Albert-Ludwigs-Universität
Institut für Informatik
Prof. Dr. S. Albers
C. Gunia, S. Schmelzer

Freiburg i. Br., den 31. Mai 2006

Software-Praktikum SS 06
Implementation von kryptographischen Protokollen
Aufgabenblatt 5

Bearbeitung bis 26.07.2006

Implementieren Sie das ECDSA-Verfahren. Folgende Funktionalitäten sind zu implementieren:

- Erzeugung eines Schlüsselpaars mit den in Blatt 1 angegebenen Schlüssellängen
- Erstellen und Verifizieren einer Signatur

Hinweise: Die in der Literatur beschriebenen Kurven *P192*, *P224*, *P256* und *P386* sollen für das ECDSA-Verfahren verwendet werden. Die Parameter dieser Kurven sind in den Dateien *P192.dat*, *P224.dat*, *P256.dat* und *P386.dat* abgelegt. Eine Datei enthält sechs BigInteger Objekte in der Reihenfolge p, a, b, G_x, G_y und r.