G. Leander
.
.

Lehrstuhl für
Informationssicherheit und Kryptologie
Ruhr-Universität Bochum

Kryptographie II
Übungsblatt 9

Abgabe bis Dienstag, 27.6.2006 NA 5/75.

Aufgabe 1 *Elliptische Kurven*
Betrachten Sie folgende elliptische Kurve über $GF(2579)$

$$E : y^2 = x^3 + x + 6.$$

Bestimmen Sie mit Hilfe des Baby-Step Giant Step Algorithmus den Diskreten Logarithmus von

$$Q = (1433, 820)$$

zur Basis

$$P = (2405, 2124).$$

Hinweis: Geben Sie hierzu auch ihren Quellcode ab.

Aufgabe 2 *Zufalls Wahl*
Wir haben bei den Generischen Gruppen keine Operation für die zufällige Wahl eines Elementes vorgesehen. Wie kann ein Algorithmus mit Zugriff auf das Gruppen Oracle eine solche Operation umsetzen?

Aufgabe 3 *Nullstellen*
Sei p prim und $n, d \in \mathbb{N}$ mit $d \leq n - 1$. Nach einem Lemma von Schwarz hat ein Polynom

$$P \in \mathbb{Z}_p[X_1, \ldots, X_n]$$

vom Grad d höchstens dp^{n-1} Nullstellen $(x_1, \ldots, x_n)$ in $\mathbb{Z}_p^n$.

1. Zeigen Sie, dass diese Grenze scharf ist. Finden Sie hierfür für jedes p, n und d eine Polynom mit genau dp^{n-1} Nullstellen.

2. Zeigen Sie, durch Angabe eines Gegenbeispiels, dass der Satz falsch ist, wenn p nicht prim ist.

Aufgabe 4 *Generische Gruppen*

1. Warum kann der Satz über Diskrete Logarithmen für generische Gruppen nicht primer Ordnung nicht stimmen?

2. An welcher Stelle im Beweis über die Schwierigkeit von Diskreten Logarithmen in generischen Gruppen geht entscheiden ein, dass die Gruppenordnung prim ist?

Hinweis: Erinnern Sie sich für den ersten Teil der Aufgabe an die Algorithmen zum Berechnen von Diskreten Logarithmen aus der Vorlesung.