RUHR UNIVERSITÄT BOCHUM RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Ilya Ozerov, Elena Kirshanova

Präsenzübungen zur Vorlesung

Kryptanalyse

SS 2014

Blatt 10 / 3 July 2014

Exercise 1:
Let α be a generator of $\mathbb{Z}_q^*$ for prime q. Show that for $i \xleftarrow{\$} \{1, \dots, q-1\}$

$$\mathrm{ord}_{\mathbb{Z}_q^*}(\alpha^i) = \frac{q-1}{\mathrm{GCD}(i, q-1)}.$$

Elliptic Curves

Exercise 2:

- Suppose that a cubic polynomial $X^3 + AX + B$ factors as
$$X^3 + AX + B = (X - r_1)(X - r_2)(X - r_3).$$
Prove that $4A^3 + 27B^2 = 0$ is and only if two (or more) of r_1, r_2, r_3 are the same.
- Let $P = (x, y)$ be a point on the elliptic curve E given by $y^2 = x^3 + Ax + b$. Show that if $y = 0$ then $3x^2 + A \neq 0$.

Exercise 3:
Show that the number of elliptic curves defined over $\mathbb{F}_p$ for prime p is $p^2 - p$.

Exercise 4:
Show that three points on an elliptic curve add to $\mathcal{O}$ if and only if they are collinear.