Esecurity: secure internet & e-passports, summer 2011

Michael Nüsken, Raoul Blankertz

3. Exercise sheet
Hand in solutions until Monday, 25 April 2011, 23:59

Exercise 3.1 (GnuPG). (6 points)

(i) Consider the model of trust in GnuPG. Describe how trust is transfered (ie. which keys are trusted?). Which parameters can be adjusted? $\boxed{4}$

(ii) Which cryptographic algorithms are implemented in GnuPG? $\boxed{2}$

Exercise 3.2 (X.509). (10 points)

Read RFC 5280 and answer the following questions:

(i) What classes of certificates are there? $\boxed{2}$

(ii) What is the basic syntax of X.509 v3 certificates? Describe the `Certificate Fields` in detail. Which signature algorithms are supported? $\boxed{2}$

(iii) What format has the `Serial Number`? What kind of knowledge do you gain from the `Serial Number`? $\boxed{2}$

(iv) What is a trust anchor? Can one use different trust anchors? $\boxed{2}$

(v) What conditions are satisfied by a prospective certification path in the path validation process? $\boxed{2}$

Exercise 3.3 (Security estimate). (8 points)

RSA is a public-key encryption scheme that can also be used for generating signatures. It is necessary 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, instead add a $\mathcal{O}(1)$ factor. Factoring the 768-bit integer RSA-768 needed about 1500 2.2 GHz CPU years (ie. 1500 years on a single 2.2 GHz AMD 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!)

$\boxed{1}$ (i) for $n = 1024$ (standard RSA),

$\boxed{1}$ (ii) for $n = 2048$ (as required for Document Signer CA),

$\boxed{1}$ (iii) for $n = 3072$ (as required for Country Signing CA).

$\boxed{2}$ (iv) Now assume that the attacker has 1000 times as many computers and 1000 times as much time as in the factoring record. Which n should I choose to be just safe from this attacker?

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

$\boxed{1}$ (v) for $n = 1024$,

1 (vi) for $n = 2048$,

1 (vii) 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 3.4 (Dixon's random squares). (0+4 points)

(i) Let $N = q_1 q_2 \cdots q_r$ be odd with pairwise distinct prime divisors q_i and $r \geq 2$. Show: The equation $x^2 - 1 = 0$ has exactly 2^r solutions in $\mathbb{Z}_N^\times$. +3

Hint: Use the Chinese remainder theorem.

Note: The claim is also true, if the q_i are pairwise distinct prime powers. To see this you have to know that also for prime powers q the equation $x^2 - 1 = 0$ has exactly 2 solutions in $\mathbb{Z}_q$.

(ii) If s, t are random elements of $\mathbb{Z}_N^\times$ satisfying $s^2 \equiv t^2 \bmod N$, then the probability for $s \not\equiv \pm t \bmod N$ is at least $1 - \frac{1}{2^{r-1}}$. +1