Summer School – Number Theory for Cryptography, Warwick
Exercises for lectures by T. Lange, June 25, 2013

1. The Elliptic Curve Digital Signature Algorithm works as follows: The system parameters are an elliptic curve E over a finite field $\mathbb{F}_p$, a point $P \in E(\mathbb{F}_p)$ on the curve, the number of points $n = |E(\mathbb{F}_p)|$, and the order ℓ of P. Furthermore a hash function h is given along with a way to interpret $h(m)$ as an integer.

   Alice creates a public key by selecting an integer $1 < a < \ell$ and computing $P_A = aP$; a is Alice's long-term secret and P_A is her public key.

   To sign a message m, Alice first computes $h(m)$, then picks a random integer $1 < k < \ell$ and computes $R = kP$. Let r be the x coordinate of R considered as an integer and then reduced modulo ℓ; for primes p you can assume that each field element of $\mathbb{F}_p$ is represented by an integer in $[0, p-1]$ and that this integer is then reduced modulo ℓ. If $r = 0$ Alice repeats the process with a different choice of k. Finally, she calculates

   $$s = k^{-1}(h(m) + r \cdot a) \bmod \ell.$$

   If $s = 0$ she starts over with a different choice of k.

   The signature is the pair (r, s).
   To verify a signature (r, s) on a message m by user Alice with public key P_A, Bob first computes $h(m)$, then computes $w \equiv s^{-1} \bmod \ell$, then computes $u_1 \equiv h(m) \cdot w \bmod \ell$ and $u_2 \equiv r \cdot w \bmod \ell$ and finally computes $S = u_1 P + u_2 P_A$. He accepts the signature as valid if the x coordinate of S matches r when computed modulo ℓ.

   (a) Show that a signature generated by Alice will pass as a valid signature by showing that $S = R$.

   (b) Show how to obtain Alice's long-term secret a when given the random value k for one signature (r, s) on some message m.

   (c) You find two signatures made by Alice. You know that she is using an elliptic curve over $\mathbb{F}_{1009}$ and that the order of the base point is $\ell = 1013$. The signatures are for $h(m_1) = 345$ and $h(m_2) = 567$ and are given by $(r_1, s_1) = (365, 448)$ and $(r_2, s_2) = (365, 969)$. Compute (a candidate for) Alice's long-term secret a based on these signatures, i.e. break the system.

2. $3 \in \mathbb{F}_{1013}^*$ generates a group of order $1012 = 4 \cdot 11 \cdot 23$, so it generates the whole multiplicative group of the finite field. Solve the discrete logarithm problem $g = 3, h = 321$ by using the Pohlig-Hellman attack, i.e. find an integer $0 < k < 1012$ such that $h = g^k$ by computing first k modulo $2, 4, 11$, and 23 and then computing k using the Chinese Remainder Theorem.

3. $3 \in \mathbb{F}_{1013}^*$ generates a group of order 1012. Solve the discrete logarithm problem $g = 3, h = 224$ using the Baby-Step Giant-Step algorithm (see below).

4. The schoolbook version of Pollard's rho method is often described with just three sets. This exercise will use the multiplicative group of a finite field, so we use multiplicative notation.

   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 lifts G_i to $\mathbb{Z}$ in the last part. At every step $G_i = g^{b_i} h^{c_i}$.

   Use this definition to attack the discrete logarithm problem given by $g = 3, h = 245$ in $\mathbb{F}_{1013}^*$ using Pollard's rho method, i.e. find an integer $0 < a < 1012$ such that $h = g^a$, using the G_i as defined above and $H_i = G_{2i}$.