2.7 Mehrfach-Verwendung eines Moduls

Frage: Was passiert, wenn beim RSA-Verfahren zwei verschiedene Teilnehmer denselben Modul n verwenden?

D. h., A und B haben die öffentlichen Schlüssel (n, e_A) und (n, e_B).

Zunächst sind offensichtlich A und B voreinander nicht sicher, da beide n faktorisieren, also auch den geheimen Schlüssel des jeweils anderen bestimmen können. Ein gemeinsamer Modul ist also höchstens in einer Kooperationssituation sinnvoll, wo A und B einander uneingeschränkt vertrauen.

Es kommt aber noch schlimmer: Falls jemand die gleiche Nachricht a an A und B schickt, kann *jeder* diese entschlüsseln. Die Geheimtexte sind:

$$c_\mathrm{A} = a^{e_\mathrm{A}} \bmod n, \quad c_\mathrm{B} = a^{e_\mathrm{B}} \bmod n.$$

Unter der nicht wesentlich einschränkenden Annahme, dass e_A und e_B teilerfremd sind, findet eine Angreiferin mit dem erweiterten EUKLIDischen Algorithmus Koeffizienten x und y mit

$$xe_\mathrm{A} + ye_\mathrm{B} = 1;$$

dabei haben x und y notwendigerweise verschiedenes Vorzeichen, o. B. d. A. $x < 0$. Ist $\mathrm{ggT}(c_\mathrm{A}, n) > 1$, so kann die Angreiferin n faktorisieren und ist fertig. Andernfalls bestimmt sie

$$g := c_\mathrm{A}^{-1} \bmod n$$

durch Kongruenzdivision (also wieder mit dem EUKLIDischen Algorithmus) und hat dann

$$g^{-x} \cdot c_\mathrm{B}^{y} \equiv (a^{e_\mathrm{A}})^x \cdot (a^{e_\mathrm{B}})^y \equiv a \pmod{n}.$$

Die geheimen Schlüssel d_A und d_B hat sie damit allerdings nicht bestimmt.

Der gemeinsame Modul n ist also nur sicher, wenn A und B sich voll vertrauen und diesen Modul außerdem geheim halten. Dann können sie nur miteinander kommunizieren – und da ist es viel effizienter, gleich eine symmetrische Chiffre zu verwenden.