RSA (nicht nur) für Mathematiker

Harold Gutch

KNF-Kongress 2003
23. November 2003

1. Allgemeines

RSA ist ein sogenanntes Public-Key Verschlüsselungsverfahren. Bei „klassischer“ Verschlüsselung besitzen Sender und Empfänger einen gemeinsamen Schlüssel, über den die beiden Nachrichten austauschen können. Wollen 10 Leute sicher miteinander kommunizieren, so brauchen sie also insgesamt bereits 45 Schlüssel. Im Gegensatz dazu steht die Public-Key Kryptographie, bei der jeder Kommunikationspartner ein Schlüsselpaar besitzt. Die eine Hälfte dieses Schlüsselpaares veröffentlicht er, die andere Hälfte hält er geheim. Der öffentliche Schlüssel wird benutzt um für ihn bestimmte Nachrichten zu verschlüsseln. Ist eine Nachricht so verschlüsselt, so kann keiner, der nicht den zugehörigen privaten Schlüssel hat (auch nicht der Sender) diese Nachricht wieder entschlüsseln. Bei unseren 10 Leuten im obigen Beispiel werden damit nur noch 10 Schlüsselpaare, oder insgesamt 20 Schlüssel benötigt.
RSA entstammt ursprünglich einer Konversation zwischen James Ellis und Clifford Cocks, die beide für die britische GCHQ, dem Äquivalent zum BND oder zur NSA arbeiteten. Ellis erzählte 1973 Cocks von der Idee der Public-Key Kryptographie, und bereits kurze Zeit später hatte dieser eine Implementation eines solchen Algorithmus gefunden. Leider waren die Computer damals noch nicht schnell genug, um den von ihm gefundenen Algorithmus zu implementieren, so dass er in der Versenkung verschwand. 4 Jahre später entdeckten Ronald Rivest, Adi Shamir und Leonard Adleman den Algorithmus neu, und benannten ihn nach den Anfangsbuchstaben ihrer Nachnamen.
RSA, der wohl bekannteste Public-Key Algorithmus, unterlag bis vor kurzem dem Patent von RSA Security Inc., wonach eine Implementation in kommerzieller Software deren Lizensierung bedurfte. Inzwischen ist dieses Patent ausgelaufen und jeder darf RSA frei benutzen wie es ihm beliebt.

2. Rechnen mit endlichen Zahlen

Das erste Problem vor dem man steht ist, dass Algorithmen und Computer mit Zahlen umgehen, man aber häufig Text verschlüsseln will. Dazu bildet man zuerst den Text umkehrbar auf eine Folge von Zahlen ab, verschlüsselt dann die einzelnen Zahlen, und sieht diese Zahlenfolge als den verschlüsselten Text an. Will der Empfänger des Textes ihn lesen, so entschlüsselt er die Zahlenfolge macht die erste Abbildung rückgängig, und sieht wieder den Klartext vor sich. Dieser Vortrag befasst sich nur mit der reinen Ver- und Entschlüsselung, also nicht mit der Transformation des Textes in eine Zahlenfolge! Anders ausgedrückt - dieser Vortrag setzt sich zum Ziel, eine Folge von Zahlen sicher zwischen zwei Personen zu übertragen.
Das nächste Problem ist, dass man irgendwie mit endlichen Zahlbereichen arbeiten will, da es unsinnig ist, wenn man einen kurzen Text zwar gut (also „ziemlich sicher“) verschlüsselt, der Text aber in verschlüsselter Form durch eine sehr große Zahl dargestellt wird (man stelle sich zur Verdeutlichung des Problems vor, dass ein Text nach der Verschlüsselung durch eine Zahl dargestellt wird, die z.B. mehr Stellen hat als das Universum

