The art of cryptography: Lattices and cryptography, summer 2013

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

8. Exercise sheet
Hand in solutions until Sunday, 16 June 2013, 23:59h.

Exercise 8.1. (10 points)

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

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

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

(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. $\boxed{5}$

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

Exercise 8.2 (An inequality of norms). (3 points)

Let $f \in \mathbb{Z}[t]$ be a polynomial of degree n. Define $\|f\|_1 := \sum_{1 \le i \le n} |f_i|$ and $\|f\|_2 := (\sum_{1 \le i \le n} f_i^2)^{1/2}$. Let $\sigma(f) := \#\{i \mid f_i \neq 1\}$ be the *sparsity* of f. Show that we have $\|f\|_1 \le \sqrt{\sigma(f)}\|f\|_2$. Hint: Use the Cauchy-Schwarz inequality $\langle f, g \rangle \le \|f\| \cdot \|g\|$, where f and g are the coefficient vectors of two polynomials of degree n. $\boxed{3}$

Exercise 8.3 (The Coppersmith method). (27+5 points)

In the lecture we discussed an algorithm for finding small polynomials with high-order roots.

(i) Implement the algorithm in a programming language of your choice. $\boxed{15}$

(ii) Play around with the parameters of the above algorithm. In particular perform the following experiments: Set $N = 2183$, $\mu = 1/2$, $v = 56$, $f = x + v$. Now compute for all $1 \le k \le 15$ the largest $c \ge 3$ for which your algorithm produces you a valid result. $\boxed{5}$

(iii) What do the results tell you in the context of the security of RSA primes? Explain detailed. $\boxed{7}$

(iv) Perform the same experiment with other values of v. $\boxed{+5}$