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

Freiburg i. Br., den 21. April 2006

Software-Praktikum SS 06
Implementation von kryptographischen Protokollen
Aufgabenblatt 1

Bearbeitung bis 10.05.2006

Erstellen Sie mit *Swing* eine Oberfläche, welche die folgenden Komponenten enthält:

- Hauptfenster: Im Hauptfenster befindet sich eine Tabelle mit allen verfügbaren Schlüsselpaaren und den wichtigsten Informationen über diese (Name, Schlüssellänge, Typ). Alle anderen Dialoge sind vom Hauptfenster erreichbar.
- Dialoge zum Ver-/Entschlüsseln: In diesen können Quell- und Zieldatei, Verschlüsselungs- und Signaturschlüssel, sowie der Betriebsmodus *ECB* oder *CBC* ausgewählt werden.
- Dialog zum Erzeugen eines neuen Schlüsselpaares: In diesem Dialog wird der Name des Schlüsselpaares, der Typ und die Schlüssellänge eingegeben. Der Schlüsselname ist eindeutig zu wählen.
- Es besteht die Möglichkeit den öffentlichen Schlüssel eines Schlüsselpaares in eine Datei zu exportieren und aus dieser zu importieren. Erstellen Sie hierfür geeignete Oberflächen.
- Schlüsselpaare können gelöscht und umbenannt werden.
- Jeder Menüeintrag des Hauptfensters soll ein mnemonisches Kürzel haben und über Beschleunigertasten angesteuert werden können.

Verfügbare Schlüssellängen:

- RSA: 512, 1024, 2048 und 4096 Bit
- DSA: 512-1024 Bit in Abständen von jeweils 64 Bit
- ECDSA: Beim ECDSA-Verfahren werden vier elliptische Kurven zur Verfügung gestellt, welche die Schlüssellängen 192, 224, 256 und 384 Bit besitzen.