Atome). Auf jeden Fall wird klar, dass man irgendwie sicherstellen muss, dass bei der Verschlüsselung eines Textes nur Zahlen bis zu einer gewissen festgelegten Obergrenze auftreten. Um dieses Problem zu umgehen, rechnet man (mathematisch) mit endlichen Zahlen, also am Computer z.B. mit Zahlen im Bereich von 0 bis $2^{32} - 1$. Summiert oder multipliziert man nun zwei Zahlen, und das Ergebnis liegt nicht mehr im Bereich des erlaubten, ist also größer als die größte erlaubte Zahl, so subtrahiert man die erste nicht mehr erlaubte Zahl, und zwar so oft bis man wieder eine Zahl im erlaubten Bereich hat. So wird $(2^{32} - 2) + 4$ zu 2. Wie man subtrahiert und dividiert, werden wir noch sehen. Mathematisch sieht man das meistens nicht als „oft subtrahieren“, sondern als Division mit Rest. Im obigen Beispiel dividiert man mit Rest durch 2^{32}, und betrachtet jetzt nur den Rest und rechnet mit dem weiter. Eigentlich rechnet man im täglichen Leben auch schon auf diese Art. Eine normale Uhr mit Zifferblatt stellt auch nur Zahlen von 0 bis 11 dar, und trotzdem weiß jeder, dass 11 Uhr plus 4 Stunden 3 Uhr ergibt. Hier beschränkt man sich auf die Addition, aber das Prinzip ist bei der Multiplikation dasselbe.

Definition 2.1. Sind a und b natürliche Zahlen, so bezeichnet man mit a MOD b (sprich: „a modulo b “) den Rest bei der ganzzahligen Division von a und b. Es ist $0 \leq a$ MOD b und a MOD $b < b$.

Beispiel 2.2.

$$5 \text{ MOD } 3 = 2$$
$$17 \text{ MOD } 4 = 1$$
$$1635675 \text{ MOD } 2 = 1$$

Anders ausgedrückt: kann man a schreiben als

$$a = k \cdot b + r$$

mit einer ganzen Zahl k, und $0 \leq r < b$, so gilt: a MOD $b := r$.

Hieran erkennt man: Wenn a MOD $n = X = b$ MOD n, dann ist also $a = k \cdot n + X$ und $b = l \cdot n + X$, mit gewissen ganzen Zahlen k und l. Das heißt, dass $(a - b) = (k - l) \cdot n$, also dass $(a - b)$ Vielfaches von n ist.

Bemerkung 2.3 *(MOD-Rechenregeln).* Für beliebige natürliche Zahlen a, b und n gilt:

(i) $(a + b)$ MOD $n = ((a \text{ MOD } n) + (b \text{ MOD } n))$ MOD n
Denn ist $a = k \cdot n + A$ und $b = l \cdot n + B$, dann ist $(a + b) = (k + l) \cdot n + (A + B)$ und das MOD n ist genau $(A + B)$ MOD n

(ii) $(a \cdot b)$ MOD $n = ((a \text{ MOD } n) \cdot (b \text{ MOD } n))$ MOD n
Denn ist $a = k \cdot n + A$ und $b = l \cdot n + B$, dann ist $(a \cdot b) = (k \cdot l \cdot n + k \cdot B + l \cdot A)n + (A \cdot B)$, und das MOD n ist genau $(A \cdot B)$ MOD n

(iii) Hat man Primzahlen p und q, und ist $x = a$ MOD p, und $x = a$ MOD q, so ist auch $x = a$ MOD $(p \cdot q)$.
Denn

$$\begin{aligned} a &= x + k \cdot p, \\ a &= x + l \cdot q, \text{ also} \\ k \cdot p &= l \cdot q \end{aligned}$$

Da in der Primfaktorzerlegung der linken Seite der Primfaktor p vorkommt, muss dies auch auf der rechten Seite der Fall sein, also ist l ein Vielfaches von p. Benutzt man nochmals $a = x + l \cdot q$, so sieht man, dass man a schreiben kann als $x + \frac{l}{p} \cdot (p \cdot q)$, also ist $x = a$ MOD $(p \cdot q)$.

Aus den ersten beiden Regeln sieht man, dass man modulo einer festen Zahl n so addieren und multiplizieren kann wie man es gewohnt ist. Zur Subtraktion macht man sich klar, dass die Subtraktion einer Zahl x nichts anders als die Addition einer bestimmten Zahl y ist, die die besondere Eigenschaft hat, dass $x + y = 0$, bzw. hier: $(x + y)$ MOD $n = 0$, also kann man die Subtraktion einer Zahl x betrachten wie die Addition von $n - x$.
Bei der Division ist es nicht so leicht, wie man leicht erkennt, ist z.B. $(4 \cdot 2)$ MOD $6 = 2$, aber wenn man das Ergebnis nun wieder durch 2 dividiert, erhält man nicht die Zahl 4, mit der man begonnen hat, sondern plötzlich die Zahl 1. Zunächst soll also keine Division erlaubt sein.

3. Die Mathematik im RSA-Verfahren

Der allgemeinen Konvention folgend, werden im Folgenden die Kommunikationspartner einer verschlüsselten Konversation als Alice und Bob bezeichnet.

