Elliptic curve cryptography, winter 2009

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

8. Exercise sheet
Hand in solutions until Monday, 11 January 2010, 23^{59}

Exercise 8.1 (Embedding degree). (3 points)

Let μ_n be the set of all nth roots of unity in the algebraic closure $\overline{k}$. Given n and q determine the minimal $e \in \mathbb{N}$ such that $\mu_n \subseteq \mathbb{F}_{q^e}^\times$. 3

Exercise 8.2 (Security estimate). (10 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)	$-\infty$	$\mathcal{O}\left(2^n\right)$
Baby-step Giant-step (any group)	1971	$\mathcal{O}\left(2^{n/2}\right)$
Pollard's ϱ method (any group)	1978	$\mathcal{O}\left(n^2 2^{n/2}\right)$
Pohlig-Hellman (any group)	1978	$\mathcal{O}\left(2^{n/2}\right)$
Index-Calculus for $\mathbb{Z}_p^\times$	1986	$2^{(\sqrt{2}+o(1))n^{1/2}\log_2^{1/2} n}$
Number-field sieve for $\mathbb{Z}_p^\times$	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), 1
(ii) for $n = 2048$ (as required for Document Signer CA), 1
(iii) for $n = 3072$ (as required for Country Signing CA). 1

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 $n = 160$, 1
(v) for $n = 200$, 1
(vi) for $n = 240$. 1

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.

4 (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`.]

Exercise 8.3 (Determinants and Trace). (6 points)

Let M and N be two 2×2 matrices with $N = \left[\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right]$. Define the adjoint matrix $\widetilde{N} = \left[\begin{smallmatrix} z & -x \\ -y & w \end{smallmatrix}\right]$.

3 (i) Show that $\operatorname{trace}(M\widetilde{N}) = \det(M+N) - \det(M) - \det(N)$.

3 (ii) Use (i) to show that for all scalars a, b we have

$$\det(aM+bN) - a^2 \det(M) - b^2 \det(N) = ab(\det(M+N) - \det(M) - \det(N))$$

Exercise 8.4 (Flexes revised). (3 points)

3 Let E be an elliptic curve defined over k. Prove that a point P on E is a flex-point iff $P \in E[3]$.

Exercise 8.5 (An alternate definition of the Weil pairing). (6+12 points)

Let E be an elliptic curve defined over a field k. In class we considered the Weil pairing $e\colon E[n] \times E[n] \to \mu_n,\ (Q, R) \mapsto e(Q, R)$. Goal of this exercise is to get a different insight in the properties of this pairing. We construct a pairing by first selecting an appropriate basis T_1, T_2 of $E[n]$ and a primitive nth root of unity ζ and require $e(T_1, T_2) := \zeta$. This leads to $e(a_1T_1 + a_2T_2, b_1T_1 + b_2T_2) =: \zeta^{a_1b_2 - a_2b_1} \in \mu_n$ by anticipating bilinearity and antisymmetry.

1 (i) Show that e is bilinear

1 (ii) and antisymmetric.

4 (iii) Show that e is nondegenerate.

+6 (iv) Prove that e is Galois compliant: $e(\sigma S, \sigma T) = \sigma(e(S, T))$.

+6 (v) Prove that e is endomorphism compliant: for separable endomorphisms α we have $e(\alpha(S), \alpha(T)) = e(S, T)^{\deg \alpha}$.