**Gregor Leander**
**28.04.2008**

**Fakultät für Mathematik**
**Ruhr-Universität Bochum**

# Kryptographie II – Übungsblatt 5

---

**Aufgabe 1** *Baby-Step-Giant-Step Algorithmus* 6 Punkte

Berechnen Sie mit Hilfe des Baby-Step-Giant-Step Algorithmus den Diskreten Logarithmus von 67 zur Basis 5 in $\mathbb{Z}_{103}$.

---

**Aufgabe 2** *Der Silver-Pohlig-Hellman Algorithmus* 12 Punkte

1. Berechnen Sie mit Hilfe des Silver-Pohlig-Hellman Algorithmus den diskreten Logarithmus von 500 zur Basis 7 in $\mathbb{F}_{601}^*$.
2. Warum wird der Silver-Pohlig-Hellman Algorithmus praktisch unmöglich, wenn die Gruppenordnung durch eine Primzahl der Länge 80 Bit geteilt wird?
3. Wie kann man den Baby-Step-Giant-Step Algorithmus in Kombination mit dem Silver-Pohlig-Hellman Algorithmus nutzen, um Diskrete Logarithmen auch in der Situation von Aufgabenteil 2 zu berechnen?
4. Welche Anforderungen sollte man daher an die Gruppenordnung einer Gruppe $G$ stellen, damit das Berechnen von Diskreten Logarithmen in $G$ heutzutage praktisch unmöglich ist?

---

**Aufgabe 3** *Index Calculus* 8 Punkte

Bestimmen Sie mit dem Index Calculus Verfahren den Logarithmus von $X^3 + X^2 + 2$ zur Basis $g = X$ in

$$\mathbb{F}_{3^5} = \mathbb{F}_3[X]/(X^5 - X + 1)$$

Nutzen Sie als Faktorbasis

$$B = \{X, X + 1, X - 1\}$$

und als "Zufallszahlen" im ersten Schritt

$$t = \{20, 22, 23\}$$

und im zweiten Schritt

$$t = 19$$

---

Abgabe: Freitag, 23.05.2008 bis 12:00 Uhr im Kasten im Gebäude NA Ebene 02 oder Samstag, 24.05.2008 bis 12:00 Uhr per Mail an `mansour.alsawadi@rub.de`.