Esecurity: secure internet & evoting, summer 2010

MICHAEL NÜSKEN, KONSTANTIN ZIEGLER

2. Exercise sheet
Hand in solutions until Sunday, 02 May 2010, 23.59 h

Exercise 2.1 (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!)

(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). 1

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

(iv) for $n = 1024$, 1

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 2.2 (Powers and goals for attackers of signatures). (10 points)

6 (i) You have encountered several levels of security:

- Unbreakability,
- Universal Unforgeability,
- Existential Unforgeability (EUF);

along with different means for an attacker:

- Key-Only Attack,
- Non-adaptive Chosen Message Attack,
- Chosen Message Attack (CMA).

Pairing an adversarial goal with an attack model defines a security notion, e.g. EUF-CMA.

Consider the RSA signature scheme. Assume that FACTORING is hard and decide for each of the 9 security notions whether the scheme is

- secure,
- not secure
- or the answer is unknown.

What can you say, if you assume that FACTORING is easy? Use the connections between the security notions to simplify your argument.

4 (ii) Prove: If RSA-sig is secure, then the hash function is one-way.

Exercise 2.3 (Amplification – or: A little bit better than guessing is enough). (8+4 points)

Think of a boolean variable T and an algorithm $\mathcal{A}$ with output A and a probability slightly better than guessing to determine the value of T, i.e.

$$p = \text{prob}(A == T) > \frac{1}{2}. \tag{2.4}$$

Imagine a new algorithm $\mathcal{B}$ which calls $\mathcal{A}$ m-times and outputs B as the majority of the As – returning failure in the event of a draw.

(i) Prove that [4]

$$\text{prob}(B == T) > \sum_{m/2<i\leq m} \binom{m}{i} p^i (1-p)^{m-i} \tag{2.5}$$

and give a simple – but still useful – lower bound for the sum. (Hint: Chernoff)

(ii) How many repetitions m do you need for $p = 0.6, 0.7, 0.8$ in order to guarantee $\text{prob}(B == T) > 0.9$. [4]

(iii) Let $p = \frac{1}{2} + \frac{1}{n}$. Determine a number of repetitions such that [+4]

$$\text{prob}(B == T) > 1 - e^{-cn}$$

for some constant $c > 0$.