Cryptography I, winter 2005/06

JOACHIM VON ZUR GATHEN, MICHAEL NÜSKEN

2. Exercise sheet
Hand in before Monday, 2005/11/14, 17^{58} in b-it 1.22.

Exercise 2.1 (AES decryption). (0+4 points)

Formulate the AES decryption algorithm. $\boxed{+4}$

Exercise 2.2 (RSA). (7+1 points)

Using the primes $p = 31$ and $q = 41$ an RSA system shall be set up. (In practice these primes are of course much too small!) We choose $e = 17$ and $N = p \cdot q$ as public key.

(i) Use the extended Euclidean algorithm to compute the corresponding secret key d such that $e \cdot d \equiv 1 \bmod \varphi(N)$. *Important:* Write down all steps in the extended Euclidean algorithm! $\boxed{3}$

(ii) Encrypt $x = 1\,190$. $\boxed{2}$

(iii) Decrypt $y = 1\,026$. $\boxed{2}$

If you use a computer algebra system, as for example MuPAD or MAPLE then hand in (a printout of) your program sources and outputs (including intermediate results of the extended Euclidean algorithm), and use the following values instead: $\boxed{+1}$

$$
\begin{aligned}
p &= & 2\,609\,899, \\
q &= & 3\,004\,217, \\
e &= & 54\,323\,425\,121, \\
x &= & 4\,364\,863\,612\,562, \\
y &= & 850\,080\,551\,629.
\end{aligned}
$$

Exercise 2.3 (Cost of the Euclidean algorithm). (3 points)

Suppose $r_0 > r_1$ are positive integers and $r_{i-1} = q_i r_i + r_{i+1}$ with $0 \leq r_{i+1} < r_i$ are the steps of the Euclidean algorithm, where i ranges from 1 to ℓ.

(i) Show that $r_{i+1} \leq \frac{1}{2} r_{i-1}$ for $i \in \{1, \ldots, \ell\}$. $\boxed{2}$

(ii) Use (i) to show that the Euclidean algorithm needs at most $2 \log_2(r_0)$ steps. $\boxed{1}$

Exercise 2.4 (Properties of the gcd). (4 points)

$\boxed{4}$ Suppose $a, b, d \in \mathbb{Z}$ are integers. Prove that the following are equivalent:

(i) There exist $s, t \in \mathbb{Z}$ such that $sa + tb = d$.

(ii) The integer d is a multiple of $\gcd(a, b)$.

Exercise 2.5 (RSA bad choice). (4 points)

Show why the 35-bit integer 23 360 947 609 is a particularly bad choice for $N = pq$. (Despite the fact that it is too small in practice.)

We claim that two prime numbers which are really close to each other are bad choices for the RSA system. To show this we use Fermat's factorization method based on the fact: Suppose $p > q$ are odd integers. Then:

$$N = pq \qquad \Longleftrightarrow \qquad N = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2 .$$

$\boxed{3}$ (i) Explain how you can use this fact to find prime factors of N. (Hint: let $s := \left\lceil \sqrt{N} \right\rceil$, and consider s, $s+1$, $s+2, \ldots$)

$\boxed{1}$ (ii) Do it for $N = 23\,360\,947\,609$.

Exercise 2.6 (First steps in MuPAD (or Maple)). (0+6 points)

Your first task is to bring MuPAD to the screen and simply play a little with it.

(i) Use the MuPAD online help, for example try F2 (in Maple Ctrl+F1) after marking some text, to get information on `!`, `float` (in Maple `evalf`), `nextprime`, `time`, `floor`.

$\boxed{+1}$ (ii) What are the first five digits of $1000!^3$?

$\boxed{+1}$ (iii) What are the digits 9995 through 9999 of the decimal expansion of π? [To make things clear: the digits 1 through 5 are 14159.]

$\boxed{+1}$ (iv) What is the smallest 1000-bit prime minus 2^{999}?

$\boxed{+1}$ (v) Compute the remainder of $2^{1\,234\,567}$ on division by 11. Can you compute this within less then, say, a tenth of a second?

$\boxed{+2}$ (vi) Set up a procedure to generate a random n-bit prime. (Use the help on `proc`.)