The art of cryptography: Lattices and cryptography, summer 2013

PROF. DR. JOACHIM VON ZUR GATHEN, DR. DANIEL LOEBENBERGER

12. Exercise sheet
Hand in solutions until Sunday, 14 July 2013, 23:59h.

Exercise 12.1 (Did you get it?). (26 points)

(i) Given a basis B, what is the lattice spanned by B? $\boxed{1}$

(ii) Which properties must be fulfilled for a *reduced* basis B? $\boxed{2}$

(iii) What is the purpose of lattice basis reduction? $\boxed{2}$

(iv) Why don't we simply use Gram-Schmidt orthogonalization to reduce the lattice basis? $\boxed{1}$

(v) Is the basis $A = \begin{pmatrix} 12 & 3 \\ 13 & 5 \end{pmatrix}$ reduced? What about the matrix $B = \begin{pmatrix} 1 & 2 \\ 8 & -5 \end{pmatrix}$? $\boxed{3}$

(vi) Why is the volume of a lattice independent of the choice of the basis? $\boxed{2}$

(vii) Give the definition of the second successive minimum $\lambda_2(L)$ of a lattice L of dimension $n \geq 2$. $\boxed{1}$

(viii) State one important inequality that relates the length of a shortest nonzero vector of a lattice to its volume. $\boxed{1}$

(ix) Name one cryptographic primitive that was broken using lattice basis reduction and describe the attack. $\boxed{4}$

(x) State one algorithm that finds an approximation to the closest vector problem up to a factor of $2^{n/2}$ where n is the dimension of the lattice. $\boxed{2}$

(xi) Assume you performed a Diffie-Hellman key exchange in $\mathbb{Z}_p$ where the size of the prime was 2000 bit. Daniel suggests to take the first 128 bits of the shared secret as a secret key for a symmetric cipher like AES. Is this a good idea? Justify your answer. $\boxed{3}$

(xii) What is the purpose of the Coppersmith method? Given one cryptographic application. $\boxed{2}$

(xiii) Is the 2^n − SVP problem difficult? What about the $2^{n/17}$ − CVP-problem? $\boxed{2}$

Exercise 12.2 (Teach!). (0+10 points)

Go carefully through the supplied lecture notes and state at least three reasonable questions that would be suitable for an oral exam. Analyze the effort that is needed to solve each of your questions! $\boxed{+10}$