Cryptography, homework sheet 5

Due: 08 October 2015, 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 the programming part to `crypto15@tue.nl` and place the written part 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 if any) as part of your homework. If you do, make sure that your programs compile and run correctly; my students will not debug your programs. The program should also be humanly readable.

If you are a student in the old masters system and for some reason cannot substitute 2MMC10 for the course (2WC09 or 2WC12) in your study program, please contact Tanja by email. To find out whether you can substitute the course, talk to your study advisor.

1. Use the schoolbook version of Pollard's rho method to attack the discrete logarithm problem given by $g = 3, h = 245$ in $\mathbb{F}_{1013}^*$, i.e. find an integer $0 < a < 1012$ such that $h = g^a$, using the t_i and r_i (the twice as fast walk) as defined in class (and repeated here). Let $t_0 = g, a_0 = 1$, and $b_0 = 0$ and define

$$t_{i+1} = \begin{cases} t_i \cdot g \\ t_i \cdot h \\ t_i^2 \end{cases}, a_{i+1} = \begin{cases} a_i + 1 \\ a_i \\ 2a_i \end{cases}, b_{i+1} = \begin{cases} b_i \\ b_i + 1 \\ 2b_i \end{cases} \text{ for } t_i \equiv \begin{cases} 0 \bmod 3 \\ 1 \bmod 3 \\ 2 \bmod 3 \end{cases},$$

   where one takes t_i as an integer. The twice as fast walk has $r_i = t_{2i}$.

   Note that this version offers less randomness in the walk, splitting into more than 3 sets increases the randomness. The walk could start at any $t_0 = g^{a_0} h^{b_0}$ for known a_0 and b_0 – but then the homework would be harder to correct.

2. Prove that for (x_1, y_1) and (x_2, y_2) on the circle $x^2 + y^2 = 1$ 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.

3. 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 $R = 2P + Q$.