Cryptography I, homework sheet 9

Due: 27 November 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.

You may use computer algebra systems such as mathematica, gp, or sage or program in C, Java, or Python. Please submit your code as part of your homework. Make sure that your programs compile and run correctly; my students will not debug your programs. The program should be humanly readable.

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. Show how to compute the addition of two points on the circle with just three field multiplications and a few additions.

3. Show how to compute point doubling, i.e., the addition of a point to itself, with just two field multiplications and a few additions.