Prof. Dr.Werner Bley
Eva Brenner

17.10.2023

1. Übungsblatt Quantencomputing

Aufgabe 1 Studieren Sie im Protokoll zur Kryptographie die Abschnitte 1 - 3 bevor Sie die folgenden Aufgaben lösen.

Aufgabe 2 a) Die Gruppe $(\mathbb{Z}/19\mathbb{Z})^\times$ ist zyklisch. Bestimme ihre sämtlichen Erzeuger.
b) Berechne alle modulo 19 verschiedenen Lösungen $(x, y), x, y \in \mathbb{Z}$ des Kongruenzsystems

$$\begin{aligned} x^2 &\equiv 11 \pmod{19}, \\ xy &\equiv -1 \pmod{19}. \end{aligned}$$

(Anleitung: Sei w ein erzeugendes Element von $(\mathbb{Z}/19\mathbb{Z})^\times$. Setze an: $x = w^k, y = w^l$ mit $1 \leq k, l \leq 18$ und leite für k, l Kongruenzen modulo 18 her.)

Aufgabe 3
Die folgende Nachricht

68094034 128468343 143911297 122013244

wurde mit dem RSA-Verfahren mit den Parametern $N = 289648273$ und $e = 17$ verschlüsselt. Dabei wurde wie folgt vorgegangen: der alphanumerische Klartext wurde zu Gruppen von je 3 Buchstaben zusammengefasst. Jeder solchen Dreiergruppe xyz, $x, y, z \in \{A, B, \ldots, Z\}$ wurde die Zahl $W(xyz) := w(x) \cdot 26^2 + w(y) \cdot 26 + w(z) \bmod N$ zugeordnet, wobei

$$w : \{A, B, \ldots, Z\} \longrightarrow \{0, 1, \ldots, 25\}$$

jedem Buchstaben einen Wert anhand der Tabelle

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

zuordnet. $W(xyz) \in \mathbb{Z}/N\mathbb{Z}$ wurde dann mit RSA verschlüsselt.
Wie lautet die Nachricht?

Zu bearbeiten bis: Mi 25.10.2023