RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Ilya Ozerov, Elena Kirshanova

Hausübungen zur Vorlesung

Kryptanalyse

SS 2014

Blatt 7 / **16** June 2014 16.15 p.m.

Lattices

Exercise 1:
Geometrical problems on lattices have been proven to be hard. However, there are several computational problems associated with lattices that can be efficiently solved. Provide algorithms for the following computational problems:

1. **Membership problem:** given a lattice basis $\mathbf{B} \in \mathbb{Z}^{n \times m}$ and a vector $\mathbf{v} \in \mathbb{Z}^n$, decide if $\mathbf{v} \in \mathcal{L}(\mathbf{B})$;
2. **Sub-lattice:** given two lattices $\mathcal{L}(\mathbf{B}_1)$ and $\mathcal{L}(\mathbf{B}_2)$, $\mathbf{B}_1, \mathbf{B}_2 \in \mathbb{Z}^{n \times m}$, decide if $\mathcal{L}(\mathbf{B}_2) \subset \mathcal{L}(\mathbf{B}_1)$.

Exercise 2:
For big enough $n \geq 3$, give an example of a full-rank n-dimensional lattice in which the successive minima do not form a basis of the lattice. *Hint:* Cesium Chloride.

Coppersmith's method

Exercise 3:
Find all small roots of the polynomial

$$f(x) = x^2 + 1515x + 138 \bmod 2309.$$

You can take $m = 3$. You can also use any computer algebra system you like. Estimate the bound X using the results of the Class Problem Nr.4. Provide the LLL-reduced matrix that you obtain for the initial basis together with the unitary transformation. In addition, provide the coefficients of the g-polynomial.

Exercise 4:
In the Coppersmith's method we obtain the bound on small solution $X = M^{\frac{1}{n}-\varepsilon}$ ($\varepsilon << 1$). Can you choose ε such that $X = \frac{M^{\frac{1}{n}}}{C}$ for some constant C? Then, change the Coppersmith's algorithm to achieve $X = M^{\frac{1}{n}}$.