Vorlesung LinADi
Wintersemester 2022/23
Prof. Dr. Bastian von Harrach
M. Sc. Andrej Brojatsch
M. Sc. Stephan Gardoll

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

8. Übungsblatt
(Ausgabe am 07.12.2022, Abgabe ab 09.12.2022 12:00 Uhr bis 14.12.2022 12:00 Uhr)

Aufgabe 8.1 (RSA-Verfahren)[4 Punkte]

Es seien $p = 7, q = 11$ gegeben. Ferner wählen wir $e = 13$.

(a) Berechnen Sie $N = p \cdot q$, $\varphi(N)$ sowie den privaten Schlüssel d. Bitte geben Sie nur die Ergebnisse an.
(b) Übertragen Sie das Wort "hallo" gemäß untenstehender Tabelle in ein 5-Tupel von Zahlen $(x_1, \ldots, x_5)$ und verschlüsseln Sie $x_1, \ldots, x_5$ gemäß RSA-Verfahren unter Verwendung des öffentlichen Schlüssels. Bitte geben Sie nur das verschlüsselte 5-Tupel als Ergebnis an.
(c) Entschlüsseln Sie das Ergebnis aus Aufgabenteil (b) durch Verwendung des privaten Schlüssels.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Aufgabe 8.2 (RSA in der Praxis)[4 Punkte]

In der Praxis wird beim RSA-Verfahren darauf geachtet, dass die Primzahlen p und q eine unterschiedliche Größenordnung haben, um die Sicherheit des Verfahrens zu gewährleisten. Zeigen Sie, dass das Verfahren andernfalls unsicher wird, indem Sie für $N = 97343$ die Primzahlen p, q mit $N = p \cdot q$ bestimmen.

Aufgabe 8.3 (Vektorrechnung)[4 Punkte]

Es seien

$$u = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} v = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \; w = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \; x = \begin{pmatrix} 8 \\ 10 \end{pmatrix}, \; y = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \; z = \begin{pmatrix} 2 \\ 1 \\ 1 \\ 2 \end{pmatrix}, \; a = 5, \; b = 10.$$

Geben Sie die Ergebnisse zu den folgenden Operationen aus der Vektorrechnung an. Sollte die Operation nicht zulässig sein, geben Sie bitte "nicht definiert" als Ergebnis an.

(a) $x + v$, (d) $a + b$, (g) $a + v$, (j) $a \cdot y$, (m) $a \cdot u + v$,
(b) $w + u$, (e) $x + w$, (h) $a \cdot x$, (k) $u \cdot x$, (n) $y \cdot z$,
(c) $y + z$, (f) $u + y$, (i) $b \cdot u$, (l) $a \cdot y + b \cdot z$, (o) $a \cdot b$.

Aufgabe 8.4 (Vektorräume)[4 Punkte]

Zeigen Sie, dass es sich bei $(\mathbb{R}^2, +, *)$ um einen $\mathbb{R}$-Vektorraum handelt. Sie dürfen dabei verwenden, dass $\mathbb{R}$ ein Körper ist.