Cryptography I, homework sheet 7

Due: 13 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. $3 \in \mathbb{F}_{1013}^*$ generates a group of order 1012, so it generates the whole multiplicative group of the finite field.

   Alice's public key is $h_A = 224$. Use ElGamal encryption to encrypt the messge $m = 42$ to her using the "random" value $k = 654$.

2. $3 \in \mathbb{F}_{1013}^*$ generates a group of order 1012, so it generates the whole multiplicative group of the finite field. Solve the discrete logarithm problem $g = 3, h = 224$ using the Baby-Step Giant-Step algorithm.

3. 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.