Cryptanalytic world records, summer 2014

DANIEL LOEBENBERGER, KONSTANTIN ZIEGLER

4. Exercise sheet
Hand in solutions until Saturday, 03 May 2014, 23:59:59

Exercise 4.1 (Quasi-polynomial time). (4 points)

In the lecture we encountered what is called quasi-polynomial complexity $n^{\mathrm{O}(\log n)}$ in a parameter n.

(i) Prove that this complexity is larger than any polynomial complexity in n. [2]

(ii) Prove that this complexity is smaller than any sub-exponential complexity in n. [2]

Exercise 4.2 (Yet another runtime estimate). (3 points)

Prove that for finite fields of size $Q = q^{2k}$ with $q \leq L_Q(\alpha)$, where $L_Q(\alpha) = \exp(\mathrm{O}((\log Q)^{\alpha}(\log\log Q)^{1-\alpha}))$, there exists a heuristic sub-exponential time algorithm for computing discrete logarithms, which runs in time $L_Q(\alpha)^{\mathrm{O}(\log\log Q)}$. [3]

Exercise 4.3 (Trivial translates). (8 points)

In the lecture we encountered transformations $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{F}_{q^2}$ and defined $m \cdot P = \frac{aP+b}{cP+d}$. Show that any m, whose entry are from $\mathbb{F}_q$ only, just gives a trivial relation. [8]

Exercise 4.4 (Towards a discrete log library). (12+140 points)

The goal of this exercise is to implement a discrete log library that will compute discrete logarithms in various groups G. To do so, perform the following tasks:

(i) Decide on a language in which you will implement the library and explain why you selected it. Hint: You will need an existing library that cares for you finite field and polynomial arithmetic. Also a factorization routine needs to be present. [2]

(ii) Implement the Baby-step giant-step algorithm for computing discrete logarithms in $G = \mathbb{F}_p^\times$ for any prime p. 4

For the following two tasks you have an additional week. Hand in your solutions until Saturday, 10 May 2014.

6 (iii) Implement the Pollard rho algorithm in $G = \mathbb{F}_p^\times$ for any prime p.

+6 (iv) Implement the Chinese remaindering algorithm for computing discrete logarithms in $G = \mathbb{F}_p^\times$ for any prime p.

+6 (v) Implement the Pohlig-Hellman algorithm in $G = \mathbb{F}_p^\times$ for any prime p.

For the following task you might use all time till the end of this summer term. Hand in your solution until Saturday, 19 July 2014.

+128 (vi) Implement the quasi-polynomial-time algorithm for solving discrete logarithms in finite fields that admit sparse medium subfield representation, presented in the lecture. Which problems do you observe? Hint: That's extremely challenging :)