Technische Universität München
Institut für Informatik
Prof. Dr. Ernst W. Mayr

WS 1998/99
Aufgabenblatt 9
18. Januar 1999

Praktikum Algorithmen-Entwurf

(Abgabetermin: Montag, den 25. Januar 1999, $24.^{00}$ Uhr)

Aufgabe 1 RSA-Verfahren

Implementieren Sie das RSA-Verfahren zum Verschlüsseln und digitalen Signieren von Files. Die Funktionalität soll hierbei auf zwei eigenständige Programme verteilt werden.

a) Das Programm `rsainit` zur Initialisierungsphase soll folgende Kommandozeilenschnittstelle realisieren:

`rsainit <Anzahl Bits von` p`> <Anzahl Bits von` q`> <Filename>`

Der Aufruf `rsainit 10 20 foo` soll die Dateien `foo.public`, `foo.private` und `foo.log` erzeugen. `foo.public` und `foo.private` bestehen aus zwei Zeilen, wobei die erste Zeile die Zahl n und die zweite Zeile die Zahl e bzw. d enthalten soll. `foo.log` besteht aus vier Zeilen, welche die Zahlen n, $\lfloor \log_2(n) \rfloor$, p und q enthalten.

Beim randomisierten Primzahltest muß festgelegt werden, wieviele Wiederholungen durchgeführt werden sollen. Bitte verwenden Sie bei Ihrer Implementierung mindestens zehn Wiederholungen. Dadurch wird eine für unsere Zwecke akzeptable Fehlerwahrscheinlichkeit von unter 0.1% erreicht.

b) Das Programm `rsamain` zur Verschlüsselung bzw. digitalen Signatur erhält folgende Kommandozeilenschnittstelle:

`rsamain <Schlüsseldatei>`

Als Schlüsseldatei gibt man die `.public`-Datei an, wenn man verschlüsseln will bzw. die `.private`-Datei zum Entschlüsseln. Zum Signieren werden die Rollen von `.public`- und `.private`-Datei vertauscht.

`rsamain` soll von der Standardeingabe lesen und auf die Standardausgabe schreiben. Hierbei besteht jede Zeile aus einem RSA-Block, der getrennt zu behandeln ist. Das Ergebnis der Ver- bzw. Entschlüsselung ist wiederum

Zeile für Zeile auszugeben (Das Fileformat vor und nach der Behandlung mit `rsamain` bleibt also gleich).

Die beiden Perl-Skripten `numencode` und `numdecode` dienen dazu, daß Sie mit `rsamain` auch Textdateien ver- und entschlüsseln können[1]. Durch

```
numencode 100 foo.txt > numfoo.txt
```

wird die Datei `foo.txt` in eine Zahldarstellung konvertiert, die als Eingabe für `rsamain` verwendet werden kann, und diese in der Datei `numfoo.txt` gespeichert. Das erste Argument steht hierbei für die maximale Länge von Bits, die ein einzelner Block (entspricht einer Zeile) umfassen darf. Man muß hier eine Zahl angeben, die kleiner ist als der Wert $\lfloor \log_2(n) \rfloor$, der von `rsainit` ausgegeben wurde.

Mit

```
numdecode 100 numfoo.txt > foo.txt
```

wird die Zahldarstellung wieder zurücktransformiert in die ursprüngliche Datei `foo.txt`. Beachten Sie, daß beim Ausführen der Perl-Skripten der in den Skripten angegebene Pfad zum Interpreter `perl` stimmen muß. Diesen Pfad müssen Sie anpassen, wenn Sie die Skripten beispielsweise unter Linux verwenden möchten.

Wenn `foo.txt` den Inhalt

```
Yet another stupid demo.
```

besitzt, so sieht `numfoo.txt` folgendermaßen aus:

```
089101116032097110111116104101
114032115116117112105100032100
101109111046010032032032032032
```

Solche Dateien sollte Ihr Programm Zeile für Zeile ver- und entschlüsseln können.

Hinweis

Versuchen Sie, möglichst viele Teile des Programms zum Primzahltest wiederzuverwenden.
Die Datei `cryexa.cry` enthält einen verschlüsselten Text, den Sie zum Testen Ihres Programmes verwenden können. Wenn Sie die Datei mit `prakkey.public` entschlüsseln und `numdecode 550` auf das Ergebnis anwenden, sollte ein mehr oder minder sinnvoller Klartext zum Vorschein kommen.

[1] In Zukunft steht also Ihrer hochgeheimen Korrespondenz nichts mehr im Wege...