Wolfgang K. Seiler
Tel. 2515

A5, Zimmer C201

Themenvorschläge für die kleinen Übungen am 19. März 2007

a) Ein Teilnehmer eines RSA-Systems hat den öffentlichen Schlüssel (N, e) mit $N = 25\,957 = 257 \cdot 101$ (beide Faktoren sind prim) und $e = 12\,047$. Berechnen Sie seinen privaten Exponenten!

b) Ein Text wird mit RSA verschlüsselt, indem man seine Buchstaben durch ihre ASCII-Codes (als Zahlen zwischen 0 und 255) ersetzt, diese als Ziffern von Zahlen $< N$ zur Basis 256 auffaßt, und dann diese Zahlen verschlüsselt. Schicken Sie die Nachricht „ja“ an den Inhaber des Schlüssels $(28\,891, 3)$!
Hinweis: „a“ hat den ASCII-Code 97.

c) Berechnen Sie den diskreten Logarithmus modulo 13 von Fünf zur Basis Sieben!

d) Zeigen Sie, daß es keinen diskreten Logarithmus modulo 13 von Fünf zur Basis Drei gibt!

e) *Richtig oder falsch:* Die Vektoren $\begin{pmatrix}\alpha\\1\end{pmatrix}$ und $\begin{pmatrix}\alpha+1\\\alpha\end{pmatrix}$ aus $\mathbb{F}_4^2$ sind linear unabhängig.

f) *Richtig oder falsch:* Die Abbildung $\varphi\colon \mathbb{F}_4 \to \mathbb{F}_4$, die α und $\alpha+1$ miteinander vertauscht und $0, 1$ auf sich selbst abbildet, ist $\mathbb{F}_2$-linear.

g) *Richtig oder falsch:* Für ein Polynom mit Koeffizienten in $\mathbb{F}_2$ ist

$$(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n)^2 = a_0 + a_1x^2 + a_2x^4 + \cdots + a_nx^{2n}\,.$$

h) Was ist $(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)(x^2 + 1)$, wenn man mit Koeffizienten aus $\mathbb{F}_2$ rechnet?

i) Zeigen Sie: Das Polynom $x^4 + 1$ ist reduzibel über $\mathbb{F}_2$.

j) Berechnen Sie den ggT der beiden Polynome $x^4 + 1$ und $x^3 + 1$ sowohl über $\mathbb{R}$ als auch über $\mathbb{F}_2$!

k) Berechnen Sie über $\mathbb{F}_2$ den ggT der beiden Polynome $f = x^4 + x^2 + 1$ und $g = x^3 + 1$, und stellen Sie ihn in der Form $\alpha f + \beta g$ dar!

l) Zeigen Sie: In $\mathbb{F}_{2^n}$ hat jedes Element genau eine Quadratwurzel.

m) Für welche Primzahlen p gilt dies auch im Körper $\mathbb{F}_p$?

n) Multiplikation in $\mathbb{F}_8 = \mathbb{F}_2^3$ mit Basis $1, \alpha, \alpha^2$ sei über das Polynom $\alpha^3 + \alpha + 1$ definiert. Berechnen Sie die Elemente

$$x = (\alpha^2 + 1)(\alpha + 1), \quad y = (\alpha^2 + 1)^2 \quad \text{und} \quad z = \frac{1}{\alpha}\,!$$

o) Multiplikation in $\mathbb{F}_{64} = \mathbb{F}_2^6$ mit Basis $1, \alpha, \alpha^2, \ldots, \alpha^6$ sei über das Polynom $\alpha^6 + \alpha + 1$ definiert. Berechnen Sie die Elemente

$$x = (\alpha^2 + 1)^3, \quad y = (\alpha^3 + 1)^3 \quad \text{und} \quad z = \frac{1}{\alpha + 1}\,!$$