Cryptography I, homework sheet 9

Due: 03 December 2010, 10:45

Both exercises should 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 $\mathbb{F}_{1013}^*$.

1. $3 \in \mathbb{F}_{1013}^*$ generates a group of order 1012, so it generated the whole multiplicative group of the finite field. Solve the discrete logarithm problem $g = 3, h = 224$, i.e. find an integer $0 < a < 1012$ such that $h = g^a$, using the Baby-Step Giant-Step algorithm.

2. 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.