RSA: Das Verfahren

Das nach seinen Autoren Rivest, Shamir und Adleman benannte *RSA-Verfahren* ist ein asymmetrisches Verschlüsselungsverfahren, das in sehr vielen weit verbreiteten Systemen angewendet wird.

Bob (B) soll eine Nachricht an *Alice* (A) schicken.

Vorbereitungen durch Alice:

- Wähle große Primzahlen p und q mit $p < q$.
  (Das ist möglich, wie wir später sehen werden.)
- Berechne $n = p \cdot q$.
- Setze $\varphi(n) = (p-1)(q-1)$, wähle $e > 1$ mit $\mathrm{ggT}(e, \varphi(n)) = 1$.
- Berechne Zahl $s < n$ mit $e \cdot s \equiv 1 \bmod \varphi(n)$. (Benutze hierbei den Euklidischen) Algorithmus!)

Alice veröffentlicht das Paar (n, e).

RSA: Bob sendet Nachricht

Die Zahlen n und e sind also nun öffentlich bekannt.
Dagegen müssen p, q und s absolut geheim bleiben!

Bobs Nachricht an Alice muss als eine Zahl im Bereich $\{0, \ldots, n-1\}$ gewählt werden. Die Nachricht sei x.

Bob macht nun Folgendes:

Berechne $y = x^e \bmod n$. (Mit schneller Exponentiation – Folie 28.6)

Sende y über einen beliebigen Kanal zu Alice.

Alice berechnet schließlich den Wert $x' = y^s \bmod n$ und geht davon aus, dass $x = x'$ gilt, d.h. dass sie Bobs Nachricht korrekt entschlüsselt hat.

Es muss also gelten: $(x^e)^s \bmod n = x$. Das zeigen wir gleich!

RSA: Ein Beispiel

Bob möchte die Nachricht 42 an Alice senden.

Vorbereitungen durch Alice:

Wähle $p = 11$ und $q = 13$.

Es gilt $11 < 13$ und p und q sind große Primzahlen!

Berechne $n = 11 \cdot 13 = 143$.

Setze $\varphi(n) = (11-1)(13-1) = 120$ und wähle $e > 1$.

1. Versuch: $e = 21$, es folgt aber $\mathrm{ggT}(21, 120) = 3$.
2. Versuch: $e = 7$, nun gilt $\mathrm{ggT}(7, 120) = 1$.

Mit Euklids Algorithmus erhalten wir $s = 103$, denn

$7 \cdot 103 = 721 \equiv 1 \bmod 120$

RSA-Beispiel (Fortsetzung)

Alice veröffentlicht das Paar $(143, 7)$.

Bob verschlüsselt die Nachricht 42 durch 42^7 mod 143:

$$42 \cdot 42 = 1764 \equiv 334 \equiv 48 \bmod 143$$
$$48 \cdot 48 = 2304 \equiv 874 \equiv 16 \bmod 143$$
$$42^7 \equiv 16 \cdot 48 \cdot 42 = 48 \cdot 672 \equiv 48 \cdot 100 = 4800 \equiv 510 \equiv 81$$

Bob sendet die verschlüsselte Nachricht 81 an Alice.

Alice berechnet y^s mod 143:

$$81^{103} = 3^{412} = 3^{27 \cdot 15} \cdot 3^7 = (3^{15})^{27} \cdot 9 \cdot 243 \equiv 9 \cdot 100 = 900 = 6 \cdot 143 + 42 \equiv 42$$

Es wurde benutzt, dass $3^{15} = (3^5)^3 = 243^3 \equiv 100^3 = 1000^2 \equiv (-1)^2 = 1 \bmod 143$.

Also hat Alice den Wert 42 korrekt berechnet.

RSA: Korrektheit

Wir müssen zeigen, dass $(x^e)^s \equiv x \bmod n$ gilt.

Da p und q teilerfremd sind, genügt es zu zeigen,
dass $(x^e)^s \equiv x \bmod p$ und $(x^e)^s \equiv x \bmod q$ gilt.

Beide Behauptungen sind nach dem selben Muster zu beweisen.
Es genügt also, die Behauptung modulo p zu prüfen:

Falls x durch p teilbar ist, gilt $(x^e)^s \equiv 0 \bmod p$, aber auch $x \equiv 0 \bmod p$.

Wenn aber x nicht durch p teilbar ist, haben wir $\mathrm{ggT}(x, p) = 1$, und folglich nach Fermats kleinem Satz $x^{p-1} \equiv 1 \bmod p$. Damit folgt:

$$(x^e)^s = x^{es} = x^{1+k(p-1)(q-1)} =$$
$$x \cdot \left(x^{p-1}\right)^{k(q-1)} \equiv x \cdot 1^{k(q-1)} \equiv x \bmod p$$

Korrektheit (Forts.)

Wir haben gesehen, dass $(x^e)^s \equiv x \bmod p$ gilt.

Auf die gleiche Weise erhalten wir auch $(x^e)^s \equiv x \bmod q$.

Da p und q teilerfremd sind, erhalten wir mit $n = pq$:

$$(x^e)^s \equiv x \bmod n.$$

Damit ist die Korrektheit der Entschlüsselung nachgewiesen.

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 $\mathrm{ggT}(k, n) = 1$ 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:

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

Beweis des Satzes von Euler

$(\mathbb{Z}/n\mathbb{Z})^*$ hat $\varphi(n)$ Elemente $g_1, g_2, \ldots, g_{\varphi(n)}$.

Nach Teil c) des Satzes aus Einheit 26 definiert $x \mapsto ax$ eine Bijektion auf $\mathbb{Z}/n\mathbb{Z}$ und daher auch auf $(\mathbb{Z}/n\mathbb{Z})^*$.

