Übungen zur Kryptologie

Blatt 9 SoS 2024 — H. Kiechle

Präsenzaufgaben

26. Gegeben sei eine Gruppe G und $g \in G$. Wie viele Gruppenoperationen (Multiplikationen) müssen Sie ausführen um g^N, $N \in \mathbb{N}$, zu berechenen? Überlegen Sie sich dazu, wie Sie das bei den vergangenen Übungsaufgaben gemacht haben.

Ist dieser (naive) Algorithmus polynomial?

Hausaufgaben

27. Wir rechnen in der Gruppe $\left(\mathbb{Z}_{53}^{\times}, \cdot\right)$. [16 Punkte]

(a) Bestimmen Sie $\overline{3}^{2^k}$ für $k \in \{0, 1, 2, 3, 4\}$ möglichst effizient.

(b) Wieviele Multiplikationen sind dazu jeweils nötig (abhängig von k).

(c) Berechnen Sie $\overline{3}^{13}$ und dann $\overline{3}^{52}$.

Anleitung: Stellen Sie 13 im Binärsystem dar und nutzen Sie die Ergebnisse aus Teilaufgabe (a) zusammen mit den Potenzrechengesetzen.

(d) Wieviele Multiplikationen sind dazu insgesamt nötig?

Vergleichen Sie mit dem naiven Algorithmus.

(e) Beschreiben Sie einen Algorithmus, der dieses Verfahren auf beliebige Gruppen und Exponenten verallgemeinert. Ist dieser Algorithmus polynomial?

28. Es sei F ein Körper. [8 Punkte]

Wie viele Elemente der Ordnung 2 gibt es in der Gruppe $F \setminus \{0\}$ (mit Beweis) ?

Hinweis: Ein solches Element ist Nullstelle des Polynoms $x^2 - 1$. Warum?