Cryptographic passports & biometrics, summer 2009

MICHAEL NÜSKEN, KONSTANTIN ZIEGLER

5. Exercise sheet
Hand in solutions until Monday, 25 May 2009.

Any claim needs a proof or argument.

Exercise 5.1 (Counting Elliptic Curves). (11 points)

Working over $\mathbb{Z}_p$, where the prime number $p \neq 2, 3$, every elliptic curve is determined by some cubic equation in Weierstrass Normal Form

$$y^2 = x^3 + ax + b$$

where we require $4a^3 + 27b^2 \neq 0$ to avoid multiple roots for the cubic polynomial on the right-hand side.

By a linear transformation of coordinates this equation can be transformed into Legendre Normal Form

$$y^2 = x(x-1)(x-\lambda).$$

(i) What is the requirement on λ to avoid multiple roots for the cubic polynomial on the right-hand side. $\boxed{1}$

(ii) Let $p = 13$ and pick some admissable λ. How many points are on your elliptic curve? $\boxed{3}$

(iii) Write an algorithm that for a given p loops over all admissable λ and counts the number of points on the corresponding elliptic curve. $\boxed{3}$

(iv) For $p = 13$ draw a graph with possible sizes of elliptic curves on the x-axis and number of curves of that given size on the y-axis. $\boxed{2}$

(v) Use the data from the last exercise to verify the Hasse bound for $p = 13$. $\boxed{2}$

Exercise 5.2 (Diffie Hellman key exchange). (6 points)

Perform a toy example of a Diffie Hellman key exchange: Fix $p = 47$ and $g = 2 \in \mathbb{Z}_p^\times$.

(i) Show that the order of g is 23, i.e. $g^{23} = 1$ but $g^k \neq 1$ for $1 \leq k < 23$. [If $\boxed{1}$
you are clever then you only need to calculate g^{23}.] $\boxed{1}$

(ii) Choose $x \in \mathbb{Z}_{23}$ (take $x \notin \{0, 1\}$ to get something interesting) and calculate $h_A := g^x$. $\boxed{1}$

$\boxed{1}$ (iii) Choose $y \in \mathbb{Z}_{23}$ (take $y \notin \{0, 1, x\}$ to get something interesting) and calculate $h_B := g^y$.

$\boxed{2}$ (iv) Now compute h_B^x and h_A^y and compare.

Exercise 5.3 (ElGamal signatures). (7 points)

Compute an ElGamal signature for your student identification number represented in binary. Use $p = 467$ and $g = 3 \in \mathbb{Z}_p^\times$ and work in $G = \langle g \rangle$. For simplicity, we take the function HASH: $\{0,1\}^* \to \mathbb{Z}_{233}$, $x \mapsto (\sum_{0 \leq i < |x|} x_i 2^i) \bmod 233$. (Eg. 18 translates to the string 10010 which in turn translates into the number $18 \bmod 233$.)

$\boxed{1}$ (i) Here $\#G = 233$ and thus $\exp_g\colon \mathbb{Z}_{233} \to G$, $a \mapsto g^a$ is an isomorphism. [Note that $166^2 = 3$ and thus $g^{233} = 1$. Since $g \neq 1 \ldots$]

$\boxed{1}$ (ii) Setup: Compute Alice' public key with $\alpha = 9$.

$\boxed{3}$ (iii) Sign: Sign the hash value of your student identification number.

$\boxed{2}$ (iv) Verify: Verify the signature.