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

Freiburg i. Br., den 10. Mai 2006

Software-Praktikum SS 06
Implementation von kryptographischen Protokollen
Aufgabenblatt 3

Bearbeitung bis 14.06.2006

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

- Erzeugung eines Schlüsselpaars mit den in Blatt 1 angegebenen Schlüssellängen
  - Bestimmung einer Primzahl in einem vorgegebenen Intervall
  - Miller-Rabin Test
  - Bildung des Inversen zur Bestimmung von e und d
- Ver- und Entschlüsseln
- Signieren und Verifizieren einer Signatur
- Betriebsmodi *ECB* und *CBC*

Hinweise:

- Wird d kleiner als ein Viertel von n gewählt, so existiert ein Angriff mit dem e bestimmt werden kann. Stellen Sie sicher, dass d ausreichend groß ist.
- RSA verschlüsselt Blöcke gleicher Größe. Der letzte Block muss deshalb im Allgemeinen aufgefüllt werden. Bei ungeschicktem Auffüllen ist auch hier die Möglichkeit eines Angriffs gegeben. Aus diesem Grund sollte immer mit Zufallswerten aufgefüllt werden.
- Beim Erstellen der Signatur wird nicht die Nachricht selbst, sondern ein Hashwert signiert. Verwenden Sie einen geeigneten Hashalgorithmus von JAVA zum Erstellen der Signatur. Wird die Signatur an die verschlüsselte Datei gehangen, so ist es möglich Unterschriften zu fälschen, d.h. die Nachricht abzuändern und für diese eine korrekte Signatur zu erzeugen. Deshalb sollte erst die Signatur erstellt und anschließend verschlüsselt werden.
- Die Verwendung eines guten Zufallszahlengenerators ist zwingend notwendig für die Sicherheit der Implementation. Informieren Sie sich über die Möglichkeiten die JAVA bietet und verwenden Sie einen geeigneten Zufallszahlengenerator.

Zusatz: Operationen mit dem privaten Schlüssel können durch die Anwendung des chinesischen Restsatzes beschleunigt werden. Diese Vorgehensweise ist bei großen Schlüssellängen zu empfehlen. Eine kurze Beschreibung zur Anwendung findet sich unter `http://tupac.euv-frankfurt-o.de/www/kryptos/rsa.html`.