Cryptography I, homework sheet 11

Due: 12 December 2013, 10:45

Please submit your homework electronically; the TAs do not want to receive homework on paper. Please bundle your scans into one pdf file. 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 `crypto13@tue.nl`.
In general, you may use computer algebra systems such as mathematica and sage; please submit your code as part of your homework if you end up using a system. Accepted systems/languages: Sage, mathematica, matlab, Pari-GP, Java.

Before the exam please train yourself in doing moduluar arithmetic. Better calculators are programmabge and is useful for you to teach it to do arithmetic modulo numbers; also XGCD is a useful program to implement. Do this before the exam. Of course you can also print and bring huge multiplication tables and hope that I use those numbers. My exercises will not assume that you have polynomial arithmetic.

1. For computing discrete logarithms on elliptic curves it is important that collisions can be recognized. This means that point addition has be computed in affine coordinates, costing at least one inversion per group operation. For this task Weierstrass curves are the most efficient, so even if a curve is given in Edwards form for efficient and secure implementation of the cryptosystem, the cryptanalyst will transform it to (short) Weierstrass form in order to attack it.

   The curve $y^2 = x^3 - 3x + 910$ over $\mathbb{F}_{2347}$ is an elliptic curve with order $\ell = 2389$, ℓ is prime. Implement Pollard's rho method (without negation is OK) to compute the discrete logarithm of $Q = (699, 835)$ to the base $P = (2232, 361)$, i.e. the integer $0 < k < \ell$ with $Q = kP$.

   The answer to this exercise consists of a number (the result) and the program computing it. Please test that your program runs and that the result is correct.

Take a look at `http://hyperelliptic.org/EFD/` for many more curve shapes and addition formulas. We'll not cover other shapes in class, but you should know that they exist.

If you ever find yourself choosing elliptic curves for applications, keep in mind that we didn't cover all possible attacks known. Take a look at `http://safecurves.cr.yp.to/` for some safe and not so safe curves.