Gregor Leander
28.04.2008

Fakultät für Mathematik
Ruhr-Universität Bochum

Kryptographie II – Übungsblatt 7

Aufgabe 1: *Rechnen auf Elliptischen Kurven I* (10 Punkte)

Betrachte die über $\mathbb{F}_{19}$ durch folgende Gleichung definierte Kurve

$$E : y^2 = x^3 + x + 9 \ .$$

1. Zeige, dass E eine elliptische Kurve ist. (2 Punkte)
2. Bestimme alle Punkte auf E über $\mathbb{F}_{19}$. (4 Punkte)
3. Bestimme die Punkte der Ordnung 2 auf E. (2 Punkte)
4. Sei $P = (1, 12) \in E$. Berechne $445 \cdot P$. (2 Punkte)

Aufgabe 2: *Rechnen mit Elliptischen Kurven II* (4+3 Punkte)

Betrachte die Kurve

$$E_{p,k} : y^2 + x\,y = x^3 - 2\,x^2 + x + 3$$

über $\mathbb{F}_{p^k}$, wobei p eine Primzahl ist und k eine natürliche Zahl ist.

1. Für welche Werte von p und k ist die Kurve $E_{p,k}$ singulär? (4 Punkte)
2. Für alle andere Werte von p und k bestimme die Weierstraß-Form von $E_{p,k}$. (3 Punkte)

Abgabe: Freitag, 6.06.2008 bis 12:00 Uhr im Kasten im Gebäude NA Ebene 02 oder Samstag, 7.06.2008 bis 12:00 Uhr per Mail an `mansour.alsawadi@rub.de`.