The Art of Cryptography: Integral Lattices, summer 2010

PROF. DR. JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER

4. Exercise sheet
Hand in solutions until Sunday, 9 May 2010, 23:59h.

Note: From the following exercise on, we assume that you have a variant of the basis reduction algorithm running on your computer. Any experiments that you have to do in the sequel will need such a library. It is highly adviced that you use C++ in the future. If you are not feeling comfortable using this language, you will have use your own implementation or you will have to search on your own for an optimized basis reduction library for the language you have in mind.

Exercise 4.1 (NTL: A Library for doing Number Theory). (5 points)

NTL is a high-performance, portable C++ library providing data structures and algorithms for manipulating signed, arbitrary length integers, and for vectors, matrices, and polynomials over the integers and over finite fields. It has a highly optimized built in basis reduction algorithm that we will employ frequently for the rest of the lecture. To start, install NTL on your computer and get familar with the NTL-API. Hints how to install NTL and details on the API can be found on `http://www.shoup.net/ntl/doc/tour.html`. Now run the code `lll.cpp` from the course page. To compile it, call for example under UNIX (or Mac OS X) the compiler in the following way: `g++ -o lll lll.cpp -lntl -lm`. You might have to include the headers using the $-I$ flag and the library using the $-L$ flag. Details on that can be found in the `man` page of `g++`. Consider now the lattice spanned by the matrix (written in row notation) [5]

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}.$$

Hand in the output of the supplied program.

Exercise 4.2 (The knapsack cryptosystem). (6 points)

In the lecture we learned about the knapsack cryptosystem. Let $m = 437$ and $c = 204$. Bob's private key is $b = (2, 6, 10, 26, 68, 161)$.

(i) Compute Bob's public key a. [2]

Now Alice wants to send the string $x = (0, 1, 0, 1, 1, 0)$.

(ii) Encrypt x with Bob's public key obtaining y. [1]

(iii) Describe in detail how Bob will decrypt the encrypted message y and do the decryption. [3]

Exercise 4.3 (Breaking the knapsack cryptosystem). (20+7 points)

Goal of this exercise is to implement the knapsack cryptosystem and the algorithm breaking it.

10 (i) Implement the knapsack cryptosystem in a programming language of your choice and hand in the source code. You will need to implement three functions:

Algorithm. Generate Key Pair.
Input: A positive integer n.
Output: The private key (b, m, c) and the public key a. The private key consists of a superincreasing sequence $b = (b_1, \ldots, b_n)$ with $b_i \in \left(\sum_{j<i} b_j, 2\sum_{j<i} b_j\right)$, a value $m \in \left(\sum_{j\le n} b_j, 2\sum_{j\le n} b_j\right)$ and a value $c \in \mathbb{N}$ with $\gcd(c, m) = 1$. The public key is a sequence $a = (cb_1 \pmod m, \ldots, cb_n \pmod m)$.

Algorithm. Encrypt.
Input: A message $x \in \{0,1\}^n$. The public key a.
Output: The encrypted message $y = \sum_{i\le n} x_i a_i$.

Algorithm. Decrypt.
Input: A message $y \in \mathbb{N}$. The private key (b, m, c).
Output: The decrypted message x.

In the lecture we have seen the following algorithm that computes (sometimes) a solution to the knapsack problem:

Algorithm. Short vectors for subset sums.
Input: Positive integers $a_0, a_1, \ldots, a_n$.
Output: $(x_1, \ldots, x_n) \in \mathbb{Z}^{n+1}$ or "failure".

1. Let $M = \lceil 2^{(n-1)/2} n^{1/2} \rceil$.
2. If $a_0 < \sum_{1\le i\le n} a_i/2$ then $a_0 \longleftarrow \tilde{a}_0 = \sum_{1\le i\le n} a_i - a_0$ else $\tilde{a}_0 = 0$.
3. For $0 \le i \le n$, let $b_i \in \mathbb{Z}^{n+1}$ be as follows:

$$b_0 = (a_0 M, 0, \ldots, 0),$$
$$b_i = (-a_i M, 0, \ldots, 0, 1, 0, \ldots, 0) \text{ with 1 in position } i, \text{ for } 1 \le i \le n.$$

4. Let $L \subseteq \mathbb{Z}^{n+1}$ be the lattice generated by $b_0, \ldots, b_n$. Run the basis reduction on this basis and return a short nonzero vector $v = (v_0, \ldots, v_n) \in L$.
5. If $\tilde{a}_0 = a_0$ then For $0 \le i \le n$, let $v_i \longleftarrow 1 - v_i$
6. If $v \in \{0,1\}^{n+1}$ then return $(v_1, \ldots, v_n)$ else return "failure".

10 (ii) Implement the above algorithm in a programming language of your choice. Hand in the source code.

+2 (iii) Assume you have intercepted the message $y = 1147$. Bob's public key is

$$a = (465, 441, 417, 241, 330, 251).$$

Compute the message $x \in \{0,1\}^6$ that Alice sent to Bob using the above algorithm.

+5 (iv) For $n = 6$ and $\varepsilon = 1/10$, we can take $B = 36238786559$. Run 100 examples with $a_1, \ldots, a_6 \xleftarrow{\text{R}} \{1, \ldots, B\}$ and $x \xleftarrow{\text{R}} \{0,1\}^6 \setminus \{(0, \ldots, 0)\}$. How often did your algorithm not succeed in finding x?