RSA: Sicherheit

Wie sicher ist die RSA-Methode?

Es gibt drei Probleme, deren Lösbarkeit dazu führen würde, dass das RSA-Verfahren nicht mehr sicher wäre:

- Faktorisiere n
- Berechne $\varphi(n)$
- Finde s mit $es \equiv 1 \bmod \varphi(n)$

Zur Zeit ist von allen diesen Problemen nicht klar, wie komplex sie tatsächlich sind. Aber man kann zeigen, dass die effiziente Lösung einer der drei Aufgaben ebenso effiziente Lösungen der anderen beiden nach sich zieht.

RSA: Sicherheit (Forts.)

Wenn man n faktorisieren kann, hat man Kenntnis von p und q. Damit ist es leicht, $\varphi(n) = (p-1)(q-1)$ zu berechnen und anschließend mit dem Euklidischen Algorithmus s zu ermitteln.

Wenn man $\varphi(n)$ finden kann, berechnet man den Wert $p + q = n - \varphi(n) + 1$ und kann daraus leicht p und q, und im Anschluss wieder s rekonstruieren.

Man kann zeigen, dass auch die Kenntnis von s ausreicht, um n zu faktorisieren und $\varphi(n)$ zu berechnen.

Obwohl die Komplexität dieser drei Probleme zur Zeit nicht bekannt ist, kann man nach heutigem Stand davon ausgehen, dass für n in der Größenordnung 2^{2000} alle drei Probleme praktisch unlösbar sind. Daher gilt RSA mit 300-stelligen Primzahlen p und q als sicher.

Eulers φ-Funktion

Als *Einheit* in einem Ring bezeichnet man ein Element, das ein Inverses bzgl. der Multiplikation in diesem Ring besitzt.

Wir interessieren uns jetzt speziell für die Einheiten im Restklassenring $\mathbb{Z}/n\mathbb{Z}$ (vgl. Folien 26.2 und 26.3).

Die multiplikative Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$ des Rings $\mathbb{Z}/n\mathbb{Z}$ besteht aus den Einheiten von $\mathbb{Z}/n\mathbb{Z}$. Ihre Größe ist $\varphi(n)$.

In anderen Worten:

> $\varphi(n)$ ist die Anzahl der natürlichen Zahlen $k < n$, für die $\text{ggT}(k, n) = 1$ gilt.

Beispiele

Wir berechnen für $n = 2, 3, 4, \ldots, 20$ die Werte $\varphi(n)$:

$\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$
$\varphi(7) = 6$, $\varphi(8) = 4$, $\varphi(9) = 6$, $\varphi(10) = 4$, $\varphi(11) = 10$
$\varphi(12) = 4$, $\varphi(13) = 12$, $\varphi(14) = 6$, $\varphi(15) = 8$, $\varphi(16) = 8$
$\varphi(17) = 16$, $\varphi(18) = 6$, $\varphi(19) = 18$, $\varphi(20) = 8$

Wenn n eine Primzahl ist, sind alle natürlichen Zahlen $k < n$ teilerfremd zu n. Also ist $\varphi(p) = p - 1$ für jede Primzahl p.
Ist umgekehrt $\varphi(n) = n - 1$, dann hat n offenbar keinen Teiler, also gilt:

$$\varphi(n) = n - 1 \quad \Longleftrightarrow \quad n \text{ ist Primzahl}$$

Zwei Spezialfälle

Motiviert durch das RSA-Verfahren fragen wir nach $\varphi(n)$ für den Fall, dass $n = pq$ das Produkt zweier Primzahlen ist:

Von 1 bis $n-1$ sind alle Zahlen teilerfremd zu n außer denen, die durch p oder durch q teilbar sind. Genau $q-1$ dieser Zahlen sind durch p teilbar, und genau $p-1$ sind durch q teilbar. Prüfen!!

Keine ist durch p und q teilbar!

Also gilt $\varphi(pq) = pq - 1 - (q-1) - (p-1) = (p-1)(q-1)$

Und was ist $\varphi(p^e)$ für eine Primzahl p und $e \geq 1$?

Von den $p^e - 1$ Zahlen, die in Frage kommen, sind genau die nicht teilerfremd zu p^e, die durch p teilbar sind. Das sind genau $p^{e-1} - 1$ Zahlen. Also folgt:

$$\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$$

Satz von Euler

Für Primzahlen p wissen wir ja schon aus dem kleinen Satz von Fermat, dass alle zu p teilerfremden Zahlen a die Kongruenz $a^{p-1} \equiv 1 \bmod p$ erfüllen.

Da $\varphi(p) = p - 1$ gilt, haben wir damit einen Spezialfall des folgenden Satzes, der als *Satz von Euler* bekannt ist:

Satz: Für teilerfremde ganze Zahlen a und n gilt:

$$a^{\varphi(n)} \equiv 1 \bmod n$$

Den Beweis führen wir in der nächsten Einheit...