Satz 3.1 (Das RSA-Verfahren). *Alice wählt zwei unterschiedliche Primzahlen p und q sowie eine Zahl d („decryption exponent“), die teilerfremd zu $((p-1) \cdot (q-1))$ ist. Dann sucht sie eine Zahl e („encryption exponent“), für die gilt, dass $(d \cdot e)$ MOD $((p-1) \cdot (q-1)) = 1$. Sie veröffentlicht die Zahlen $n := p \cdot q$ und e, behält aber die Faktoren p und q, sowie d geheim. Wie wir noch sehen werden, ist es für einen Aussenstehenden praktisch nicht möglich, d ohne Kenntnis von p und q zu berechnen. Möchte nun Bob eine Nachricht m („message“) sicher an Alice übermitteln, so berechnet er:*

$$c = m^e \text{ MOD } n$$

Zum Entschlüsseln berechnet Alice $x = c^d$ MOD n, und das zunächst erstaunliche ist, dass $x = m$. In Kurzform:

$p \neq q$, beide prim, $n := pq$
d mit $ggT(d, (p-1)(q-1)) = 1$

e so daß ed MOD $(p-1)(q-1) = 1$
$c = m^e$ MOD n
$m = c^d$ MOD n

Zum Verständnis des RSA-Verfahrens fehlen 2 Sachen. Zum einen die Berechnung von e, und zum anderen der Beweis dass $x = m$.

Satz 3.2 (Der erweiterte Euklidsche Algorithmus). *Für zwei ganze Zahlen a und b mit $a > b$ lässt sich der größte gemeinsame Teiler $ggT(a,b)$ auf folgende Art bestimmen:*

$$\begin{aligned}
n_1 &= a, n_2 = b \\
n_1 &= d_1 \cdot n_2 + n_3 \text{ (also } n_3 = n_1 \text{ MOD } n_2) \\
n_2 &= d_2 \cdot n_3 + n_4 \text{ (also } n_4 = n_2 \text{ MOD } n_3) \\
&\dots \\
n_{i-2} &= d_{i-2} \cdot n_{i-1} + n_i \text{ (also } n_i = n_{i-2} \text{ MOD } n_{i-1}) \\
n_{i-1} &= d_{i-1} \cdot n_i + n_{i+1} \text{ (also } n_{i+1} = n_{i-1} \text{ MOD } n_i) \\
n_i &= d_i \cdot n_{i+1} \text{ (also kein Rest bei der Division)}
\end{aligned}$$

Die Zahl n_{i+1} gibt dann den ggT von a und b an. Weiterhin lassen sich nun Zahlen k und l bestimmen für die gilt: $a \cdot k + b \cdot l = ggT(a,b)$

Beweis. n_i ist nach der letzten Zeile Vielfaches von n_{i+1}, also ist n_{i+1} gemeinsamer Teiler von n_i und n_{i+1} (sich selbst). Nach der vorletzten Zeile ist dann n_{i-1} Vielfaches von n_{i+1}. Geht man so die Gleichungen im Euklidschen Algorithmus von unten nach oben durch, sieht man schließlich, dass n_{i+1} Teiler von n_2 (also b) und n_1 (also a ist).
Dass n_i der größte gemeinsame Teiler ist (das heißt, dass ein beliebiger gemeinsamer Teiler von a und b Vielfaches von n_i ist, also geschrieben werden kann als $c \cdot n_i$ - dabei darf c durchaus auch 1 sein), sieht man wie folgt:
Gibt man sich einen beliebigen gemeinsamen Teiler h von a und b (also n_1 und n_2) vor, dann ist nach der ersten Zeile im Algorithmus h auch ein Teiler von n_3 (nach n_3 auflösen, und die andere Seite ist Vielfaches von h, also ist auch n_3 Vielfaches von h). Aus demselben Grund ist dann auch n_3 Vielfaches von h, und nachdem man den Algorithmus nach unten durchgegangen ist, ist ebenso dann schließlich auch n_{i+1} Vielfaches von h.
Zuletzt wollen wir noch Zahlen k und l finden, für die gilt $a \cdot k + b \cdot l = ggT(a,b)$. Dazu drücken wir zunächst $ggT(a,b)$ als Summe von Vielfachen von n_{i-1} und n_{i-2} aus, dann als Summe von Vielfachen von n_{i-2} und n_{i-3} und schließlich als Summe von Vielfachen von a und b. Wir gehen den Algorithmus rückwärts durch, beginnend mit der vorletzten Zeile, und sehen:

