1.4 Geeignete RSA-Parameter

Satz 3 *Für eine natürliche Zahl $n \geq 3$ sind äquivalent:*

(i) *n ist quadratfrei.*

(ii) *Es gibt ein $r \geq 2$ mit $a^r \equiv a \pmod{n}$ für alle $a \in \mathbb{Z}$.*

(iii) **[RSA-Gleichung]** *Für jedes $d \in \mathbb{N}$ und $e \in \mathbb{N}$ mit $de \equiv 1 \pmod{\lambda(n)}$ gilt $a^{de} \equiv a \pmod{n}$ für alle $a \in \mathbb{Z}$.*

(iv) *Für jedes $k \in \mathbb{N}$ gilt $a^{k \cdot \lambda(n)+1} \equiv a \pmod{n}$ für alle $a \in \mathbb{Z}$.*

Beweis. „(iv) $\Longrightarrow$ (iii)“: Da $de \equiv 1 \pmod{\lambda(n)}$, ist $de = k \cdot \lambda(n) + 1$ für ein geeignetes k. Also ist $a^{de} \equiv a \pmod{n}$ für alle $a \in \mathbb{Z}$.

„(iii) $\Longrightarrow$ (ii)“: Da $n \geq 3$, ist $\lambda(n) \geq 2$. Wählt man d beliebig mit $\mathrm{ggT}(d, \lambda(n)) = 1$ und e dazu passend mittels Kongruenzdivision $\mathrm{mod}\lambda(n)$, so ist (ii) erfüllt mit $r = de$.

„(ii) $\Longrightarrow$ (i)“: Gäbe es eine Primzahl p mit $p^2|n$, so müsste nach (ii) $p^r \equiv p \pmod{p^2}$ gelten. Da $r \geq 2$, ist aber $p^r \equiv 0 \pmod{p^2}$, Widerspruch.

„(i) $\Longrightarrow$ (iv)“: Nach dem chinesischen Restsatz reicht es zu zeigen, dass $a^{k \cdot \lambda(n)+1} \equiv a \pmod{p}$ für alle Primfaktoren $p|n$.

1. Fall: $p|a$. Dann ist $a \equiv 0 \equiv a^{k \cdot \lambda(n)+1} \pmod{p}$.

2. Fall: $p \nmid a$. Da $p - 1|\lambda(n)$, ist $a^{\lambda(n)} \equiv 1 \pmod{p}$, also $a^{k \cdot \lambda(n)+1} \equiv a \cdot (a^{\lambda(n)})^k \equiv a \pmod{p}$. $\diamond$

Korollar 1 *Das RSA-Verfahren ist mit einem Modul n genau dann durchführbar, wenn n quadratfrei ist.*

Um passende Exponenten d und e zu finden, muss man $\lambda(n)$ kennen, also am besten (und wie sich zeigen wird, sogar notwendigerweise) die Primzerlegung von n.

Damit wird folgendes Verfahren zur Schlüsselerzeugung nahegelegt:

1. Wahl von verschiedenen Primzahlen $p_1, \ldots, p_r$; Bildung des Moduls $n := p_1 \cdots p_r$.
2. Bestimmung von $\lambda(n) = \mathrm{kgV}(p_1 - 1, \ldots, p_r - 1)$ mit dem EUKLIDischen Algorithmus.
3. Wahl eines öffentlichen Exponenten $e \in \mathbb{N}_2$, teilerfremd zu $\lambda(n)$, insbesondere e ungerade.
4. Bestimmung des privaten Exponenten d mit $de \equiv 1 \pmod{\lambda(n)}$ durch Kongruenzdivision.

Als öffentlicher Schlüssel wird das Paar (n, e) genommen, als privater Schlüssel der Exponent d.

Korollar 2 *Wer die Primzerlegung von n kennt, kann aus dem öffentlichen Schlüssel (n, e) den privaten Schlüssel d bestimmen.*

Praktische Erwägungen

1. Man wählt so gut wie immer $r = 2$, hat also nur zwei, dafür aber sehr große Primfaktoren p und q. Solche Zahlen $n = pq$ sind besonders schwer zu faktorisieren. Die Primfaktoren sollen außerdem zufällig gewählt, also besonders schwer zu erraten sein. Mehr dazu später.

2. Für e kann man eine Primzahl wählen mit $e \nmid \lambda(n)$ oder eine „kleine“ Zahl ab $e = 3$ – mehr dazu später.

   Eine verbreitete Standard-Wahl ist die Primzahl $e = 2^{16} + 1$, sofern $\nmid \lambda(n)$. Da diese Zahl nur zwei Einsen in ihrer Binärdarstellung hat, ist das binäre Potenzieren für die Verschlüsselung besonders effizient. (Bei der digitalen Signatur ist dies das Verfahren der Signaturprüfung.) Für die Entschlüsselung (bzw. die Erzeugung einer digitalen Signatur) bringt eine solche Wahl von e allerdings keinen Effizienzvorteil.

3. p, q und $\lambda(n)$ werden nach der Schlüsselerzeugung nicht mehr benötigt, könnten also eigentlich vergessen werden.

   Aber: Da d eine „zufällige“ Zahl im Bereich $[1 \dots n]$ ist, ist das binäre Potenzieren mit d aufwendig. Zur Erleichterung kann die Besitzerin des privaten Schlüssels $c^d \bmod p$ und $\bmod q$ rechnen – also mit nur etwa halb so langen Zahlen – und das Ergebnis $\bmod n$ mit dem chinesischen Restsatz zusammensetzen. Dadurch ergibt sich ein kleiner Geschwindigkeitsvorteil bei der Entschlüsselung (bzw. der Erstellung einer digitalen Signatur).

4. Statt $\lambda(n)$ kann man für die Bestimmung der Exponenten auch das Vielfache $\varphi(n) = (p-1)(q-1)$ verwenden.

   Vorteil: Man spart sich (einmal) die kgV-Bestimmung.

   Nachteil: Der Exponent d wird im allgemeinen größer, und das wirkt sich bei jeder Entschlüsselung aus.

5. Trotz des obigen Korollars 1 kann man das RSA-Verfahren auch durchführen, wenn der Modul n nicht quadratfrei ist – der Entschlüsselungsschritt ist etwas komplizierter, da noch ein zusätzlicher „Hensel-Lift“ zwischengeschaltet werden muss. Außerdem geht die Entschlüsselung schief, wenn der Klartext a ein Vielfaches einer Primzahl p mit $p^2 | n$ ist. [D. h., es gibt keinen Widerspruch zum Korollar 1!] Die Gefahr, dass ein Klartext Vielfaches eines Primfaktors von n ist wird stets vernachlässigt; auch für einen quadratfreien Modul n würde ein solcher Klartext ja sofort zur Faktorisierung von n und somit zur Bestimmung des privaten Schlüssels führen.

Achtung

Die kryptoanalytischen Ansätze im folgenden Abschnitt ergeben eine Reihe von Nebenbedingungen, die für die Sicherheit des RSA-Verfahrens bei der Schlüsselerzeugung beachtet werden müssen.

Übungsaufgaben

1. Sei $n = p^2q$ mit zwei verschiedenen ungeraden Primzahlen p und q. Für welche $a \in \mathbb{Z}/n\mathbb{Z}$ gilt die RSA-Gleichung $a^{de} \equiv a \pmod{n}$? Verallgemeinerung auf beliebige n?

2. Zeige, dass $d \in \mathbb{N}$ genau dann zu $\lambda(n)$ teilerfremd ist, wenn es zu $\varphi(n)$ teilerfremd ist.