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 4

Bearbeitung bis 05.07.2006

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

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

Hinweis: Die Erzeugung der Primzahlen p und q ist im Anhang des zweiten Dokuments der Literaturliste ausführlich beschrieben.