$$\begin{aligned}
n_{i+1} &= n_{i-1} - d_{i-1} \cdot n_i = \\
&= n_{i-1} - d_{i-1} \cdot (n_{i-2} - d_{i-2} \cdot n_{i-1}) =
\end{aligned}$$

$$= \quad (-d_{i-1}) \cdot n_{i-2} + (d_{i-1}d_{i-2} + 1) \cdot n_{i-1}$$

Analog geht man den Algorithmus durch bis auf der rechten Seite eine Summe von zwei Vielfachen von n_1 und n_2 steht. □

Beispiel 3.3. Es soll der ggT von 76 und 56 berechnet werden, weiterhin sollen zwei Zahlen k und l wie oben berechnet werden.

$$\begin{aligned}
76 &= 1 \cdot 56 + 20 \\
56 &= 2 \cdot 20 + 16 \\
20 &= 1 \cdot 16 + 4 \\
16 &= 4 \cdot 4 \\
4 &= \underline{20} - \underline{16} = \\
&= \underline{20} - (\underline{56} - 2 \cdot \underline{20}) = -1 \cdot \underline{56} + 3 \cdot \underline{20} = \\
&= -1 \cdot \underline{56} + 3 \cdot (\underline{76} - \underline{56}) = 3 \cdot \underline{76} - 4 \cdot \underline{56}
\end{aligned}$$

Beispiel 3.4. Es soll der ggT von 37 und 5 sowie k und l wie oben berechnet werden.

$$\begin{aligned}
37 &= 7 \cdot 5 + 2 \\
5 &= 2 \cdot 2 + 1 \\
2 &= 2 \cdot 1 \\
1 &= \underline{5} - 2 \cdot \underline{2} = \\
&= \underline{5} - 2 \cdot (\underline{37} - 7 \cdot \underline{5}) = (-2) \cdot \underline{37} + 15 \cdot \underline{5}
\end{aligned}$$

Hat man also zwei teilerfremde Zahlen a und b gegeben (das heißt $ggT(a, b) = 1$), so findet man Zahlen k und l, so dass $k \cdot a + l \cdot b = 1$, das heißt $k \cdot a$ MOD $b = 1$. Das ist insbesondere dann der Fall, wenn die größere der beiden eine Primzahl ist.

Mit der letzten Bemerkung nochmal zurück zu einem anfangs erwähnten Problem, der Division. Ähnlich wie eine Subtraktion durch eine geschickte Addition ausgedrückt werden kann, kann auch eine Division durch eine geschickte Multiplikation ausgedrückt werden. Anstatt durch eine Zahl x zu dividieren, multipliziert man durch eine bestimmte Zahl y mit der besonderen Eigenschaft $x \cdot y = 1$, oder, wenn man „Modulo n“ rechnet,

$$x \cdot y \text{ MOD } n = 1$$

Wie wir eben gesehen haben, ist es möglich, ein solches y immer dann zu finden, wenn x und n teilerfremd sind! Damit ist das erste fehlende Puzzlestück gefunden - zu gegebenen teilerfremden Zahlen d und n, die teilerfremd sind, findet sich eine Zahl e, so dass $d \cdot e$ MOD $n = 1$.

Satz 3.5 (Kleiner Fermat). *Sei p eine Primzahl. Dann gilt für alle Zahlen x die teilerfremd zu p sind:*

$$x^{p-1} \text{ MOD } p = 1$$

Beweis. Wir betrachten die Zahlen

$$\{x, 2x, 3x, \ldots, (p-1)x\} \text{ (alle Elemente MOD p)} \tag{1}$$

Diese sind alle verschieden, denn wäre dies nicht so, also hätte man

$$ax \text{ MOD } p = bx \text{ MOD } p \text{ für } 1 \leq a < b \leq p-1,$$

dann wäre also

$$(b-a)x = bx - ax = lp \text{ mit einer ganzen Zahl } l$$

Betrachtet man nun die Primfaktorzerlegung der linken Seite, so muss darin der Faktor p auftauchen, da dies auch auf der rechten Seite so der Fall ist. x ist aber nicht Vielfaches von p, also muss der Faktor p im Term $b-a$ auftauchen. Es gilt aber $1 \leq (b-a) \leq p-2$, also kann $b-a$ nicht Vielfaches von p sein.
Man hat also in (1) eine Menge von $(p-1)$ verschiedenen Zahlen, die alle größer als 1 und kleiner als p sind, also genau die Menge

$$\{1, 2, \ldots, p-1\}$$

Also gilt:

$$x \cdot 2x \cdot \ldots \cdot (p-1)x \text{ MOD } p = 1 \cdot 2 \cdot \ldots \cdot (p-1) \text{ MOD } p$$

