The electronic health card, summer 2008

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

10. Exercise sheet
Hand in solutions until Monday, 07 July 2008.

Exercise 10.1 (Secret sharing). (11 points)

In class you have learnt a method for secret sharing. First let us recall this method using an example. Let $p = 10000019$ and $u_1 = 1484998$, $u_2 = 8055552$, $u_3 = 412501$, $u_4 = 8994679$, $u_5 = 236054$.

(i) Compute the secret from $f(u_1) = 2016419$, $f(u_2) = 951970$, $f(u_3) = 9707737$, $f(u_4) = 6395629$, $f(u_5) = 8552973$. [2]

(ii) Name values for $(f(u_i))_i$, so that the corresponding secret $f(0)$ is your student registration number. [2]

Furthermore, we want to investigate which data yields sensitive information and which data does not. This time we use $p = 1009$ so that iterations over all of $\mathbb{F}_p$ are reasonable. Let f_0 be your student registration number modulo p, choose $u_1, \ldots, u_7, f_1, \ldots, f_7 \in \mathbb{F}_p$ at random with the u_i pairwise distinct and not 0. Finally, no u_i should be equal to 1008.

(iii) Suppose a coalition of the secret bearers 1 through 7 has found out that $u_0 = 1008$. Compute the distribution of possible secrets. (Try all values for $f(u_0)$ and count how many times each possible secret occurs as the value $f(0)$.) [2]

(iv) Now suppose a coalition of secret bearers 1 through 7 has learnt that $f(u_0) = 1008$. Once again compute the distribution of possible secrets. (Try all values for u_0 and count the number of times that each possible secret occurs as the value $f(0)$.) [2]

(v) Compare the results: is one of the indiscretions a problem for secret bearer 0? Which one? Why? Can you describe "how much" information was disclosed? [3]

Hints: MUPAD knows a function `interpolate` that allows to do interpolation modulo a prime number with great ease. (The help is useful here.)

Exercise 10.2 (Point doubling on elliptic curves). (3+1 points)

Let $P = (x_P, y_P)$ be a point on the elliptic curve

$$E = \{(x, y) \in F^2 : y^2 = x^3 + ax + b\}$$

over a field F of characteristic not 2 or 3.

3 (i) Show that $S = (x_S, y_S) = P + P = 2P$ can be computed using the following formulae, if $y_1 \neq 0$:

$$\alpha = \frac{3x_P^2 + a}{2y_P},$$
$$x_3 = \alpha^2 - 2x_P,$$
$$y_3 = (x_P - x_S)\alpha - x_S - y_P.$$

Hint: Use the tangent to the curve in the point P.

+1 (ii) What happens if $y_P = 0$?

Exercise 10.3 (Elliptic Curve Miniquiz). (8 points)

1 (i) Does the equation $y^2 = x^3 + 7x + 2$ define an elliptic curve over $\mathbb{F}_{37}$?

2 (ii) Are the points $P = (0, 2)$ and $Q = (7, 5)$ on the elliptic curve $y^2 = x^3 + 5x + 2$?

1 (iii) What is the negative of the points $P = (2, 4)$, $Q = (3, 5)$, $R = (9, 2)$ on the elliptic curve over $\mathbb{F}_{13}$ given by $y^2 = x^3 + 3x + 2$?

2 (iv) On the curve $y^2 = x^3 + 7x$ over $\mathbb{F}_{23}$, compute $(3, 5) + (10, 9)$ and

2 (v) compute $2 \cdot (3, 18)$.

Exercise 10.4 (Addition on elliptic curves). (2 points)

2 Consider an elliptic curve $E\colon y^2 = x^3 + ax + b$ over $\mathbb{F}_q$. Let P be a point on the curve. Explain how to compute $39P$.