Tanja Lange
TU/e

23 Feb 2010

1. Take-home exercises mastermath class "Algebraic Geometry in Cryptology"

Deadline: March 6, 2009, 18:00 Utrecht time

To submit your homework attach a pdf or jpeg to an email and send it to `tanja@hyperelliptic.org`. You are encouraged to use latex for your presentation but a scan of a handwritten solution is also acceptable. Word documents will NOT be accepted. You may use a computer algebra system such as sage in your calculations and some exercises rely on computer help.

1. Consider the following public-key cryptosystem:
   Key set up: Alice chooses two integers a and b, puts $M = ab - 1$, chooses two more integers a' and b', and sets $e = a'M + a$, $d = b'M + b$, and $n = (ed - 1)/M$.
   The public key is (n, e), the private key is d.

   Encryption and Decryption: To send Alice a plaintext m, Bob computes $c = em \bmod n$.
   Alice deciphers the ciphertext by multiplying c by d modulo n.

   (a) Show that n is an integer.

   (b) Why does this recover the plaintext? I.e. explain why $m = dc \bmod n$ holds.

   (c) Set up your own public key in this system; document the intermediate steps.

   (d) Alice's public key is $(8495535633017684, 26176918391)$; send her a message of your choice.

   (e) Alice received the ciphertext 7957782655548030. Find out which message she received, i.e., break the system.

2. Consider the curve $C_1 : y^2 = x^3$ over $\mathbb{F}_p$ with $p = 1071508607186267320948425049060$
   $001810561404811705533607443750388370351051124936122493198378815695858127 5$
   $946729175531468251871452856923140435984577574698574803934567774824230985 4$
   $210746050623711418779541821530464749835819412673987675591655439460770629 1$
   $457119647768654216766042983165262438683720566806967 3$. On the set of points of $C_1(\mathbb{F}_p) \setminus \{(0,0)\}$ one can define the same addition law as on an elliptic curve in Weierstrass form, i.e. use $(x, y) + (x, -y) = P_\infty$, and otherwise for $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$

$$P_1 + P_2 = (\lambda^2 - x_1 - x_2, \lambda(x_1 - (\lambda^2 - x_1 - x_2)) - y_1), \text{ where } \lambda = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2} & P_1 \neq \pm P_2 \\ \frac{3x_1^2}{2y_1} & P_1 = P_2 \neq -P_2 \end{cases}$$

(a) Study C_1 for singularities.

(b) Let $P = (82553022009387336145524668234779684573257825612189350561427260591100273885807062957824535658566640445289519686699130892045362755603232210453015344364857661496157602368246826902571003166703222751965680950886098150975158225223444790211148742706306105007570333186823325386941410982827793281555791168926 30, 78604519532530080163343190869730836715219851018677841800165871094026336277112120531825940931901834110741035370648293278340798040385254914517005404246836126854400792527836228243994335485991401731270510991354610576113635361090312945114840677985486442186368878917913292707236928961109857008717893055369 49) be the basis point.
Solve the discrete logarithm problem for $Q = (53276092970282927792815133095220612790724142642074227418629311414759731217194740429033065633960936222267008538606442811228881753887722994573849537355380047723326522322482825479200423389511554031524112359669829022818628190836279783288286978404321951326910746901669743852068266851834333908786159792873 5, 67675747879983740453125312544858892673466358042108805733241983991031208185828691006926687233488537756261414508342408565163044688825931538063375407086552495274045594853225858462324330499500114506616838663083695320449853758614384081670884168261064788606671459542482044853404186062940028815018617264413 01)$, i.e., find a natural number k so that $Q = kP$ holds.

3. Consider the curve $C_2 : y^2 = x(x-1)^2$ over $\mathbb{F}_p$ with p odd.

(a) Study C_2 for singularities.

(b) As in the previous exercise one can define a group law on $C_2(\mathbb{F}_p) \setminus \{(0,1)\}$; this time using $\lambda = (3x_1^2 - 4x_1 + 1)/(2y_1)$ in case $P_1 = P_2$. How can you solve the discrete-logarithm problem on this curve? Show differences and similarities with the previous exercise.
Attention: Do not list generic attacks here, only attacks that are faster than $\sqrt{p}$ count. You may use claims made in the lectures.

4. Let k be a field with $\mathrm{char}(k) \neq 2$. The projective curve $C \subset \mathbb{P}^3$ is defined over k and has generators of $I(C)$

$$F_1 = X^2 + Y^2 - Z^2 - dT^2, F_2 = XY - ZT,$$

where $d \in k \setminus \{0,1\}$. Study C for singularities by using the standard covering of $\mathbb{P}^3$ by copies of $\mathbb{A}^3$ and dehomogenizing F_1 and F_2.