Cryptography I, homework sheet 11
Due: 23 December 2011, 10:45

Both exercises can be done with the help of a computer but you should submit your programs as part of the homework solution. The program can be based on any computer algebra system, in particular for computing in $\mathbb{F}_{1013}^*$ and $\mathbb{F}_{1019}^*$. Make sure that your programs compile and run correctly; my students will not debug your programs. The program should be humanly readable.

1. The schoolbook version of Pollard's rho method is often described with a simpler iteration function than we had in class.

   Let $G_0 = g, b_0 = 1$, and $c_0 = 0$ and define

   $$G_{i+1} = \begin{cases} G_i \cdot g \\ G_i^2 \\ G_i \cdot h \end{cases}, b_{i+1} = \begin{cases} b_i + 1 \\ 2b_i \\ b_i \end{cases}, c_{i+1} = \begin{cases} c_i \\ 2c_i \\ c_i + 1 \end{cases} \text{for } G_i \equiv \begin{cases} 0 \bmod 3 \\ 1 \bmod 3 \\ 2 \bmod 3 \end{cases},$$

   where one takes G_i as an integer.

   Use this definition 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 G_i as defined above and $H_i = G_{2i}$.

   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 $G_0 = g^i h^j$ for known i and j – but then the homework would be harder to correct.

2. For a numerical example for the index calculus attack have a look at `http://hyperelliptic.org/tanja/teaching/NTCrypto10/pictures/19-Nov-10`, in particular `IMGP2371.JPG`.

   Use factor base $\mathcal{F} = \{2, 3, 5, 7, 11, 13\}$ to solve the DLP $h = 281$, $g = 2$, in $\mathbb{F}_{1019}^*$.