Warum RSA funktioniert

Mathematisch formuliert wollen wir folgendes wissen: Wir starten mit $N = p \cdot q$ und $M = (p-1)(q-1)$. Dann bestimmen wir doch d so, daß $ed - 1$ durch M teilbar ist, wofür wir kurz schreiben

$$ed \equiv_M 1.$$

Im nächsten Schritt nehmen wir irgendeine Nachricht x zwischen 0 und $N-1$ und berechnen $y := x^e \bmod N$ und danach $z := y^d \bmod N$. Es ist nicht schwer einzusehen, daß dann $z \equiv_N (x^e)^d \equiv_N x^{ed}$ ist. Wir wollen also wissen, warum jetzt $z = x$ ist. Zu zeigen ist demnach

$$x^{ed} \equiv_N x.$$

Zunächst brauchen wir dazu ein wichtiges Ergebnis, welches auf Pierre de Fermat (1601–1665) zurückgeht.

FERMATS KLEINER SATZ. [1] *Sei p eine Primzahl und x nicht durch p teilbar (also $x \not\equiv_p 0$). Dann gilt*

$$x^{p-1} \equiv_p 1.$$

Der Beweis ist zwar nicht eigentlich schwer, aber weil er ein bißchen länger ist, verschieben wir ihn auf später.

ÜBUNG. *Was passiert, wenn x durch p teilbar ist?*

LEMMA (Miniversion des Chinesischen Restsatzes). *Seien p und q zwei unterschiedliche Primzahlen und x und y beliebige ganze Zahlen. Ist nun $x \equiv_p y$ und $x \equiv_q y$, so ist auch $x \equiv_{pq} y$.*

BEWEIS. Nun, nach Voraussetzung gilt: p ist ein Teiler von $x - y$ und q auch. Aber beide sind Primzahlen und verschieden. Aus der Voraussetzung lesen wir ab, daß in der Primfaktorzerlegung von $x - y$ sowohl p als auch q vorkommen. Also ist $x - y$ ein Vielfaches von $p \cdot q$. □

Als nächstes verallgemeineren wir Fermats kleinen Satz auf zwei Primzahlen.

[1] Dies ist nicht „Fermats letzter Satz“, der vor ein paar Jahren berühmt geworden ist. Mehr als dreihundert Jahre nach Fermats Tod war es endlich gelungen, Fermats letzte Vermutung (jetzt Satz) zu beweisen. Fermats kleiner Satz ist dagegen trivial, wie Mathematiker sagen.

SATZ. *Seien p und q zwei unterschiedliche Primzahlen und x nicht durch p teilbar und auch nicht durch q. Dann gilt*

$$x^{(p-1)(q-1)} \equiv_{pq} 1,$$

falls x weder durch p noch durch q teilbar ist.

BEWEIS. Nun betrachten wir $x^{(p-1)(q-1)}$ modulo p. Nach Fermats kleinem Satz ist $x^{p-1} \equiv_p 1$. Aber natürlich ist $1^{q-1} \equiv_p 1$. Also ist $x^{(p-1)(q-1)} \equiv_p (x^{p-1})^{q-1} \equiv_p 1^{q-1} \equiv_p 1$. Ebenso ist $x^{(q-1)(p-1)} \equiv_q 1$ wie man durch Vertauschen von p und q sieht. Da die Vertauschung im Exponenten nichts ändert, nämlich $x^{(p-1)(q-1)} = x^{(q-1)(p-1)}$ ist, können wir mit dem Lemma die Behauptung folgern. □

SATZ (RSA funktioniert). *Seien p und q zwei Primzahlen, $N = p \cdot q$ deren Produkt und $M = (p-1)(q-1)$. Gilt für zwei weitere Zahlen e und d die Gleichung $ed \equiv_M 1$, so folgt für irgendeine Nachricht x, die weder durch p noch durch q teilbar ist, die Gleichung*

$$x^{ed} \equiv_N x,$$

Die Entschlüsselung der codierten Nachricht x^e mod N liefert die ursprüngliche Nachricht x also wieder zurück.

