Electronic passport and biometrics, winter 2006

MICHAEL NÜSKEN

4. Exercise sheet
Hand in solutions until Tuesday, 28 November, $12^{\underline{15}}$.

Exercise 4.1 (Email with signature). (4 points)

Send a verifiable digitally signed email to me at `nuesken@bit.uni-bonn.de` from your personal account. I recommend using `enigmail` and `gpg`. Make sure to upload your key eg. at `http://wwwkeys.de.pgp.net/`. [2]

Print out the fingerprint of your key in several copies, and bring it to the next tutorial. (This part cannot be done electronically, of course.) [2]

This and any future electronically handed in solution must be signed. You'll win 1 point for each finally verifiably signed hand-in and you'll lose 1 point for each unsigned electronic hand-in. [± 1]

Exercise 4.2 (Security estimate). (6 points)

RSA is a public-key encryption scheme that can also be used for generating signatures. It is neccessary for its security that it is difficult to factor large numbers (which are a product of two primes). The best known factoring algorithms achieve the following (heuristic, expected) running times:

method	year	time for n-bit integers
trial division	$-\infty$	$\mathcal{O}^{\sim}(2^{n/2})$
Pollard's $p-1$ method	1974	$\mathcal{O}^{\sim}(2^{n/4})$
Pollard's ϱ method	1975	$\mathcal{O}^{\sim}(2^{n/4})$
Pollard's and Strassen's method	1976	$\mathcal{O}^{\sim}(2^{n/4})$
Morrison's and Brillhart's continued fractions	1975	$2^{\mathcal{O}(1)n^{1/2}\log_2^{1/2} n}$
Dixon's random squares	1981	$2^{(\sqrt{2}+o(1))n^{1/2}\log_2^{1/2} n}$
Lenstra's elliptic curves method	1987	$2^{(1+o(1))n^{1/2}\log_2^{1/2} n}$
quadratic sieve		$2^{(1+o(1))n^{1/2}\log_2^{1/2} n}$
general number field sieve	1990	$2^{((64/9)^{1/3}+o(1))n^{1/3}\log_2^{2/3} n}$

It is not correct to think of $o(1)$ as zero, but for the following rough estimates just do it. Factoring the 663-bit integer RSA-200 needed about 165 1GHz CPU years (ie. 165 years on a single 1GHz Opteron CPU) using the general number field sieve. Estimate the time that would be needed to factor an n-bit RSA number assuming the above estimates are accurate with $o(1) = 0$ (which is wrong in practice!)

[1] (i) for $n = 1024$ (standard RSA),

[1] (ii) for $n = 2048$ (as required for Document Signer CA),

[1] (iii) for $n = 3072$ (as required for Country Signing CA).

Repeat the estimate assuming that only Pollard's ϱ method is available

[1] (iv) for $n = 1024$,

[1] (v) for $n = 2048$,

[1] (vi) for $n = 3072$.

Remark: The statistics for discrete logarithm algorithms are somewhat similar as long as we consider groups $\mathbb{Z}_p^\times$. For elliptic curves (usually) only generic algorithms are available with running time $2^{n/2}$.

Exercise 4.3 (MRTD life cycle). (4+2 points)

Go to the BSI article "Common Criteria Protection Profile". (There's a link on the webpage.)

[4] (i) Summarize the life cycle of an electronic passport.

[+2] (ii) Translate all acronyms.