Prof. Dr. M. Kreuzer
P. Ackermann

Abgabe: 27.06.2005, 14h

Kryptografie
Übungsblatt 10

Aufgabe 30:
Gegeben seien der Körper $K = \mathbb{Q}$ oder $K = \mathbb{Z}/p\mathbb{Z}$ mit $p \notin \{2, 3\}$ sowie eine elliptische Kurve $E(K)$ über K mit Gleichung $y^2 = x^3 + ax + b$.

a) Schreiben Sie eine Funktion `EllipticAdd(...)`, die die Summe zweier Punkte von $\overline{E}(K)$ berechnet. Der unendlich ferne Punkt $\mathcal{O}$ werde dabei durch den String `'InfPoint'` repräsentiert.

b) Verwenden Sie die Funktion aus a), um eine Funktion `EllipticMult(...)` zu schreiben, die zu gegebenen $n \in \mathbb{Z}$ und $P \in \overline{E}(K)$ den Punkt $nP \in \overline{E}(K)$ berechnet. Berechnen Sie dazu die Punkte $2^i P$ und gehen Sie wie bei der Berechnung großer Potenzen vor.

Aufgabe 31:
Gegeben sei eine Zahl $e > 0$ und der Körper $K = \mathbb{F}_q$ mit $q = 2^e$.

a) Zeigen Sie, dass die Abbildung $\mathrm{Tr} : \mathbb{F}_q \longrightarrow \mathbb{F}_2$, die gegeben ist durch $\mathrm{Tr}(x) = \sum_{i=0}^{e-1} x^{2^i}$, surjektiv ud $\mathbb{F}_2$-linear ist.

b) Beweisen Sie, dass die Gleichung $y^2 + y = x$ für ein gegebenes $x \in \mathbb{F}_q$ genau dann in $\mathbb{F}_q$ lösbar ist, wenn $\mathrm{Tr}(x) = 0$ gilt.
Tipp: Genau die Hälfte der Elemente $x \in \mathbb{F}_q$ erfüllt $\mathrm{Tr}(x) = 0$.

c) Finden Sie einen Algorithmus, wie man für $x \in \mathbb{F}_q$ mit $\mathrm{Tr}(x) = 0$ ein $y \in \mathbb{F}_q$ mit $y^2 + y = x$ finden kann.
Tipp: Wählen Sie eine $\mathbb{F}_2$–Basis von $\mathbb{F}_q$ und stellen Sie die Elemente x, y als Linearkombinationen in dieser Basis dar.

d) Sei die elliptische Kurve $E(K)$ über K gegeben durch $y^2 + ay = x^3 + bx + c$ oder $y^2 + axy = x^3 + dx^2 + e$ mit $a, b, c, d, e \in K$ (vgl. Aufgabe 27). Finden Sie einen probabilistischen Algorithmus, wie man einen Punkt von $E(K)$ berechnen kann.