RUHR
UNIVERSITÄT
BOCHUM

RUB

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

**Hausübungen zur Vorlesung**

# Kryptanalyse

**SS 2014**

Blatt 9 / 7 July, 2014

**Exercise 1** (10 Punkte)**:**
Using index-calculus method solve the dlog problem $\beta = \alpha^x \mod p$ for

$$(\alpha, \beta, p) = (204667, 733106, 759377).$$

Use the factor-base of $B$-smooth numbers for $B = 200$ (you can increase/decrease $B$). In addition, provide the discrete logarithms for the factor-base elements.

**Exercise 2** (4 Punkte)**:**
Let $E$ be $y^2 = x^3 - 20x + 21 \mod 35$ and $P = (15, -4)$.

1. Check that $P \in E$
2. Factor 35 by trying to compute $3P$
3. Factor 35 by trying to compute $4P$ by doubling twice
4. Compute both $3P$ and $4P$ on $E \mod 5$ and $E \mod 7$. Explain why the factor 5 is obtained by computing $3P$ and 7 is obtained by computing $4P$.

**Exercise 3** (6 Punkte)**:**

1. Prove that there are $q+1$ points on the elliptic curve $y^2 = x^3 - x$ defined over $\mathbb{F}_q$ when $q = 3 \mod 4$.
2. Suppose that for any $a \in \mathbb{Z}$ there is an efficient algorithm of generation a point $P = (x, y)$ such that $y^2 = x^3 + ax \mod n$. Explain why it would *not* be a good idea to use the elliptic curves $y^2 = x^3 + ax$ with various $a$'s to factor $n$.