Martin Ziegler
Carsten Rösnick

Distributed on 2012-01-19
Solutions to be submitted by 2012-01-26 14h25

Complexity Theory

WS 2011/2012, Exercise Sheet #10

EXERCISE 26:

a) Install the *public-key* system `pgp` on your computer; free versions are available from `GNU` for LINUX, WINDOWS, and MACOS X. (Users of the mathematics department's computer pool may skip this task and employ the installed `gpg`...)

b) Make yourself familiar with the software from a); even if that might mean to RTFM.

c) Create a key pair. Ponder on where and how to store the private part. Distribute the public part: on your home page, on a *keyserver* like `http://wwwkeys.de.pgp.net`, or elsehow. Bring ten print-outs of your public key's *fingerprint* on 2012-01-27.

d) Send me your solutions to Exercises 27 and 28 electronically (scanned or pdf/latex), signed with your private key and encoded with my† public key.

EXERCISE 27:

a) Fix $n \in \mathbb{N}$. Verify that $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$ constitutes a commutative ring with respect to operations $x \oplus y := (x+y)$ rem n and $x \otimes y := (x \cdot y)$ rem n. Prove: $(x \text{ rem } n) + (y \text{ rem } n) = (x+y) \text{ rem } n$ and $(x \text{ rem } n) \cdot (y \text{ rem } n) = (x \cdot y) \text{ rem } n$ for all $x, y \in \mathbb{Z}$.

b) i) Each $x \in \mathbb{Z}_n$ coprime to n admits a multiplicative inverse $x^{-1} \in \mathbb{Z}_n$.
ii) If p is even a prime, every $x \in \mathbb{Z}_p$ has $x^p = x$ (so-called Fermat's little theorem).
iii) If p, q are coprime and $a, b \in \mathbb{Z}$ with $a \equiv b \bmod p$ and $a \equiv b \bmod q$, then $a \equiv b \bmod pq$.

Hint: To coprime $a, b \in \mathbb{Z}$, the extended Euclidean Algorithm yields $r, s \in \mathbb{Z}$ with $ra + sb = 1$. You may furthermore employ Lagrange's Theorem.

c) Let p, q be distinct primes, $n := p \cdot q$ and $\varphi := (p-1) \cdot (q-1)$. Furthermore let $1 \neq e \in \mathbb{Z}_\varphi$ be coprime to φ and $d := e^{-1}$ rem φ according to b). Conclude that the functions

$$E(\tilde{e}) : \mathbb{Z}_n \setminus \{0\} \ni x \mapsto x^e \text{ rem } n \in \mathbb{Z}_n \quad \text{and} \quad D(\tilde{d}) : \mathbb{Z}_n \setminus \{0\} \ni y \mapsto y^d \text{ rem } n \in \mathbb{Z}_n$$

are computable in polynomial time and satisfy $D\big(\tilde{d}, E(\tilde{e}, x)\big) = x$ as well as $E\big(\tilde{e}, D(\tilde{d}, y)\big) = y$, where $\tilde{e} := \langle e, n \rangle$ and $\tilde{d} := \langle d, n \rangle$.

d) The *public-key* system from c) is known as RSA after the initials of its inventors RIVEST, SHAMIR, and ADLEMAN. Here, $\tilde{e}$ works as public key and $\tilde{d}$ as private one. How can the operations sign and encrype from Exercise 26d) be realized?
Suppose integers can be factored in polynomial time: How would that compromise RSA?

†available, e.g., from `http://www.mathematik.tu-darmstadt.de/~ziegler/public.key`, fingerprint: `AF37 ECD4 AEBE 3D4E 76EB 4445 227F 4D27 4A4B E6FE`

EXERCISE 28:

a) For $\vec{x} \in \{0,1\}^n$ fixed and $\vec{y}$ a random binary string of length n, the probability that $\vec{x}$ and $\vec{y}$ differ at precisely j places is $\binom{n}{j} \cdot 2^{-n}$.

b) Let X be a 0/1 random experiment (i.e. a Bernoulli random variable) succeeding with (possibly very small) probabiliy $p > 0$. Prove: Among $\frac{20}{p}$ repetitions, at least one of the experiments will succeed with probability $\geq 1 - e^{-20}$, that is practically certain.

c) Let X again denote a Bernoulli random variable with success probability p. Calculate the probability that among n repetitions more than half of the trials succeed. Determine the expectation μ and variance σ^2 of the random variable $Y := \sum_{j=1}^{n} X_j$ describing tha number of successful trials.

d) Again let X denote a Bernoulli random variable with $p \geq 1/2 + \varepsilon$ and $n := 40/\varepsilon^2$. Prove that among n repetitions of X more than half the trials succeeds with almost certainty; and that in case $p \leq 1/2 - \varepsilon$ almost certainly less than half of the trials succeeds. Hint: Look up and apply the Chernoff Bound. How about Chebyshev's inequality?