Übungen zur Kryptologie

Blatt 10 SoS 2024 — H. Kiechle

Präsenzaufgaben

29. *Diffie-Hellman-Schlüsselaustausch*

Gegeben sei die zyklische Gruppe $\mathbb{Z}_{31}^{\times}$ und das Erzeugende $\overline{3}$.

(a) Ermitteln Sie eine fünfstellige Binärzahl N durch Münzwurf (oder ähnlich; in jedem Fall zufällig und gleichverteilt).

(b) Berechnen Sie $A := (\overline{3})^N$ und erzeugen Sie mit einer Ihrer Nachbar*innen einen gemeinsamen (geheimen?) Schlüssel.

30. Wahr oder falsch?

(a) Die Anzahl der Ziffern einer Zahl N im 12-er System ist $\lfloor \log_{12} N \rfloor + 1$.

(b) Die übliche Division mit Rest ist ein exponentieller Algorithmus.

(c) Jede zyklische Gruppe ist kommutativ.

(d) Jede kommutative Gruppe ist zyklisch.

Hausaufgaben

31. *Der Satz von Euler*

Sei G eine endliche Gruppe mit $|G| = n$. Beweisen Sie für alle $a \in G$

(a) $a^n = e$;

(b) für $m \equiv 1 \mod n$ gilt $a^m = a$;

(c) Wie kann man a^{-1} durch Potenzieren ermitteln?

32. Setzen Sie Ihr eigenes RSA-System auf. (Bezeichnungen wie in der Vorlesung)

(a) Wählen Sie (möglichst zufällig) zwei 6 Bit Primzahlen und berechnen Sie n.

(b) Bestimmen Sie zu $e = 17$ das passende d.

(c) Stellen Sie 17 als Binärzahl dar. Welchen Vorteil bietet die Wahl $e = 17$?

(d) Bestimmen Sie alle sicheren 6-Bit Primzahlen.