3.6 RSA und Pseudoprimzahlen

Das für die Anwendbarkeit des RSA-Verfahrens grundlegende Problem, wie man Primzahlen findet, wird durch den probabilistischen RABIN-Test zwar hocheffizient, aber nicht restlos befriedigend gelöst: Was passiert, wenn man eine „falsche“ Primzahl erwischt?

Sei dazu $n = pq$ ein vermeintlicher RSA-Modul, für den p und q nicht notwendig Primzahlen – aber zueinander teilerfremd – sind. Bei der Konstruktion der Schlüssel d, e mit

$$de \equiv 1 \pmod{\tilde{\lambda}(n)}$$

werden dann statt der wahren Werte $\varphi(n)$ und $\lambda(n)$ für EULER- und CARMICHAEL-Funktion die möglicherweise davon abweichenden Werte

$$\tilde{\varphi}(n) := (p-1)(q-1), \quad \tilde{\lambda}(n) := \mathrm{kgV}(p-1, q-1)$$

verwendet.

Funktioniert das RSA-Verfahren noch? Sei $a \in \mathbb{Z}/n\mathbb{Z}$ ein Klartext. Der Fall $\mathrm{ggT}(a,n) > 1$ führt – wie auch sonst – zur Faktorisierung des Moduls und wird hier – wie auch sonst – wegen seiner extrem geringen Wahrscheinlichkeit ignoriert. Andernfalls ist $\mathrm{ggT}(a,n) = 1$, und zu fragen ist, ob

$$a^{de-1} \stackrel{?}{\equiv} 1 \pmod{n}$$

gilt. Nun, das ist nach dem chinesischen Restsatz genau dann der Fall, wenn

$$a^{de-1} \equiv 1 \pmod{p} \quad \text{und} \quad \pmod{q}$$

ist. Hinreichend dafür ist

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{und} \quad a^{q-1} \equiv 1 \pmod{q};$$

d. h., eine Nachricht a wird höchstens dann nicht korrekt entschlüsselt, wenn p oder q nicht pseudoprim zur Basis a ist. Also:

- Verwendet man statt einem Primfaktor p eine CARMICHAEL-Zahl, funktioniert das RSA-Verfahren trotz der „falschen“ Parameter korrekt, wenn a zu n teilerfremd ist; allerdings ist die (extrem geringe) Wahrscheinlichkeit, durch einen Klartext a, der nicht zu n teilerfremd ist, zufällig den Modul n zu faktorisieren, geringfügig vergrößert.
- Andernfalls – falls p weder prim noch eine CARMICHAEL-Zahl ist –, gibt es eine geringe Chance, dass eine Nachricht nicht korrekt entschlüsselt werden kann.

Aus diesem Grund werden bei vielen Implementierungen des RSA-Verfahrens nach der Schlüsselerzeugung – wenn der probabilistische Primzahltest von RABIN eingesetzt wird – ein paar Probever- und -entschlüsselungen durchgeführt; das entspricht aber auch nur ein paar zusätzlichen Pseudoprimzahltests. Geht dabei etwas schief, wird der Modul verworfen. Es ist nicht bekannt, ob dieser Fall schon einmal eingetreten ist.