The Art of Cryptography: Integral Lattices, summer 2010

PROF. DR. JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER

8. Exercise sheet
Hand in solutions until Sunday, 13 June 2010, 23:59h.

Exercise 8.1 (Key exchange). (13+5 points)

As a preliminary step for the Diffie-Hellman key exchange protocol, Alice and Bob have to agree on a cyclic group G and a generator g.

Protocol 8.2. Diffie-Hellman key exchange.

1. Alice chooses $a \in \mathbb{N}_{<\#G}$ and computes g^a. $\quad \xrightarrow{\quad g^a \quad}$
2. Bob chooses $b \in \mathbb{N}_{<\#G}$ and computes g^b. $\quad \xleftarrow{\quad g^b \quad}$
3. Alice computes $(g^b)^a = g^{ab}$.
4. Bob computes $(g^a)^b = g^{ab}$.

There are three central topics to be dealt with: correctness, efficiency, and security. The first one is evident from the definition of the protocol. The latter two depend on the choice of the group.

(i) First a note on the efficiency: For the protocol Alice needs to compute g^a. Sketch an efficient algorithm that computes g^a that runs with at most $2\log(a)$ group operations. [3]

(ii) Can you do better? Justify. [+5]

(iii) Name a group G and a generator g for which security may not be ensured. Hint: Extended Euclidean algorithm. [3]

(iv) Consider $G = \mathbb{Z}_p^\times$ with p and $\frac{1}{2}(p-1)$ prime, $n := \lfloor \log_2 p \rfloor + 1$. The most efficient known algorithms for computing discrete logarithms in these groups have a running time of $c \cdot \exp((1 + o(1))\sqrt{n \log n})$. (The algorithm implemented in MAPLE, `numtheory[mlog]`, is a combination of Pohlig-Hellman and baby step – giant step and thus has a running time of $c' 2^{n/2}$.) During an experiment with prime numbers p as above in the range of 2^{45} the running time for the computation of a discrete logarithm was about 3 seconds. (Even MAPLE can do this!) [Suggestion: Conduct your own experiment ...] [4]

How big should n be so that the key exchange is secure for 100, 1 000 or 10 000 years, respectively? [You are to assume $o(1) = 0$.]

(v) How long would MAPLE take for the value found for n that would take 100 years for the faster algorithms? [3]

Exercise 8.3 (Close vectors). (5+7 points)

In the lecture we have seen the following algorithm for computing an approximation to the closest vector problem:

Algorithm. Nearest plane.
Input: A reduced basis $B = (b_1, \ldots, b_n)$ of an n-dimensional lattice L in $\mathbb{R}^n$, and $z \in \mathbb{R}^n$.
Output: $x \in L$ with $||z - x|| \leq 2^{n/2} d(z, L)$.

1. Compute the GSO $(b_1^*, \ldots, b_n^*)$ of $(b_1, \ldots, b_n)$.
2. Compute the representation $z = \sum_{1 \leq i \leq n} a_i b_i^*$ of z in the GSO basis, with $a_1, \ldots, a_n \in \mathbb{R}$.
3. $a_n' \longleftarrow \lceil a_n \rfloor$,
   $y \longleftarrow z - (a_n - a_n') b_n^*$,
   $v \longleftarrow a_n' b_n$.
4. If $n = 1$, then return $x = v$. Else let M be the lattice generated by $b_1, \ldots, b_{n-1}$. Call the algorithm recursively to return $w \in M$ close to $y - v$.
5. Return $x = v + w$.

5 +2 (i) Consider the reduced basis $B := \begin{bmatrix} 3 & 2 & 1 \\ -2 & 1 & 4 \\ -2 & 2 & -2 \end{bmatrix}$ and the vector $z = (8, 9, 10)$.
Trace the values of the above algorithm by hand and give the approximate solution to the CVP.

+5 (ii) Implement the algorithm in a programming language of your choice. Hand in the source code.

Exercise 8.4 (The embedding technique). (6+5 points)

There is yet another way to solve the CVP approximately. The technique is called the *embedding technique* and works as follows. Suppose you are given an n-dimensional lattice $L = \mathcal{L}(B)$ and a vector $z \in \mathbb{R}^n$. A solution to the CVP corresponds to integers $a_1, \ldots, a_n \in \mathbb{Z}$ wuch that $z \approx \sum_{1 \leq i \leq n} a_i b_i$. The crucial observation is now that the length of $v := z - \sum_{1 \leq i \leq n} a_i b_i$ is small. The idea is now to construct out of L a lattice L' that contains v as a short vector.

2 (i) Show that the lattice L' spanned by the vectors $(b_1, 0), \ldots, (b_n, 0), (z, M)$, where $M \in \mathbb{R}_{>1}$ is some real number contains the vector (v, M).

4 (ii) You are now given the basis

$$B := \begin{bmatrix} 72 & 13 & 5 \\ 38 & 99 & 57 \\ 60 & 19 & 9 \end{bmatrix}$$

and the vector $z = (98, 99, 100)$ and $M = 1$. Use the above technique to compute a vector in L that is close to z.

+5 (iii) Perform some experiments with different values of M. For which do you obtain a solution?