Übung zur Vorlesung

# Kryptographie und Komplexität

Prof. Dr. Christoph Kreitz
Universität Potsdam, Theoretische Informatik, WS 2009/10

**Blatt 3 (Version 1) — Abgabetermin: 26.1.2010**

---

## Aufgabe 3.1 (El Gamal Systeme)

1. Gegeben sei ein öffentlicher ElGamal Schlüssel $K := (53, 2, 30)$ und ein ElGamal-Schlüsseltext $(24, 37)$. Bestimmen Sie den zugehörigen Klartext $x$.

2. Gegeben sei ein öffentlicher ElGamal Schlüssel $K := (p, g, A)$. Wie kann man aus zwei ElGamal-Schlüsseltexten $(B_1, y_1)$ und $(B_2, y_2)$ einen gültigen ElGamal-Schlüsseltext $(B_3, y_3)$ erzeugen, ohne den geheimen Schlüssel $a$ mit $A = g^a$ oder die Zufallszahlen $b_i$ mit $B_i = g^{g_i}$ zu kennen? Wie kann man diesen Angriff verhindern?

## Aufgabe 3.2 (Elliptische Kurven)

1. Wieviele Punkte hat die elliptische Kurve $y^2 = x^3 + x + 1$ über $\mathbb{Z}_7$? Ist die Punktgruppe zyklisch? Wenn ja, bestimmen Sie einen Erzeuger.

2. Gegeben sei ein ECC ElGamal Schlüssel $K := (E(23, 2, 8), (10, 4), 5, (0, 13))$ und ein ElGamal-Schlüsseltext $((6, 11), (13, 0))$. Bestimmen Sie den zugehörigen Klartextpunkt $x$.

## Aufgabe 3.3 (Diskrete Logarithmen)

1. Lösen Sie $15 = 2^x \bmod 239$ und $693 = 3^x \bmod 1823$ mit dem Algorithmus von Shanks.

2. Lösen Sie $2 = 3^x \bmod 65537$ mit dem Algorithmus von Pohlig-Hellmann.

3. Lösen Sie $507 = g^x \bmod 1117$ für den kleinsten Erzeuger $g$ von $\mathbb{Z}_{1117}$ mit dem Algorithmus von Pohlig-Hellmann.

4. Lösen Sie $15 = g^x \bmod 3167$ für den kleinsten Erzeuger $p$ von $\mathbb{Z}_{3167}$ mit dem Pollard $\rho$-Algorithmus.

5. Lösen Sie $13 = 7^x \bmod 2039$ mit der Index-Calculus Methode und der Faktorbasis $\{2, 3, 5, 7, 11\}$.