Kryptographie - Algebraischer Hintergrund
Prof . Dr. F.-O. Schreyer
Übungsblatt 7: Diskrete Logarithmen

Abgabetermin 2.7.2002
Voraussetzungen: Vorlesungskapitel Diskrete Logarithmen, Elliptische Kurven.

1. Implementieren Sie Shanks' baby-step giant-step Methode zur Berechnung von diskreten Logarithmen für eine allgemeine Gruppe G und testen Sie Ihr Skript mit

   (a) $G = \mathbb{F}_p^*$ und

   (b) $G = E(\mathbb{F}_p)$. Bestimmen Sie nicht die Gruppenordnung $|E(\mathbb{F}_p)|$, sondern verwenden Sie die obere Abschätzung aus dem Satz von Hasse.

2. Implementieren Sie Pollards ρ-Methode zur Berechnung von diskreten Logarithmen in $\mathbb{F}_p^*$ (Speicherung von β_{2^j} und β_i für $i = 2^j + 1, ..., 2^{j+1}$) und testen Sie sie an Beispielen.

3. Implementieren Sie den Pohlig-Hellman-Algorithmus für $\mathbb{F}_p^*$ und testen Sie ihn an Beispielen.

4. Vergleichen Sie die Laufzeit der Skripte aus den Aufgaben 1, 2 und 3 an Beispielen.

5. Berechnen Sie mit dem Index-Calculus-Algorithmus unter Verwendung der Faktorbasis

   $$F := \{2, 3, 5\}$$

   die Lösung von

   $$13^x \equiv 19 \bmod 479$$

Abgabe der Aufgaben bitte als email an:

boehm@btm8x5.mat.uni-bayreuth.de
oder
boehm@math.uni-sb.de