Also gilt:

$$(\mathbb{Z}/n\mathbb{Z})^* = \{g_1, g_2, \ldots, g_{\varphi(n)}\} = \{ag_1, ag_2, \ldots, ag_{\varphi(n)}\}$$

Wir definieren g als das Produkt aller Elemente von $(\mathbb{Z}/n\mathbb{Z})^*$.
Dann folgt:

$$g \equiv \prod_{i=1}^{\varphi(n)} ag_i \equiv a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} g_i \equiv a^{\varphi(n)} g$$

Diese Berechnungen sind natürlich modulo n zu verstehen.

Da g invertierbar ist, folgt die Behauptung.

Wie berechnet man $\varphi(n)$?

Wir zeigen zunächst, dass für teilerfremde Zahlen m und n gilt:

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Denn der Isomorphismus zwischen $\mathbb{Z}/mn\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, den wir aus dem Chinesischen Restsatz kennen, bildet Einheiten auf Einheiten ab. Also liefert die Einschränkung auf $(\mathbb{Z}/mn\mathbb{Z})^*$ einen Isomorphismus zwischen $(\mathbb{Z}/mn\mathbb{Z})^*$ und $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$, d.h.

$$\varphi(mn) = |(\mathbb{Z}/mn\mathbb{Z})^*| = |(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*| = \varphi(m)\varphi(n)$$

Daher gilt mit der Primfaktorzerlegung $n = p_1^{e_1} \cdots p_r^{e_r}$ die Formel:

$$\varphi(n) = \varphi(p_1^{e_1}) \cdots \varphi(p_r^{e_r})$$

und aus der letzten Einheit kennen wir bereits die Werte $\varphi(p^e)$ für Primzahlen p. Daraus folgt die Formel $\varphi(n) = n \cdot \prod_{p|n} (1 - \frac{1}{p})$

Noch ein Satz über die φ-Funktion

Satz: $\sum_{t|n} \varphi(t) = n$

Beachte, dass t hier von 1 bis n alle Teiler von n durchläuft!

Zum Beweis betrachtet man die Menge $N = \{\frac{0}{n}, \frac{1}{n}, \ldots, \frac{n-1}{n}\}$.

Nun kürzen wir alle Brüche in N, dann erhalten wir Brüche, deren Nenner Teiler von n sind und deren Zähler teilerfremd zum jeweiligen Nenner sind.

Für jeden Teiler t von n enthält N genau $\varphi(t)$ viele Brüche mit Nenner t. Und insgesamt sind es n Brüche.

Damit folgt die Behauptung!

Beispiel: $n = 12$, $N = \{\frac{0}{1}, \frac{1}{12}, \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{5}{12}, \frac{1}{2}, \frac{7}{12}, \frac{2}{3}, \frac{3}{4}, \frac{5}{6}, \frac{11}{12}\}$

Verallgemeinerung des Satzes von Euler

Der folgende Satz verallgemeinert den kleinen Satz von Fermat und den Satz von Euler:

Satz: Für jede kommutative Gruppe G und jedes $a \in G$ gilt: $a^{|G|} = 1$

Wie in den Spezialfällen beweisen wir auch diesen Satz, indem wir die Gruppe G einmal als $\{b_1, \ldots, b_{|G|}\}$ schreiben, und dann als $\{ab_1, \ldots, ab_{|G|}\}$. Da a invertierbar ist, sind diese beiden Mengen gleich, d.h. das Produkt aller Elemente hat jeweils den selben Wert. Daher muss $a^{|G|} = 1$ gelten.

Dieser Satz gilt übrigens auch für beliebige endliche Gruppen.

In dieser allgemeineren Form heißt er Satz von Lagrange.

Ein exaktes Primzahlzertifikat

Satz: Es sei $n \geq 2$, $n \in \mathbb{N}$. Falls für alle Primzahlen p mit $n \equiv 1 \bmod p$ eine Zahl $a \in \mathbb{Z}$ existiert, so dass

$$a^{n-1} \equiv 1 \bmod n \quad \text{und} \quad a^{\frac{n-1}{p}} \not\equiv 1 \bmod n$$

gilt, dann ist n eine Primzahl.

Bemerkung (ohne Beweis): Dieses Kriterium erfüllen alle Primzahlen.

Zum Beweis des Satzes genügt es zu zeigen, dass $\varphi(n)$ durch $n-1$ teilbar ist. Dazu zeigen wir für jede Primzahl p:

$$p^r \mid n-1 \quad \Longrightarrow \quad p^r \mid \varphi(n)$$

Denn daraus folgt, dass $n-1$ ein Teiler von $\varphi(n)$ ist, aber es gilt ja immer $\varphi(n) < n$, also folgt $\varphi(n) = n-1$, d.h. n ist prim.

Beweis

Sei p ein beliebiger Primteiler von $n-1$, und sei p^r die größte Potenz von p, die in $n-1$ aufgeht. Wir wählen eine ganze Zahl a gemäß der Voraussetzung, d.h. $a^{n-1} \equiv 1 \bmod n$, aber $a^{\frac{n-1}{p}} \not\equiv 1 \bmod n$. Ferner sei m die *Ordnung von* a, d.h. die kleinste positive ganze Zahl mit $a^m \equiv 1 \bmod n$.

Da a teilerfremd zu n ist, gilt auch $a^{\varphi(n)} \equiv 1 \bmod n$.

Damit ist m sowohl Teiler von $n-1$, als auch Teiler von $\varphi(n)$.
Andererseits ist m nicht Teiler von $\frac{n-1}{p}$, daher teilt p^r auch m.

Nun ist p^r ein Teiler von m und m ein Teiler von $\varphi(n)$,
also teilt p^r auch $\varphi(n)$, wie zu beweisen war.