The Art of Cryptography: Integral Lattices, summer 2010

PROF. DR. JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER

## 11. Exercise sheet
## Hand in solutions until Sunday, 04 July 2010, 23:59h.

**Exercise 11.1** (The Coppersmith method). (22 points)

In the lecture we discussed the following algorithm for finding small polynomials with high-order roots:

**Algorithm.** Small polynomial with high-order roots.

Input: a monic linear polynomial $f \in \mathbb{Z}[t]$, positive integers $N$, $c$, and $k$, and real $\mu$ with $0 < \mu \leq 1$.

Output: $g \in \mathbb{Z}[t]$.

1. $\ell \longleftarrow \lceil k/\mu \rceil$.
2. $$h_i \longleftarrow \begin{cases} N^{k-i} f^i & \text{for } 0 \leq i \leq k, \\ x^{i-k} f^k & \text{for } k < i < \ell. \end{cases}$$
3. Form the $\ell \times \ell$ matrix $A$ whose rows are the coefficient vectors of $h_0(ct), \ldots, h_{\ell-1}(ct))$.
4. Apply the basis reduction algorithm to the rows of $A$, with output $B = UA$ and $U \in \mathrm{GL}_\ell(\mathbb{Z})$ unimodular. Let $(u_o, \ldots, u_{\ell-1}) \in \mathbb{Z}^\ell$ be the top row of $U$.
5. Return $g = \sum_{0 \leq i < \ell} u_i h_i$.

(i) Implement the algorithm in a programming language of your choice. Note that the basis reduction code in MuPAD supplied on the webpage is *extremely* slow when compared to the built in Maple-routine or the C++ library NTL. $\boxed{10}$

(ii) Play around with the parameters of the above algorithm. In particular perform the following experiments: Set $N = 2183$, $\mu = 1/2$, $f = x+u$, $c = 59-u$. Now compute for all $1 \leq k \leq 15$ the smallest $u$ for which your algorithm produces you a valid result. $\boxed{5}$

(iii) What do the results tell you in the context of the security of RSA primes? Explain detailed. $\boxed{7}$