Cryptography I, homework sheet 11
Due: 11 December 2014, 10:45

Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually. To submit your homework, email it to `crypto14@tue.nl` or place it on the lecturer's table before the lecture. Do not email Tanja or put homework in mailboxes.
This is a good moment to figure out how your pocket calculator can do computations modulo biggish primes.

1. Compute the twisted Edwards curve corresponding to the Montgomery curve $v^2 = u^3 + 486662u^2 + u$ over $\mathbb{F}_{2^{20}-3}$.
   The point $P = (2, 117777)$ is on the Montgomery curve. Compute the point corresponding to $2P$ on the twisted Edwards curves by
   (a) computing $2P$ on the Montgomery curve and mapping the result to the twisted Edwards curve and
   (b) computing the point P' corresponding to P on the Edwards curve and then computing $2P'$ on the twisted Edwards curve.

   The results from these two ways of computing should be equal. Check that they are on the twisted Edwards curve.

2. Consider the short Weierstrass equation $y^2 = x^3 + ax + b$. Show that the curve is not an elliptic curve, i.e. the curve is singular, if and only if $4a^3 - 27b^2 = 0$. You can use that $y^2 = f(x)$ is singular if and only if $\gcd(f, f')$ is $\neq 0$ and is not constant. Note that here the field does not have characteristic 2 or 3.