RSA-Verschlüsselung

von Johannes Becker

Gießen

2006/2008

Zusammenfassung

Es wird gezeigt, wieso das nach Ronald L. **R**ivest, Adi **S**hamir und Leonard **A**dleman genannte RSA-Kryptosystem funktioniert, das mittlerweile alltäglich z.B. bei verschlüsselter Datenübertragung benutzt wird.

1 Vorbereitung

Wir benötigen ein paar Begriffe aus der Zahlentheorie. Im Folgenden repräsentieren die Variablen immer ganze Zahlen.

Definition 1.
*Eine positive ganze Zahl $p>1$ heißt **Primzahl**, wenn sie sich nur durch p und 1 teilen lässt.*

Beispiel 2.
Die Zahlen 2, 3, 5, 7, 11, 13, 17 sind Primzahlen, die dazwischenliegenden nicht.

Definition 3.
*Zwei Zahlen n und m heißen **teilerfremd**, wenn sie positive ganze Zahlen sind und wenn 1 die einzige Zahl ist, die sowohl n also auch m teilt, anders ausgedrückt: Der größte gemeinsame Teiler von n und m ist 1.*

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

Beispiel 4.
8 und 9 sind teilerfremd.
9 und 12 sind nicht teilerfremd, weil sie beide durch 3 geteilt werden.

Definition 5.
Für zwei positive Zahlen m und n bezeichnen wir den Rest r bei der Division von m durch n mit

$$r = m \bmod n$$

d.h. es ist $0 \leqslant r < m$ und es gibt eine Zahl k (der ganze Anteil bei der Division von m durch n) mit $m = k \cdot n + r$

Beispiel 6.
7 geteilt durch 5: Es ist $7 = 1 \cdot 5 + 2$ also

$$7 \bmod 5 = 2$$

13 geteilt durch 4: Es ist $13 = 3 \cdot 4 + 1$ also

$$13 \bmod 4 = 1$$

2 Das RSA-Verschlüsselungsverfahren

Jeder Text kann als Zahl dargestellt werden, indem man den einzelnen Buchstaben verschiedene Zahlen zuordnet, z.B.

$$A \to 01, B \to 02, C \to 03, D \to 04, E \to 05, F \to 06, \ldots$$

So wird z.B. aus dem Text FADE die Zahl 06010405. Damit wir immer gleich rechnen können, verstehen wir deshalb im Folgenden unter „Klartext“ und „Code“ schon die Zahlen, die sich aus dem Text ergeben.

Rezept zum Erzeugen der Schlüssel	**kleines Beispiel**
Nimm zwei verschiedene (große) Primzahlen p und q	$p=43$, $q=67$
Setze $k=p\cdot q$	$k=43\cdot 67=2881$
Setze $m=(p-1)\cdot(q-1)$	$m=42\cdot 66=2772$
Wähle eine Zahl s zwischen 1 und m, sodass s und m teilerfremd	$s=125$
Finde ein positives t, sodass $s\cdot t \bmod m=1$	$t=377$
Veröffentliche $(s\|k)$ als den öffentlichen Schlüssel	$(125\|2881)$
Bewahre $(t\|k)$ als geheimen Schlüssel	$(377\|2881)$
Rezept zum Verschlüsseln	$T=1001$
Aus dem Klartext T wird der Geheimtext G mit:	$T^s=1001^{125}$
$G=T^s \bmod k$	$G=T^s \bmod 2881=147$
Rezept zum Entschlüsseln	
Aus dem Geheimtext G wird der Klartext T mit:	$G^t=147^{377}$
$T=G^t \bmod k$	$G^t \bmod 2881=1001\checkmark$

Bemerkung 7. Aus der letzten Zeile folgt, dass der Klartext T kleiner sein muss als die (große) Zahl k. Wenn der Klartext länger sein sollte, muss er in kleinere Stücke aufgeteilt werden, die dann getrennt verschlüsselt werden. Weiter unten, im Beweis zum RSA-Verfahren, stellt sich heraus, dass T sogar kleiner sein sollte als p und als q.

