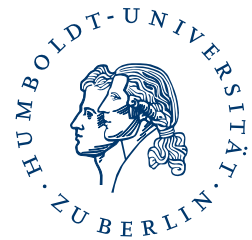
Einführung in die Kryptologie

Johannes Köbler



Institut für Informatik
Humboldt-Universität zu Berlin

SS 2022

Zahlentheoretische Grundlagen

Für das Verständnis der Public-Key Verfahren benötigen wir noch einige Hilfsmittel aus der Zahlentheorie

Definition. Sei G eine endliche Gruppe.

- Die Ordnung von G ist die Anzahl $|G|$ ihrer Elemente
- Die Ordnung eines Elements $a \in G$ ist $\mathrm{ord}_G(a) = \min\{n \geq 1 \mid a^n = 1\}$
- Ist $G = \mathbb{Z}_m^*$, so schreiben wir einfach $\mathrm{ord}_m(a)$ anstelle von $\mathrm{ord}_{\mathbb{Z}_m^*}(a)$
- Die von a in G erzeugte Untergruppe $\{a^0, \ldots, a^{\mathrm{ord}_G(a)-1}\}$ bezeichnen wir mit $\langle a \rangle_G$ oder mit $\langle a \rangle$, wenn G aus dem Kontext ersichtlich ist

- Sei $e \geq 1$ der kleinste Exponent mit $a^e = a^{e'}$ für ein $e' \in \{0, \ldots, e-1\}$
- Dann gilt $a^i \neq a^j$ für alle $0 \leq i < j < e$ und wegen $a^{e-e'} = a^e a^{-e'} = a^e a^{-e} = 1 = a^0$ muss $e - e' = e$, also $e' = 0$ sein
- Dies zeigt, dass $\mathrm{ord}_G(a) = e$ ist und die Menge $\{a^0, \ldots, a^{\mathrm{ord}_G(a)-1}\}$ tatsächlich eine Untergruppe von G der Ordnung $\mathrm{ord}_G(a)$ bildet