Mathe für die Informatik I – WiSe 2019/20

Dr. Samuel Hetterich

Blatt 11 DM — Abgabe: Mo 27.01.2020, 10:15 Uhr

Hinweis:
▶ **Begründen Sie bitte alle Ihre Anworten! Unbegründete Anworten werden nicht bewertet. Rechnungen können Begründungen sein.**

Aufgabe 11.1 — 6 Punkte

a) Für das RSA-Verfahren sei der Modul $\mathsf{N} = p \cdot q$ mit Primfaktoren $p = 37$ und $q = 89$. Berechnen Sie den Dekodierschlüssel zum Schlüssel $\mathsf{e} = 103$ für den Modul N.

b) Entschlüsseln Sie die (bereits mit e verschlüsselte) Nachricht $m = 125$.

c) Erzeugen Sie zur Nachricht $a = 6$ und den Parametern aus a) eine RSA-Signatur (a, c) und zeigen Sie, dass diese Signatur gültig ist (sich mit Kenntnis von d verifizieren lässt).

Aufgabe 11.2 — 5 Punkte

Es seinen $p' = 34$ und $q' = 7$ und $e' = 3$ ein öffentlicher Schlüssel.

a) Wieviele mögliche öffentliche Schlüssel gibt es für das Modul $\mathsf{N}' = p' \cdot q'$?

b) Verschlüsseln Sie die Nachricht $a = 80$ mit dem Schlüssel e'.

c) Ein Angreifer greift 3-mal die selbe, aber verschiedenverschlüsselte Nachricht ab, wobei der öffentliche Schlüssel bei allen $e = 3$ ist. Die verschlüsselten Nachrichten der Form (c, N) lauten $(1, 4)$, $(6, 7)$ und $(8, 9)$. Mit Hilfe des chinesischen Restsatz kann die nicht verschlüsselte Nachricht zurück gewonnen werden.

$$\begin{aligned} c &\equiv 1 \pmod 4 \\ c &\equiv 6 \pmod 7 \\ c &\equiv 8 \pmod 9 \end{aligned}$$

Die nicht verschlüsselte Nachricht a berechnet sich aus $a = c^3 \pmod{4 \cdot 7 \cdot 9}$. Berechnen Sie a.

Zusatzaufgabe 11.3 Determinante — Für alle, die Spaß dran haben!

a) Geben Sie die Determinanten der folgenden Matrizen an:

$$A = \begin{pmatrix} 11 & 2 & 5 \\ 3 & 17 & 8 \\ 5 & 2 & 3 \end{pmatrix} \qquad B = \begin{pmatrix} 3 & 4 \\ 7 & 8 \end{pmatrix}$$

b) Entwickeln Sie die Determinante der Matrix $C = \begin{pmatrix} 0 & 1 & 2 & 0 \\ 5 & 0 & 2 & 1 \\ 1 & 3 & 2 & 6 \\ 1 & 0 & 1 & 3 \end{pmatrix}$

nach der ersten Zeile.

Zusatzaufgabe 11.4 Eigenwerte — Für alle, die Spaß dran haben!

Diagonalisieren Sie folgende Matrix:

$$A = \begin{pmatrix} 3 & -1 & 1 \\ -4 & 6 & 4 \\ -3 & 3 & 7 \end{pmatrix}$$

d.h. berechnen Sie eine Matrix $B \in \mathbb{R}^{3\times 3}$ und k_1,k_2,k_3 mit

$$A = B \cdot \begin{pmatrix} k_1 & 0 & 0 \\ 0 & k_2 & 0 \\ 0 & 0 & k_3 \end{pmatrix} \cdot B^{-1}$$