Es gibt immer mindestens eine Zahl s wie oben gefordert, denn die größere der beiden Zahlen p und q erfüllt die Bedingung. Allerdings darf man gerade p oder q nicht verraten.

Wie man die Zahl t findet, wird in 3.1 erklärt.

Ein Beweis, dass der Rechenaufwand zum Knacken des Schlüssels sehr hoch ist, wird hier nicht gegeben. Es wird nur gezeigt, dass das Verschlüsseln/Entschlüsseln funktioniert.

Nebenrechnung Ausgeführt mit dem Programm PARI/GP. Für a^b tippt man dort a^b, und für $a \bmod b$ tippt man a % b. (Nicht zu verwechseln mit Prozent.)

```
                GP/PARI CALCULATOR Version 2.1.7 (released)

pari] e = 1001^125  /* potenzieren */

  %1 = 113307768067783277734975216789059184885833405090373919699704926409381466187\
  27424289689068934442654313634935059728753820777794245822084472112198107413416003 9\
  94315955059678540150908189398494675569941366106426950605457248791213175697733261 9\
  24517657233463166178932188338980929205995942933916282306780104492919394564307665 2\
  05593879489975499142407867777144493600409666927577501250010 01

pari] q = e \ 2881  /* ganzer Anteil bei der Division */

  %2 = 393293190099907246563607139149806264789425217252252411314491240574041881941\
  25040922211277106708275993179226170526740092946179263526846484249212451972981617 4\
  74196303574031725619257859765687870773833273538448283948133456408237333209764879 9\
  87912729029722895449261327105105620291551346525221389471642153741476551767815568 2\
  24900657722927799869517069688110009026066181629911493 4

pari] G = e % 2881  /* Rest bei der Division */

  %3 = 147
```

```
pari] probe = q * 2881 + 147 - 1001^125
  %4 = 0
pari] 147^377
  %5 = 11984921672959130266021278957901500368230579106826205679910669564183642992576\
  30157279017041027739244928422775050478992157097131696905567345438610188875469112\
  61023849460711696404240840190181688777847350205573070716113337121000486595302947\
  23611725737277366137270909552691122716926575671453713949606694383753294704852917\
  15526487307744551774074487006900687376089780584330369490180164729651463067138908\
  44971421542256585207594285800171823317978935593192384964367651356849481202150549\
  34065355844923569532139252107467406705122155598016841048437313676504519601071714\
  90126913415153338116505845110038752768587992302492553955450777998525082346342441\
  14671495430243591815699885297843854953773404262800613828557589174502223820170031\
  90987379699813068463583265485406011780694898424976152344962853074663075750005089\
  96474858452787
pari] entschluessel = 147^377 % 2881
  %6 = 1001
```

Interessant ist, wie unregelmäßig die Zuordnung „Klartext ⇒Geheimtext“ aussieht. Beispiele:

$$1001 \to 147,\ 1002 \to 483,\ 1003 \to 1932,\ 1004 \to 66,\ 1005 \to 938,\ \ldots$$

Bemerkung 8.

- Die Verschlüsselung hat nur mit Computer Sinn, weil der Rechenaufwand hoch ist.
- Die RSA-Verschlüsselung ist nicht absolut sicher. Wer das Produkt der beiden Primzahlen in die einzelnen Primzahlen zerlegen kann, hat den Schlüssel geknackt. Zur Zeit ist der Rechenaufwand dafür wesentlich höher als der Aufwand zur Herstellung der Schlüssel. Mehr noch: Der Rechenenaufwand zur Primzahlzerlegung wächst sehr viel schneller als die Größe der Primfaktoren. Wenn die Computer so schnell werden, dass sie die zur Zeit benutzen Schlüssellängen knacken können, muss man die Schlüssel nur ein wenig länger machen, um dann wieder auf der sicheren Seite zu sein. Eine wirkliche Bedrohung wäre eine neue mathematische Idee, die die Primzahlzerlegung wesentlich schneller machen würde. Oder eine prinzipielle neue Sorte von Computern. (Quantencomputer).
- Dass das RSA-Verfahren mit Verschlüsseln und Entschlüsseln funktioniert, bedeutet in Formeln

  $$\boxed{T = G^t \bmod k = (T^s \bmod k)^t \bmod k}$$

  Zum Beweis braucht man mathematische Ideen aus über 2000 Jahren:

