Cryptography I, homework sheet 8

Due: 21 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.

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.

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.

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 (also, see below).

   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. Use factor base $\mathcal{F} = \{2, 3, 5, 7, 11, 13\}$ to solve the DLP $h = 281$, $g = 2$, in $\mathbb{F}_{1019}^*$. I.e. pick random powers of $g = 2$, check whether they factor into powers of 2,3,5,7,11, and 13; if so, add a relation.

   E.g. $2^{291} \equiv 52 \bmod 1019$; over the integers $52 = 2^2 \cdot 13$, so we incluclude the relation $291 \equiv 2a_2 + a_{13} \bmod 1018$. Note that you can run into difficulties inverting modulo 1018 since it is not prime. E.g. $2^{658} \equiv 729 \bmod 1019$; over the integers $729 = 3^6$, so we incluclude the relation $658 \equiv 6a_3 \bmod 1018$ but 6 is not invertible modulo 1018 and we can only determine $a_3 \equiv 449 \bmod 509$ and need to test whether $a_3 = 449$ or $a_3 = 449 + 509$. Here $2^{449} \equiv 1016 \bmod 1019$ and $2^{449+509} \equiv 3 \bmod 1019$, thus $a_3 = 958$.

   Hint: if you're using Pari-GP you'll find

   ```
   factor(lift(Mod(2^i,p)))
   ```

   a usefull command.