Cryptography I, homework sheet 9

Due: 28 November 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.

Please email Tanja in case you have found no way of obtaining a programmable calculator to use for the exam. Your calculator should be able to do modular arithmetic; there is no need to have the calculator do polynomial arithmetic. To explain this: if your calculator is programmable you can 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. Prove that for (x_1, y_1) and (x_2, y_2) on the circle $^2 + y^2 = 1$ also their sum $(x_1, y_1) + (x_2, y_2) = (x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$ is on the circle.

2. Find all points (x_1, y_1) on the Edwards curve $x^2 + y^2 = 1 - 5x^2y^2$ over $\mathbb{F}_{13}$. Verify that $P = (6, 3)$ and $Q = (3, 7)$ are on the curve. Compute $R = 2P + Q$.