  1. Der Euklidische Algorithmus zur Bestimmung des kleinsten gemeinsamen Teilers zweier Zahlen
  2. Der Chinesische Restzahlsatz
  3. Der Satz von Fermat

3 Bausteine zum Beweis

3.1 Der Euklidische Algorithmus

Durch wiederholte Division mit Rest kann man den ggT (größten gemeinsamen Teiler) zweier Zahlen berechnen. Als Nebenprodukt erhält man eine Methode, wie man zu der im RSA-Verfahren zur Zahl s die Zahl t findet. Wir führen den Algorithmus am Beispiel für die Suche nach dem ggT von 816 und 294 vor.

$$\begin{array}{rlr@{\quad}rcl} 816:294 & \text{geht 2 mal mit Rest} & 228 & 816 & = & 2\cdot 294+228 \\ 294:228 & \text{geht 1 mal mit Rest} & 66 & 294 & = & 1\cdot 228+66 \\ 228:66 & \text{geht 3 mal mit Rest} & 30 & 228 & = & 3\cdot 66+30 \\ 66:30 & \text{geht 2 mal mit Rest} & 6 & 66 & = & 2\cdot 30+6 \\ 30:6 & \text{geht 5 mal mit Rest} & 0 & 30 & = & 5\cdot 6+0 \end{array}$$

Man überlegt sich, dass der größte gemeinsame Teiler der beiden ersten Zahlen von Zeile zu Zeile erhalten bleibt. In diesem Fall ist das die Zahl 6. Von der vorletzten Zeile erhalten wir Schritt für Schritt rückwärts gehend

$$\begin{aligned} 6 &= 66-2\cdot 30 \\ &= 66-2\cdot(228-3\cdot 66)=7\cdot 66-2\cdot 228 \\ &= 7\cdot(294-1\cdot 228)-2\cdot 228=7\cdot 294-9\cdot 228 \\ &= 7\cdot 294-9\cdot(816-2\cdot 294) \\ &= -9\cdot 816+25\cdot 294 \end{aligned}$$

Man bekommt auf diese Weise den ggT 6 als Kombination der beiden Ausgangszahlen 816 und 294.

Das nützt beim Erzeugen der RSA-Schlüssel an folgender Stelle: Gegeben waren teilerfremde Zahlen s und m, d.h. $\mathrm{ggT}(s,m)=1$. Dann finden wir mit Euklid eine Kombination

$$\begin{aligned} 1 &= -b\cdot m+t\cdot s \\ t\cdot s &= b\cdot m+1 \end{aligned}$$

d.h. wenn $t\cdot s$ durch m dividiert wird, geht das b mal und es bleibt der Rest 1

$$t\cdot s \bmod m = 1$$

wie gefordert. (Fall t eine negative Zahl ist, muss man noch ein Vielfaches von m addieren, um zu einem positiven Kandidaten zu kommen.)

3.2 Der kleine Satz von Fermat

Satz 9. *Es sei p eine Primzahl und a eine positive ganze Zahl, die kein Vielfaches von p ist. Dann gilt*

$$a^{p-1} \bmod p = 1$$

Beispiel 10.

$$\begin{array}{ll} p=5, a=2 & a^{p-1}=16=3\cdot 5+1 \\ p=5, a=3 & a^{p-1}=81=16\cdot 5+1 \\ p=7, a=9 & a^{p-1}=531441=75920\cdot 7+1 \end{array}$$

Vor dem Beweis des Satzes von Fermat brauchen wir noch einige Hilfmittel.

3.3 Das Rechnen mit Restzahlen

Für den noch ausstehenden Beweis des Satzes von Fermat usw. hilft folgende Schreibweise für bessere Übersicht.

