Number theory in cryptography

– Exercise set 8 –

The exercises P8.2, P8.3 have to be handed in on Tuesday, 23rd April 2024, 8:30 at latest.

Theoretical questions

T 8.1 In this exercise, you will prove that for a group G and $g \in G$ of order a prime power q^e, the discrete log problem of solving $g^x = h$ for $h \in G$ can be solved in $\mathcal{O}(eS_q)$ steps, where S_q is such that the DLP can be solved in G for an element of order q in time $\mathcal{O}(S_q)$. The idea of the proof is to write the exponent x as

$$x = x_0 + x_1 q + x_2 q^2 + \cdots + x_{e-1} q^{e-1} \text{ where } 0 \leqslant x_i < q$$

and to successively determine the x_i.

a) Show that one must have $h^{q^{e-1}} = (g^{q^{e-1}})^{x_0}$ and argue that therefore x_0 can be determined in S_q steps.

b) Having found x_0, now show that $h^{q^{e-2}} = g^{x_0 q^{e-2}} \cdot g^{x_1 q^{e-1}}$ and again use this to argue that x_1 can be found in S_q steps.

c) Explain how to continue this procedure to find $x_2, x_3, \ldots$ and finish the proof.

Programming exercises

P 8.1 Implement the sieve of Eratosthenes.

P 8.2 Implement a function `sieve`(n, B, L) that takes three arguments: an integer n, a smoothness bound B and the size of the sieving array L and sieves (as seen as part of the quadratic sieve) over the values of x in $\lfloor\sqrt{n}\rfloor + 1, \ldots, \lfloor\sqrt{n}\rfloor + L$, returning[1] the list of the numbers $x^2 - n$ that are B-smooth where $\lfloor\sqrt{n}\rfloor < x \leqslant \lfloor\sqrt{n}\rfloor + L$. Note: you may use SAGE functions to compute the roots of a polynomial modulo p.

P 8.3 Implement a function `factorQS`(n, B, L) doing the quadratic sieve algorithm for trying to find a non trivial factor of n. Find a non trivial factor of $n = 74354845706467$ using your algorithm.

[1] You can output more data if you want (for instance if needed in `factorQS`).