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

DANIEL LOEBENBERGER AND MICHAEL NÜSKEN

1. Exercise sheet
Hand in solutions until Monday, 29 October 2012, 23:59:59

A word on the exercises. They are important. Of course, you know that. You need 50% of the credits to be admitted to the final exam. As an additional motivation, you will get a bonus for the final exam if you earn more than 70% or even more than 90% of the credits. The bonus does not help passing the exam, but if you pass the bonus will increase your mark by up to two thirds.

Exercise 1.1 (Secure email). (4 points)

(i) Send a digitally signed email with the subject [2]

`[12ws-ac] hello`

to us at

`daniel@bit.uni-bonn.de` and `nuesken@bit.uni-bonn.de`

from your personal account. The body of your email must be nonempty and the signature must be verifiable and correct. [It is a good idea to verify this by sending a blind carbon copy (Bcc) to oneself.]

With Thunderbird I recommend using `enigmail` and `gpg`. In any case make sure to register your key at `http://pgp.mit.edu/`.

Choose yourself among this and possible other solutions. In any case use a pgp key pair.

(ii) Find the fingerprint of your own PGP key. Bring two printouts of it and an identification document to the next tutorial. (Do not send us an email with it. Guess, why!) [2]

Note: Future exercise hand-ins will only be accepted via signed email. Then a bonus point will be awarded for a correct signature and a malus for a missing or invalid signature.

Exercise 1.2 (Degenerations). (4 points)

Let G_1, G_2 and G_3 be finite groups. Assume that all group orders $\#G_1 = \#G_2 = \#G_3 = p$ for some prime p. Consider a bilinear map [4]

$$e\colon \begin{array}{ccc} G_1 \times G_2 & \longrightarrow & G_3, \\ (g_1, g_2) & \longmapsto & e(g_1, g_2) \end{array}$$

Show that e is non-degenerate, i.e. that

- if for all $Q \in G_2$, we have $e(P, Q) = 1$, then $P = \mathcal{O}$,
- if for all $P \in G_1$, we have $e(P, Q) = 1$, then $Q = \mathcal{O}$.

if and only if there are points $P \in G_1$ and $Q \in G_2$ with $e(P, Q) \neq 1$. Hint: Note that under the above restrictions all considered groups are cyclic.

Exercise 1.3 (Formulas for the addition law on elliptic curves). (6 points)

[6] Given an elliptic curve

$$E\colon y^2 = x^3 + ax + b$$

and two points $P = (x_1, y_1) \neq \mathcal{O}$ and $Q = (x_2, y_2) \neq \mathcal{O}$ with $P \neq Q$ describe the coordinates of $P + Q$ as functions of the coordinates of P and Q. Hint: Write down the equation for the line connecting P and Q and plug the result into the curve equation. Then solve the equation for x, noting that you already know two solutions.

Exercise 1.4 (The group law). (11+4 points)

Consider the elliptic curve $E\colon y^2 = x^3 - x + 1$ over $\mathbb{R}$. The three points $P = (-1, 1)$, $Q = (0, 1)$, $S = (3, -5)$ lie on the curve.

[1] (i) Plot the real picture of the curve.

[1] (ii) Compute $-P$.

[1] (iii) Write down the line connecting P and $-P$.

[2] (iv) Compute $P + Q$ and $Q + S$ together with the two lines connecting them.

[2] (v) Include also those two lines in your plot.

[2] (vi) Compute $(P + Q) + S$ and $P + (Q + S)$. What do you observe?

[1] (vii) Compute $((P + Q) + S) + Q$.

[1] (viii) Compute $P + \mathcal{O}$ and $\mathcal{O} + \mathcal{O}$.

[+4] (ix) Do the same computations as in (i) – (viii) when considering the curve over $\mathbb{F}_{17}$.