

Aufgabe 11: (4 Punkte)

Bestimmen Sie die Lösung $x \in \mathbb{Z}_{210}$ des folgenden Systems von Kongruenzen. Erläutern Sie Ihre Vorgehensweise!

$$\begin{aligned}x &= 3 \pmod{5} \\x &= 3 \pmod{6} \\x &= 2 \pmod{7}\end{aligned}$$

Aufgabe 12: (6 Punkte)

Sei $n = pq$, wobei $p \neq q$ jeweils ungerade Primzahlen sind. Bezeichne weiterhin $\mathbb{Z}_n^* := \{a \in \mathbb{Z}_n \mid \text{ggT}(a, n) = 1\} \subset \mathbb{Z}_n$ die Menge der zu n teilerfremden ganzen Zahlen a mit $0 < a < n$. Das Produkt n sei bekannt, die Faktoren p und q jedoch nicht.

- (a) Angenommen man kennt die Werte $c = m^e \pmod{n}$ und e mit $0 \leq e < \varphi(n)$, wobei man über m nur weiß, dass $m \in (\mathbb{Z}_n \setminus \mathbb{Z}_n^*)$ und $m \not\equiv 0 \pmod{n}$ ist.

Zeigen Sie, dass man dann aus c die Faktorisierung von n (also p und q) effizient berechnen kann (Hinweis: Dies ist lösbar in Laufzeit $\mathcal{O}(\log_2^2(n))$).

- (b) Sie wählen ein $m \in \mathbb{Z}_n$ zufällig gleichverteilt. Mit welcher Wahrscheinlichkeit gilt dann $m \in (\mathbb{Z}_n \setminus \mathbb{Z}_n^*)$? Geben Sie einen Näherungswert für diese Wahrscheinlichkeit an, wenn man annimmt, dass p und q beide jeweils 512 Bit Länge besitzen.

Aufgabe 13: (8 Punkte)

Der öffentliche Schlüssel beim Rucksack-Verfahren sei die Gewichtsfolge

$$w' = (1394, 1256, 1508, 1987, 439, 650, 724, 339, 2303, 810)$$

Angenommen, ein Angreifer hat erfahren, dass $n = 2503$ benutzt wird, d.h. es gilt

$$w'_i = w_{\pi_i} \cdot k \pmod{2503}, \quad 1 \leq i \leq 10$$

für ein $k \in \mathbb{Z}_n^*$ und eine Permutation π auf der Menge $\{1, \dots, 10\}$.

- (a) Finden Sie durch Ausprobieren einen Wert $k \in \mathbb{Z}_n^*$, so dass die durch $w_i = w'_i \cdot k^{-1} \pmod{n}$ definierte Gewichtsfolge eine Permutation einer superwachsenden Folge ist. Sie können dazu z.B. ein kurzes Programm schreiben, das aber nicht abgegeben werden muss. Erläutern Sie kurz das Vorgehen Ihres Programms und bestimmen Sie die Werte k , $k^{-1} \pmod{n}$ und die (aufsteigend sortierte) superwachsende Folge w .
- (b) Wie lässt sich die zur Entschlüsselung benötigte Permutation π bestimmen? Wie lautet sie?
- (c) Entschlüsseln Sie $C = 3243$.