BEWEIS. Nach Voraussetzung können wir doch $ed = 1 + M \cdot s$ mit einer geeigneten Zahl s schreiben. Also ist nach dem letzten Satz

$$x^{ed} \equiv_N x(x^{(p-1)(q-1)})^s \equiv_N x1^s \equiv_N x.$$ □

ÜBUNG. *Was passiert, wenn x durch p oder q teilbar ist?*

Und jetzt noch der verschobene Beweis.

BEWEIS (Fermats kleiner Satz). Wir beginnen mit einer Vorüberlegung:

Wenn $ab \equiv_p 0$ gilt,
so folgt $a \equiv_p 0$ oder $b \equiv_p 0$.

Unser Ausgangspunkt dabei ist nämlich, daß p das Produkt ab teilt. Da p eine Primzahl ist, muß es in der Primfaktorzerlegung von ab vorkommen. Also muß es in der Primfaktorzerlegung von a oder von b vorkommen. Aber das heißt ja gerade, daß p (mindestens) eine der Zahlen a und b teilt.

Nun betrachten wir die Menge

$$A := \{1, 2, 3, \ldots, p-1\}.$$

Multipliziere jedes Element modulo p mit x:

$$Ax = \{1 \cdot x \bmod p, 2 \cdot x \bmod p, 3 \cdot x \bmod p, \ldots, (p-1) \cdot x \bmod p\}.$$

Behauptung: Die Menge hat sich nicht geändert, in Formeln: $Ax = A$.

Zuerst zeigen wir, daß die Menge Ax in der Menge A enthalten ist, in Formeln $Ax \subset A$. Wir müssen also zeigen, daß jedes Element $i \cdot x \bmod p$ $(0 < i < p)$ aus Ax in A liegt. Nehmen wir an, daß das falsch ist, es also ein i gibt, $0 < i < p$, mit $i \cdot x \bmod p \notin A$. Nun, modulo p fehlt nur ein einziges Element in A nämlich 0. Also ist $i \cdot x \equiv_p 0$. Also ist nach der Vorüberlegung $i \equiv_p 0$ oder $x \equiv_p 0$. Aber $0 < i < p$ kann nicht 0 sein modulo p. Aber nach Voraussetzung ist auch $x \not\equiv_p 0$. Das ist ein Widerspruch, unsere Annahme, daß $i \cdot x$ nicht in A liegt, ist demnach falsch. Es gilt tatsächlich $Ax \subset A$.

Nun zeigen wir, daß die Elemente $i \cdot x$ für $0 < i < p$ paarweise verschieden sind. Nehmen wir an, das ist nicht so. Dann gibt es $i \neq j$ mit $0 < i, j < p$ und $i \cdot x \equiv_p j \cdot x$. Das bedeutet $(i - j) \cdot x \equiv_p 0$. Nach der Vorüberlegung muß also $i - j \equiv_p 0$ oder $x \equiv_p 0$ gelten. Letzteres kann nach Voraussetzung nicht sein, also bleibt $i \equiv_p j$. Weil $0 < i, j < p$ gilt, kann das aber auch nicht sein, außer wenn $i = j$ ist. Aber das ist ein Widerspruch. Also ist unsere Annahme falsch und damit sind tatsächlich die Elemente $i \cdot x$ für $0 < i < p$ paarweise verschieden.

Fassen wir die letzten beiden Dinge zusammen, so ist klar, daß $Ax = A$ ist, denn Ax liegt in A und hat gleich viele Elemente.

Wenn wir nun die Elemente von Ax modulo p miteinander multiplizieren, so erhalten wir das gleiche Ergebnis, wie wenn wir alle Elemente von A modulo p miteinander multiplizieren:

$$1x \cdot 2x \cdot 3x \cdot \ldots \cdot (p-1)x \equiv_p 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1),$$

Umsortieren ergibt $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \cdot x^{p-1} \equiv_p 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$ oder

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \cdot (x^{p-1} - 1) \equiv_p 0.$$

Wenden wir die Vorüberlegung mehrfach an, so muß einer der Faktoren modulo p gleich 0 sein. Aber $1, \ldots, p-1$ sind modulo p sicher nicht 0. Also folgt $x^{p-1} - 1 \equiv_p 0$ oder

$$x^{p-1} \equiv_p 1.$$

Das wollten wir zeigen. □