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: Ist eine der folgenden Aufgaben effizient lösbar, so auch die anderen:

(A) Finden des geheimen Schlüssels d.

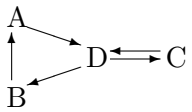
(B) Bestimmung von $\lambda(n)$ (CARMICHAEL-Funktion).

(C) Bestimmung von $\varphi(n)$ (EULER-Funktion).

(D) Faktorisierung von n.

Genauer gesagt, wird die Faktorisierung aus den anderen Aufgaben nur für den Fall hergeleitet, dass n ein Produkt von zwei Primzahlen ist. Ansonsten wird n als quadratfrei, $n = p_1 \cdots p_r$ mit verschiedenen Primzahlen p_1, $\ldots$, p_r vorausgesetzt.

Der Beweis folgt dem Schema:



Das Brechen von RSA ist die Aufgabe:

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

Es ist klar, dass „A $\longrightarrow$ 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 $\longrightarrow$ C“: $\varphi(n) = (p_1 - 1) \cdots (p_r - 1)$.

„D $\longrightarrow$ B“: $\lambda(n) = \mathrm{kgV}(p_1 - 1, \ldots, p_r - 1)$.

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

„C $\longrightarrow$ D“: [Nur, wenn $n = pq$ Produkt von zwei Primfaktoren] Da $\varphi(n) = (p-1)(q-1) = n - (p+q) + 1$, ist $p + q = n + 1 - \varphi(n) =: t$ bekannt. Da ferner $p \cdot q = n$, ergibt sich für p die quadratische Gleichung $p \cdot (t - p) = n$, also

$$p^2 - tp + n = 0,$$

mit der Lösung

$$p = \frac{1}{2} \cdot (t + \sqrt{t^2 - 4n}), \qquad q = t - p.$$

Ist n Produkt von mehr als zwei Primfaktoren, so ist $\varphi(n)$ die alternierende Summe der elementarsymmetrischen Funktionen der Primfaktoren, aber damit ist nicht ohne weiteres etwas anzufangen.

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

Vorbemerkungen

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

1. Findet man ein $w \in [1 \ldots n-1]$ mit $\mathrm{ggT}(w, n) > 1$, so ist n faktorisiert, da $\mathrm{ggT}(w, n)$ ein echter Teiler von n ist.
2. Findet man ein $w \in [2 \ldots n-2]$ 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 $n | w^2 - 1 = (w+1)(w-1)$ und $n \nmid w \pm 1$, ist $\mathrm{ggT}(n, w+1) > 1$, 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

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

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

- $\mathrm{ggT}(w, n) > 1$ – dann ist n faktorisiert.
- $\mathrm{ggT}(w, n) = 1$ – 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 $w \in [1 \ldots n-1]$ vier Ausgänge, zwei, bei denen n faktorisiert wird, und zwei, bei denen dies nicht der Fall ist. Die letzteren werden mit

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

bezeichnet. Insgesamt ergibt sich die Baumstruktur:

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

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