here.] 5

Exercise 7.2 (Square roots of 1). (10 points)

(i) Determine all solutions of $x^2 = 1$ in the ring $\mathbb{Z}_{89 \cdot 97}$. [Recall that whenever p is prime then $+1$ and -1 are all solutions of this equation in $\mathbb{Z}_p$.] 4

In the ring $\mathbb{Z}_N$,

$$N = 736\,518\,644\,769\,481\,063\,127\,931\,153\,488\,032\,823\,524\,624\,691\,168\,931\,264\,550\,157,$$

somebody found the solution

$$x = 114\,929\,747\,478\,656\,946\,659\,840\,400\,558\,284\,171\,506\,013\,987\,113\,875\,892\,871\,679.$$

(ii) Verify that $x^2 - 1 = 0$ but $x - 1 \neq 0$ and $x + 1 \neq 0$ in $\mathbb{Z}_N$. 2

(iii) Use this information to factor N. 4

Exercise 7.3 (Cracking RSA). (9 points)

Write a program for the following:

(i) Generate random RSA keys with N about 200 Bits. Keep the private key (N, d) secret and tell only the public key. Do not throw away anything this time. [You may assume that MuPAD's `random(a..b)` yields a function(!) outputting *uniformly random* numbers in the interval $a..b$.] 2

(ii) Use only N and L to recover the primes. 3

(iii) Compute a second pair (e', d') and use the two pairs (and possibly N) to recover L. 4

Exercise 7.4 (RSA signatures). (15+2 points)

Compute a signature! And find out what it is...

[1] (i) Generate random RSA keys with N about 30 Bits. Keep the private key (N, d) secret and tell only the public key.

[2] (ii) You are given a document, say x is your student identification number. Compute $y \leftarrow x^d$ in $\mathbb{Z}_N$.

[2] (iii) Verify that $y = x^d$ without using the secret key. [So you may only use the public key here!]

[4] (iv) Give a defintion explaining when y is a signature of x.

[2] (v) Explain how a signature on xr^e can be used to get a signature on x.

[4] (vi) Use the previous to decide whether the scheme is good (secure) or not.

[+2] (vii) Explain why using the same RSA key for encryption and signing is a very bad idea in practice.