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

Freiburg i. Br., den 9. Mai 2006

Software-Praktikum SS 06
Implementation von kryptographischen Protokollen
Aufgabenblatt 2

Bearbeitung bis 24.05.2006

Informieren Sie sich über die Verfahren RSA, DSA und ECDSA. Setzen Sie die Algorithmen in eine geeignete Klassenstruktur um. Folgende Punkte sind zu bearbeiten.

1. Erstellen Sie eine Klassenhierarchie für die drei genannten Verfahren und implementieren Sie die Oberklassen mit den allgemeinen Funktionalitäten. Beachten Sie dabei, welche Gemeinsamkeiten alle drei zu implementierenden Algorithmen aufweisen (Schlüsselpaarerzeugung, Schlüsselpaar aus privatem und öffentlichem Schlüssel, ...).

2. Definieren Sie Klassen und Methoden, welche allgemeine Funktionalitäten aufnehmen (Umwandlung eines Bytestroms in eine natürliche Zahl, ...).

3. Implementieren Sie die Datenbank zur Speicherung der Schlüsselpaare.

4. Legen Sie einen geeigneten Header für verschlüsselte Dateien fest. Implementieren Sie das Erstellen und Auslesen dieses Headers.