

## 2.6 Brechen eines Geheimtextes

Das Brechen von Geheimtexten könnte aber noch leichter sein: Für einen gegebenen Geheimtext  $c$  könnte nämlich  $E_e^r(c) = c$  sein, obwohl  $E_e^r \neq \mathbf{1}_M$  ist. Ist dann  $m$  der Klartext, also  $c = E_e(m)$ , so kann der Kryptoanalytiker berechnen:

$$E_e^{r-1}(c) = D_e(E_e^r(c)) = D_e(c) = m.$$

Die mathematische Beschreibung dieser Situation sieht so aus:

- $\mathbb{M}_{\lambda(n)}$  operiert auf der Menge  $M = \mathbb{Z}/n\mathbb{Z}$ , ebenso die zyklische Untergruppe  $G := \langle e \rangle \leq \mathbb{M}_{\lambda(n)}$ .
- Für  $m \in M$  ist  $G \cdot m = \{m^{e^k} \mid 0 \leq k < s\}$  die Bahn.
- Der Stabilisator  $G_m = \{f \in G \mid m^f \equiv m \pmod{n}\}$  ist Untergruppe von  $G$ ; zwischen den Mengen  $G \cdot m$  und  $G/G_m$  gibt es eine natürliche Bijektion.
- Für die Bahnlänge  $t = \#G \cdot m$  gilt

$$t = \frac{s}{\#G_m}, \quad t|s|\lambda(\lambda(n))$$

$$E_e^r(c) = c \iff E_e^r(m) = m \iff t|r.$$

- $G \cdot c = G \cdot m$  und  $\#G_c = \#G_m$ . (Die beiden Stabilisatoren sind zueinander konjugiert.)

Damit sind wir auf ein weiteres Problem gestoßen:

3. Wann ist  $t = s$ , d. h., der Stabilisator  $G_m$  trivial? Oder zumindest sehr klein?

Antwort auch hier: meistens.

Das Finden der Bahnlänge  $t$  von  $m$  und  $c$  ist also mindestens so schwierig wie das Brechen des Geheimtextes  $c$ .