KTH Computer Science and Communication

Homework 2

Due on May 24 at 16.00. Many of the problems are of such nature that the solutions can be found in the literature. Please solve the problems by yourself. Problems can be discussed in groups of up to three people but solutions should be written and handed in on an individual basis. It goes without saying that everybody handing in a solution should understand it fully. Also please specify with whom you have been collaborating.

1 Given n linearly independent vectors $\vec{b}_i$, $i = 1, \ldots n$ in R^n we define a lattice L to be all points of the form $\sum_{i=1}^{n} a_i \vec{b}_i$ for integers a_i. The vectors $\vec{b}_i$ are called a *basis* for L. As a simple example consider the two-dimensional lattice L_0 spanned by $\vec{b}_1 = (10, -1)$ and $\vec{b}_2 = (3, -1)$.

1a (5p) What is the shortest non-zero vector in L_0?

1b (5p) How many different bases are the for L_0?

1c (5p) The determinant of a lattice L is defined to the absolute value of a determinant whose ith row is the vector $\vec{b}_i$. Prove that this is well-defined in that different bases for the same lattice give the same value for the determinant of L. What is the determinant of L_0?

1d (5p) Define the dual lattice, L^*, of L as the set of vectors x in R^n such that the inner product (x, v) is an integer for any $v \in L$. What is L_0^*?

1e (5p) Is there a natural way to define $(L_0^*)^*$? Can you draw some general conclusions form this?

2 (20p) Let P be your 10 digit personal number. You want to find an elliptic curve group with $10^n \cdot P + 1$ elements for as large integer n as possible. Give and estimate of the largest n for which you think you can find such a curve, using moderate implementation time and at most 24 hours of computer time on an ordinary PC. You should describe the overall mathematical approach, your choice of algorithms, and motivate your estimate of the running time, but no implementation is needed.

3 (20p) In the Cramer-Shoup cryptosystem the key-generation of the system is defined by $h = g_1^z$ while the simulator uses $h = g_1^{z_1} g_2^{z_2}$. Suppose we used the same definition for the two occasions, what would happen? Note that there are two examples to consider, using $h = g_1^z$ and using $h = g_1^{z_1} g_2^{z_2}$ for both algorithms. Would the proof work in either case? If the proof breaks down you do not have to try to fix it, only point to the source of the problems. There is a set of lecture notes on Cramer-Shoup on the home-page of the course from 2003.

4 (20p) Suppose you have n honest-but-curious players, with P_i holding the bit x_i. Assume that no player is willing to cooperate with any other player and we want to compute the logical and-function of all the bits. In other words, we want a protocol that is 1-secure and want to computer $\wedge_{i=1}^{n} x_i$. Suppose each pair of players have a joint private channel. Design and analyze a protocol that solves this problem. Try for the best possible complexity where the complexity is to measure as the total number of messages sent in the network as a function of n.

5 (20p) Formally prove that the following symmetric encryption scheme is semantically secure. The secret key is given by a uniformly random index $k \in \{0,1\}^n$ of a family of pseudorandom functions, f_k, which maps $\{0,1\}^n$ to $\{0,1\}$. To encrypt a message $(m_i)_{i=1}^n$ one chooses a random n-bit string iv and sets $c_i = xor(f_k(iv+i), m_i)$ (where the addition in the argument is counted mod 2^n). The cryptotext is given by iv and $(c_i)_{i=1}^n$.

The attack model is that of "Chosen Plaintext Attack" and thus the attacker might as for a polynomial number (in security parameter n) of encryptions of messages.