The Art of Cryptography: Integral Lattices, summer 2010

PROF. DR. JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER

10. Exercise sheet
Hand in solutions until Sunday, 27 June 2010, 23:59h.

Exercise 10.1 (The security of leading Diffie Hellman bits). (6+15 points)

In the lecture we discussed a reduction from computing a solution to the computational Diffie-Hellman problem over $\mathbb{Z}_p^\times$ to the problem of computing ℓ highest order bits of the solution to the problem.

(i) Compute bounds on ℓ when the prime p has $512, 1024, 2048$ or 4096 bits. $\boxed{2}$

(ii) What is in each cases a lower bound on the probability that your reduction worked? Use here the bound $1/2$ on the success probability of the hidden number algorithm given uniformly selected inputs. $\boxed{2}$

(iii) Give better bounds. $\boxed{2}$

(iv) On the website you find a Diffie-Hellman challenge. It contains several parameter choices as well as an instance of the computational Diffie-Hellman problem. Additionally there is a routine (which should serve as a black box) which implements the leading bit algorithm employed in the reduction from the lecture. As a reminder: The reduction algorithm from the lecture works as follows: $\boxed{+15}$

Algorithm. Reduction from DH to leading bits of DH.
Input: A prime p, a generator g of $\mathbb{Z}_p^\times$, and $A, B \in \mathbb{Z}_p^\times$.
Output: Some $w \in \mathbb{Z}_p^\times$, likely to solve the DH problem for A, B.

1. $\lambda \longleftarrow (\log_2 p)^{1/2}$,
   $\ell \longleftarrow \lceil 5\lambda \rceil$,
   $n \longleftarrow \lfloor \lambda/2 \rfloor$.
2. $r \xleftarrow{\text{⚅}} \mathbb{Z}_{p-1}$,
   $C \longleftarrow Ag^r$.
3. For $1 \leq i \leq n$ do steps 4 and 5.
4. $d_i \xleftarrow{\text{⚅}} \mathbb{Z}_{p-1}$,
   $D_i \longleftarrow Bg^{d_i}$,
   $t_i \longleftarrow C^{d_i}$.
5. Call a leading bit algorithm for C and D_i, to return $v_i \in V_\ell(\varrho(y_i))$, where (C, D_i, y_i) is a DH triple.
6. Call the algorithm for the hidden number problem with input $t = (t_1, \ldots, t_n)$ and $v = (v_1, \ldots, v_n)$ to return $u \in \mathbb{Z}_p^\times$ or "failure". In the latter case Return "failure".
7. Return $w = uB^{-r} \in \mathbb{Z}_p^\times$.

Solve the challenge. Remark: A major problem might be the efficiency of your basis reduction. It would be better if you use floating-point arithmetic. But beware: You need to set the floating-point accuracy properly such that no fatal rounding errors occur!

Exercise 10.2. (10 points)

Let $p \neq q$ be prime numbers, $N = p \cdot q$, $f = x \in \mathbb{Z}_N[x]$.

2 (i) Show that $p^2 + q^2$ is a unit in $\mathbb{Z}_N^\times$, i.e. $\gcd(p^2 + q^2, pq) = 1$.

1 (ii) Let $u \in \mathbb{Z}_N$ be the inverse of $p^2 + q^2$. Show that $f = u(px + q)(qx + p)$.

5 (iii) Prove that the two linear factors in (ii) are irreducible in $\mathbb{Z}_N[x]$. Hint: Consider the situation in $\mathbb{Z}_p$ and and $\mathbb{Z}_q$ separately.

2 (iv) Conclude that factoring N is polynomial-time reducible to factoring polynomials in $\mathbb{Z}_N[x]$.

Exercise 10.3 (An inequality of norms). (4 points)

4 Let $f \in \mathbb{Z}[t]$ be a polynomial of degree n. Define $\|f\|_1 := \sum_{1 \leq i \leq n} |f_i|$ and $\|f\|_2 := (\sum_{1 \leq i \leq n} f_i^2)^{1/2}$. Let $\sigma(f) := \#\{i \,|\, f_i \neq 1\}$ be the *sparsity* of f. Show that we have $\|f\|_1 \leq \sqrt{\sigma(f)}\|f\|_2$. Hint: Use the Cauchy-Schwarz inequality $\langle f, g\rangle \leq \|f\| \cdot \|g\|$, where f and g are the coefficient vectors of two polynomials of degree n.