Dr. Markus Junker — Diskrete Algebraische Strukturen — Sommer 2011
Übungsblatt 6

Verantwortlich für die Übungen:
Dr. Fritz Hörmann (fritz.hoermann@math.uni-freiburg.de)

1. **Effizientes Potenzieren modulo** N (4 Punkte). Schreiben Sie eine Funktion (in einer Programmiersprache Ihrer Wahl), die effizient modulo N mittels „binärer Exponentiation“ potenziert. D. h. gegeben $N \in \mathbb{N}_{>0}$, $0 \leq x < N$ und $y \in \mathbb{N}$, berechne $0 \leq z < N$ so, dass
$$(\overline{x})^y = \overline{z}$$
in $\mathbb{Z}/N\mathbb{Z}$.
Die Funktion sollte für alle $N < \sqrt{b}$ korrekt sein, wobei b der verwendete Zahlbereich ist (also z.B. $b = 2^{64}$ bei der Verwendung von 64-Bit Zahlen).

2. **Eulersche φ-Funktion** (4 Punkte). Seien p und q zwei verschiedene Primzahlen. Beweisen Sie, dass
$$\varphi(p \cdot q) = (p-1) \cdot (q-1).$$

3. **RSA-Verfahren** (8 Punkte). Der folgende (hexadezimale) Code enthält eine mit dem RSA-Verfahren verschlüsselte Nachricht
```
481fab24 d4b06fd8 0eea354b 73dedbe6
```
Der öffentliche Schlüssel ist ($N = 4\ 111\ 577\ 933, e = 63\ 139$).
Ihnen ist die folgende Faktorisierung in Primzahlen bekannt:
$$4\ 111\ 577\ 933 = 62\ 731 \cdot 65\ 543.$$
Berechnen Sie den privaten Schlüssel und dekodieren Sie die Nachricht.
Der Text der Originalnachricht wurde wie folgt kodiert. Er wurde im ANSI/ASCII Zeichensatz repräsentiert und dann in Folgen aus 4 Zeichen zerlegt. Jede dieser Zeichenfolgen aus 4 Zeichen ergibt so eine Zahl x zwischen 0 und $2^{32}-1$, die dann mit dem RSA-Verfahren mit öffentlichem Schlüssel ($N = 4\ 111\ 577\ 933, e = 63\ 139$) codiert wurde, d. h. es wurde x^e modulo N berechnet. Bitte geben Sie alle Schritte Ihrer Rechnung an.

*4. **RSA knacken** (4 Zusatzpunkte). Die folgende Nachricht wurde, ähnlich wie in Aufgabe 2, diesmal mit einem Schlüssel zur Basis $N = 4\ 258\ 931\ 557$ verschlüsselt:
```
aaeb874b d6c50e2a 23b15fb8 28f0c546
```
Ermitteln Sie mittels eines geeigneten Programmes durch Probieren den privaten und öffentlichen Schlüssel und dekodieren Sie die Nachricht.
Hinweis: Sie dürfen annehmen, dass die verschlüsselte Nachricht nur aus den Zeichen ‘a’ bis ‘z’ besteht (Kleinbuchstaben).
Diese Aufgabe zeigt insbesondere, dass das RSA-Verfahren mit kleinem N und/oder ohne vorheriges Komprimieren der Daten unsicher sein kann.

Abgabe am 20.6.2011 im Hörsaal vor Beginn der Vorlesung