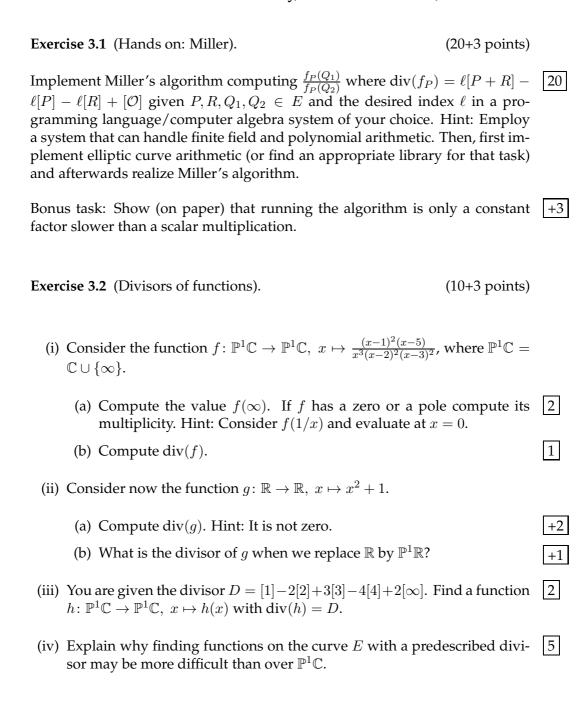
Advanced cryptography: Pairing-based cryptography winter term 2012/13

Daniel Loebenberger and Michael Nüsken

3. Exercise sheet Hand in solutions until Monday, 12 November 2012, 23:59:59



Exercise 3.3 (Security estimate).

(4+6 points)

The ElGamal signature scheme works over some publicly known group of (often prime) order ℓ , where ℓ has length n. In many cases this is a subgroup of some \mathbb{Z}_p^{\times} with another (larger) prime p; then $\ell | (p-1)$. However, it is necessary for its security that it is difficult to compute a discrete logarithm in the group and also, if applicable, in the surrounding group \mathbb{Z}_p^{\times} . The best known discrete logarithm algorithms achieve the following (heuristic, expected) running times:

method	year	time for a group size of n -bit
brute force (any group)	$-\infty$	$\mathcal{O}^{\sim}\left(2^{n}\right)$
Baby-step Giant-step (any group)	1971	$egin{aligned} \mathcal{O}^{\sim}\left(2^{n/2} ight)\ \mathcal{O}\left(n^22^{n/2} ight) \end{aligned}$
Pollard's ϱ method (any group)	1978	$\mathcal{O}\left(n^{2}2^{n/2}\right)$
Pohlig-Hellman (any group)	1978	$\mathcal{O}^{\stackrel{\searrow}{\sim}}(2^{n/2})^{'}$
Index-Calculus for $\mathbb{Z}_p^{ imes}$	1986	$2^{(\sqrt{2}+o(1))n^{1/2}\log_2^{1/2}n}$
Number-field sieve for \mathbb{Z}_n^{\times}	1990	$2^{((64/9)^{1/3} + o(1))n^{1/3}\log_2^{2/3}n}$

It is not correct to think of o(1) as zero, but for the following rough estimates just do it. Estimate the time that would be needed to find a discrete logarithm in a group whose order has n-bits assuming the (strongest of the) above estimates are accurate with o(1) = 0 (which is wrong in practice!)

- (i) for n = 1024 (standard size),
- (ii) for n = 2048 (as required for Document Signer CA),
- (iii) for n = 3072 (as required for Country Signing CA).

Repeat the estimate assuming that for the given group only Pollard's ϱ method is available, for example in case the group is a ℓ -element subgroup of \mathbb{Z}_p^{\times} or an elliptic curve,

- (iv) for n = 160,
- (v) for n = 200,
- (vi) for n = 240.

4

In April 2001 Reynald Lercier reported (http://perso.univ-rennes1. fr/reynald.lercier/file/nmbrJL01a.html) that they can solve a discrete logarithm problem modulo a 397-bit prime p within 10 weeks on a 525MHz computer.

(vii) Which bit size for the prime p is necessary to ensure that they cannot solve the DLP problem in \mathbb{Z}_p^{\times} given —say— 10′000 10GHz computers and 1 year (disregarding memory requirements).

[Note: The record for computing discrete logs in $\mathbb{F}_{2^n}^{\times}$ lies at n=613, see Antoine Joux http://perso.univ-rennes1.fr/reynald.lercier/file/nmbrJL05a.html.]