

2.2 Schlüsselbestimmung und Faktorisierung

Frage: *Wie kann man beim RSA-Verfahren den geheimen Exponenten d aus dem öffentlichen Exponenten e und dem Modul n bestimmen?*

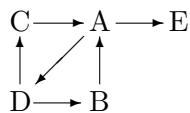
Antwort: Jede der folgenden Aufgaben lässt sich effizient auf die anderen zurückführen:

- (A) Finden eines passenden geheimen Schlüssels d .
- (B) Bestimmung von $\lambda(n)$ (CARMICHAEL-Funktion).
- (C) Bestimmung von $\varphi(n)$ (EULER-Funktion).
- (D) Faktorisierung von n .

Das Brechen von RSA ist die (möglicherweise echt) leichtere Aufgabe:

- (E) Ziehen von e -ten Wurzeln in $\mathbb{Z}/n\mathbb{Z}$.

Der Beweis folgt dem Schema:



Sei dazu $n = p_1 \cdots p_r$ mit verschiedenen Primzahlen p_1, \dots, p_r . Es wird stets angenommen, dass außer n auch der „öffentliche“ Exponent e bekannt ist.

Es ist klar, dass „ $A \rightarrow E$ “ gilt: Wenn d bekannt ist, zieht man die e -te Wurzel durch Potenzieren mit d . Die Umkehrung ist hier allerdings nicht bekannt: *Es könnte sein, dass das Brechen von RSA leichter als die Faktorisierung ist.*

„ $D \rightarrow C$ “: $\varphi(n) = (p_1 - 1) \cdots (p_r - 1)$.

„ $D \rightarrow B$ “: $\lambda(n) = \text{kgV}(p_1 - 1, \dots, p_r - 1)$.

„ $B \rightarrow A$ “: d wird durch Kongruenzdivision aus $de \equiv 1 \pmod{\lambda(n)}$ gewonnen.

„ $C \rightarrow A$ “: Da $\varphi(n)$ genau die gleichen Primfaktoren hat wie $\lambda(n)$, ist e auch zu $\varphi(n)$ teilerfremd. Durch Kongruenzdivision aus $de \equiv 1 \pmod{\varphi(n)}$ wird ein Exponent d gewonnen, der nicht der „echte“ ist, aber genauso als geheimer Schlüssel funktioniert, da auch $de \equiv 1 \pmod{\lambda(n)}$.

„ $A \rightarrow D$ “ ist wesentlich komplizierter zu zeigen; es wird auch nur ein probabilistischer Algorithmus konstruiert.

Vorbemerkungen

1. *Es reicht, n in zwei echte Faktoren zu zerlegen.*

(a) Ist nämlich $n = n_1 n_2$ eine solche Zerlegung und o. B. d. A. $n_1 = p_1 \cdots p_s$ mit $1 < s < r$ so ist

$$\lambda(n_1) = \text{kgV}(p_1 - 1, \dots, p_s - 1) \mid \text{kgV}(p_1 - 1, \dots, p_r - 1) = \lambda(n),$$

also auch $de \equiv 1 \pmod{\lambda(n_1)}$. Also ist das Problem auf das analoge für n_1 und n_2 reduziert.

(b) Da die Zahl der Primfaktoren von n höchstens $2 \log(n)$ ist, ist die dadurch gegebene rekursive Reduktion effizient.

2. *Wie kann eine zufällig gewählte Restklasse $w \in \mathbb{Z}/n\mathbb{Z}$ bei der Faktorisierung von n helfen?*

(a) Findet man ein $w \in [1 \dots n - 1]$ mit $\text{ggT}(w, n) > 1$, so ist n faktorisiert, da $\text{ggT}(w, n)$ ein echter Teiler von n ist.

(b) Findet man ein $w \in [2 \dots n - 2]$ mit $w^2 \equiv 1 \pmod{n}$ (also eine nichttriviale Quadratwurzel aus 1 in $\mathbb{Z}/n\mathbb{Z}$), so ist n ebenfalls faktorisiert:

Da $n \mid w^2 - 1 = (w+1)(w-1)$ und $n \nmid w \pm 1$, ist $\text{ggT}(n, w+1) > 1$, also n nach 1. faktorisiert.

Sei also jetzt ein Paar (d, e) von zusammengehörigen Exponenten bekannt. Dann ist auch $u := ed - 1 = k \cdot \lambda(n)$ bekannt (k und $\lambda(n)$ allerdings nicht).

Da $\lambda(n)$ gerade ist, ist

$$u = r \cdot 2^s \quad \text{mit } s \geq 1 \text{ und } r \text{ ungerade.}$$

Wählt man irgendein $w \in [1 \dots n - 1]$, so gibt es zwei Möglichkeiten:

- $\text{ggT}(w, n) > 1$ – dann ist n faktorisiert.
- $\text{ggT}(w, n) = 1$ – dann ist $w^{r2^s} \equiv 1 \pmod{n}$.

Im zweiten Fall findet man effizient das minimale $t \geq 0$ mit

$$w^{r2^t} \equiv 1 \pmod{n}.$$

Es gibt wieder zwei Fälle:

- $t = 0$ – Pech gehabt.
- $t > 0$ – dann ist $w^{r2^{t-1}}$ eine Quadratwurzel $\neq 1$ aus 1 in $\mathbb{Z}/n\mathbb{Z}$.

Im zweiten Fall wird unterschieden:

- $w^{r2^{t-1}} \equiv -1 \pmod{n}$ – Pech gehabt.
- $w^{r2^{t-1}} \not\equiv -1 \pmod{n}$ – dann ist n nach Vorbemerkung 2 faktorisiert.

Insgesamt haben wir bei diesem Verfahren nach beliebiger Wahl von $w \in [1 \dots n - 1]$ vier Ausgänge, zwei, bei denen n faktorisiert wird, und zwei, bei denen dies nicht der Fall ist. Die letzteren werden mit

$$\begin{aligned} (\mathbb{E}_{n,u}(w)/\text{I}) \quad w^r &\equiv 1 \pmod{n} \quad \text{und} \\ (\mathbb{E}_{n,u}(w)/\text{II}) \quad w^{r2^t} &\equiv -1 \pmod{n} \quad \text{für ein } t \text{ mit } 0 \leq t < s \end{aligned}$$

bezeichnet. Insgesamt ergibt sich die Baumstruktur:

$$\begin{aligned} w \in [1 \dots n - 1] &\longrightarrow \\ \text{ggT}(w, n) > 1 &\longrightarrow n \text{ faktorisiert. } \diamond \\ w \in \mathbb{M}_n &\longrightarrow \\ w^r &\equiv 1 \pmod{n} \longrightarrow (\mathbb{E}_{n,u}(w)/\text{I.}) \diamond \\ w^r &\not\equiv 1 \pmod{n} \longrightarrow \\ w^{r2^t} &\equiv -1 \pmod{n} \longrightarrow (\mathbb{E}_{n,u}(w)/\text{II.}) \diamond \\ w^{r2^t} &\not\equiv -1 \pmod{n} \longrightarrow n \text{ faktorisiert. } \diamond \end{aligned}$$

Wir können also n „mit hoher Wahrscheinlichkeit“ faktorisieren, wenn es nur „wenige“ solcher „schlechten“ Zahlen mit $(\mathbb{E}_{n,u}(w)/\text{I,II})$ gibt. Wie viele es sind, wird im nächsten Abschnitt untersucht.