Weil $1, \ldots (p-1)$ teilerfremd zu p sind, darf man, wie oben zur Division MOD p bemerkt, sie kürzen (also auf beiden Seiten durch sie teilen), und es bleibt stehen:

$$x^{p-1} \text{ MOD } p = 1$$

□

Folgerung 3.6. *Sind p und q verschiedene Primzahlen, und ist* $n \text{ MOD } (p-1)(q-1) = 1$, *so ist* $x^n \text{ MOD } n = x$ *für alle* $x < n$.

Beweis. Der Fall $x = 0$ ist klar, dann ist nämlich $x^n = 0 = x$, also erst recht $x^n \text{ MOD } n$. Ansonsten hat n die Darstellung

$$n = l(p-1)(q-1) + 1$$

für eine gewisse Zahl l. Also ist

$$\begin{aligned} x^n \text{ MOD } p &= x^{l(p-1)(q-1)+1} \text{ MOD } p = \\ &= x \cdot (x^{p-1})^{l(q-1)} \text{ MOD } p = \\ &= x \cdot 1^{l(q-1)} \text{ MOD } p = x \text{ MOD } p \end{aligned}$$

wobei in der vorletzten Zeile aufgrund der Teilerfremdheit von x und p der kleine Satz von Fermat für die Aussage $x^{p-1} \text{ MOD } p = 1$ benutzt werden konnte. Ebenso zeigt man:

$$x^n \text{ MOD } q = x \text{ MOD } q$$

p und q sind teilerfremd, also gilt nach den Modulo-Rechenregeln:

$$x^n \text{ MOD } (p \cdot q) = x$$

□

Womit die zweite noch fehlende Behauptung im RSA-Algorithmus bewiesen wäre.

4. Wie sicher ist RSA?

Kann ein Angreifer die Zahl n in ihre Primfaktoren zerlegen, so hat er den geheimen Schlüssel geknackt. Es ist also sicherlich geschickt, zwei sehr große Primfaktoren zu nehmen, jeweils in der Größenordnung von mindestens 10^{100} (das ist ca. 2^{330}, man hätte also insgesamt eine Schlüssellänge von ca. 660 Bit). Weiterhin sollten die beiden Primfaktoren einen deutlichen Größenunterschied aufweisen, denn es ist

$$n = p \cdot q = (\frac{p+q}{2})^2 - (\frac{p-q}{2})^2$$

und es ist $s := \frac{p-q}{2}$ klein, so ist $t := \frac{p+q}{2}$ eine ganze Zahl, die etwas größer als $\sqrt{n}$ ist - man lässt also eine Schleife durchlaufen, die die ganzen Zahlen k ab $\sqrt{n}$ daraufhin testet, ob $k^2 - n$ eine Quadratzahl ist. Wenn ja, ist $k = t$ und $s = \sqrt{t^2 - n}$, woraus man einfach p und q bestimmt.
Weiterhin ist es bei bestimmten Schlüsseln möglich, einfach durch wiederholte Verschlüsselung bereits nach wenigen Schritten wieder den Klartext zu erhalten, z.B. für $p = 47, q = 59, n = pq = 2773, (p-1)(q-1) = 2668, e = 17, d = 157$. Verschlüsselt man nun die Nachricht $m = 518$, so erhält man

$$518^{17} \text{ MOD } 2773 = 1781$$

und nun einfach durch Wiederholung der Verschlüsselungsoperation:

$$1781^{17} \text{ MOD } 2773 = 894$$
$$894^{17} \text{ MOD } 2773 = 1364$$
$$1364^{17} \text{ MOD } 2773 = 518$$

Der „Wiederherstellungsexponent“ ist in diesem Fall 3, da man durch 3 weitere Verschlüsselungsvorgänge wieder zum Klartext kommt. Man sieht also, dass es sogenannte „schwache“ RSA-Schlüssel gibt. Starke Schlüssel dagegen sind z.B. solche, bei denen nicht nur p und q Primzahlen sind, sondern zusätzlich auch $\frac{p-1}{2}$ und $\frac{q-1}{2}$.