Gregor Leander
28.04.2008

Fakultät für Mathematik
Ruhr-Universität Bochum

Kryptographie II – Übungsblatt 6

Aufgabe 1 *Diskrete Logarithmen* 2+4+4=10 Punkte

1. Ein Algorithmus nutzt zum Berechnen des Diskreten Logarithmus in einer (zyklischen) Gruppe G primer Ordnung nur die Gruppenoperation und keine speziellen Eigenschaften der Gruppe.

   Wie viele Operationen muss er mindestens Ausführen, um den Diskreten Logarithmus eines zufälligen Elements in G mit einer Wahrscheinlichkeit größer als $1/2$ zu lösen? Begründe Deine Antwort.

2. Was bedeutet diese Aussage für die Schwierigkeit des DL Problems über elliptischen Kurven?

3. Ein Algorithmus A berechnet beliebige Diskrete Logarithmen in einer gegebenen, festen Gruppe G mit etwa 2^{160} Elementen in ungefähr 2^{53} Gruppenoperationen. Was bedeutet diese Aussage für die Gruppe G und den Algorithmus A?
   Zeige mindestens zwei Szenarien, in denen diese Situation geschehen kann.

Aufgabe 2 *Zufalls Wahl* 3 Punkte

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* 4+4=8 Punkte

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* 3+3=6 Punkte

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?

Abgabe: Freitag, 30.05.2008 bis 12:00 Uhr im Kasten im Gebäude NA Ebene 02 oder Samstag, 31.05.2008 bis 12:00 Uhr per Mail an `mansour.alsawadi@rub.de`.