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 a der Klartext, also $c = E_e(a)$, so kann der Kryptoanalytiker berechnen:

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

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 $a \in M$ ist $G \cdot a = \{a^{e^k} \mid 0 \leq k < s\}$ die Bahn.
- Der Stabilisator $G_a = \{f \in G \mid a^f \equiv a \pmod{n}\}$ ist Untergruppe von G; zwischen den Mengen $G \cdot a$ und G/G_a gibt es eine natürliche Bijektion.
- Für die Bahnlänge $t = \#G \cdot a$ gilt

$$t = \frac{s}{\#G_a}, \qquad t|s|\lambda(\lambda(n))$$
$$E_e^r(c) = c \iff E_e^r(a) = a \iff t|r.$$

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

Damit sind wir auf ein weiteres Problem gestoßen:

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

   Antwort auch hier: meistens.

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

Zwei neuere Artikel zeigen, wie gering das Risiko ist, versehentlich eine kleine Bahnlänge zu erwischen und somit den Iterationsangriff zu ermöglichen:

- J. J. Brennan/ Bruce Geist, Analysis of iterated modular exponentiation: The orbits of x^α mod N. **Designs, Codes and Cryptography** 13 (1998), 229–245.
- John B. Friedlander/ Carl Pomerance/ Igor E. Shparlinski, Period of the power generator and small values of Carmichael's function. **Mathematics of Computation** 70 (2001), 1591–1606, + 71 (2002), 1803–1806.