Definition 11. *Wir schreiben*

$$x \underset{m}{=} y$$

wenn die ganzen Zahlen x und y bei der Division durch m denselben Rest ergeben, d.h. wenn

$$x \bmod m = y \bmod m$$

oder anders ausgedrückt: Es gibt einen ganzzahligen Faktor k mit

$$x-y = k\cdot m$$

Satz 12. (Rechenregeln mit Resten)
Es seien x, y ganze Zahlen und x', y' Zahlen mit gleichen Resten bei der Division durch m, d.h. $x \underset{m}{=} x', y \underset{m}{=} y'$. Dann gilt

$$x + y \underset{m}{=} x' + y' \tag{1}$$
$$x \cdot y \underset{m}{=} x' \cdot y' \tag{2}$$
$$x^y \underset{m}{=} (x')^y \tag{3}$$

Beispiel 13. $x = 17, y = 24, m = 5$

$$41 = 17 + 24 \underset{5}{=} 2 + 4 = 6 \underset{5}{=} 1$$
$$408 = 17 \cdot 24 \underset{5}{=} 2 \cdot 4 = 8 \underset{5}{=} 3$$
$$3394486713146119046435041171 21 = 17^{24} \underset{5}{=} 2^{24} = 16777216 \underset{5}{=} 1$$

Achtung: Den Exponenten y auf der rechten Seite von Gleichung (3) kann man nicht durch y' ersetzen. Man sieht, dass die Rechenregeln manchmal erlauben, das Ergebnis mit erheblich weniger Rechenaufwand zu bekommen. Bei der Berechnung von $(17^{24} \bmod 5)$ muss man – wie die letzte Gleichung zeigt – gar nicht die Zahl 17^{24} ausrechnen. Es geht noch mit weniger Aufwand: auch die explizite Berechnung von 2^{24} lässt sich vermeiden, wenn man nur den Rest wissen will.

$$2^{24} = 2^{4 \cdot 6} = (2^4)^6 = 16^6 \underset{5}{=} 1^6 = 1$$

Beweis. (zu Satz 12)
Nach Voraussetzung lassen sich $(x - x')$ und $(y - y')$ durch m dividieren, d.h. es gibt k und l mit

$$\begin{aligned} (x - x') &= k \cdot m \\ (y - y') &= l \cdot m \end{aligned} \tag{4}$$

Durch Addition der beiden Gleichung erhält man

$$(x + y) - (x' + y') = (k + l) \cdot m$$

in Worten: $(x + y)$ und $(x' + y')$ unterscheiden sich durch ein Vielfaches von m. Mit Definition 11 folgt daraus die Gleichung (1). Nun multiplizieren wir Gleichung (4) mit y und erhalten

$$y \cdot (x - x') = y \cdot x - y \cdot x' = y \cdot k \cdot m$$

Das bedeutet $y \cdot x \underset{m}{=} y \cdot x'$. Ebenso folgt $y \cdot x' \underset{m}{=} y' \cdot x'$, also insgesamt Gleichung (2). Wenn man in Gleichung (2) links und rechts den gleichen Faktor wählt, erhält man $x^2 \underset{m}{=} (x')^2$. Das darf man wieder nach Gleichung (2) rechts mit x und links mit x' multiplizieren: $x^3 \underset{m}{=} (x')^3$ Durch wiederholtes Multiplizieren folgt Gleichung (3). □

Satz 14. (Chinesischer Restzahlsatz) *Es seien p, q zwei teilerfremde Zahlen. Dann folgt aus*

$$r \underset{p}{=} y$$
$$r \underset{q}{=} y$$

auch

$$r \underset{p \cdot q}{=} y$$

Vor dem Beweis erst das

Beispiel 15.

$$\begin{aligned} 1 &= 16 \bmod 3 \\ 1 &= 16 \bmod 5 \\ \text{also auch: } 1 &= 16 \bmod 15 \end{aligned}$$

Gegenbeispiel für den Fall, dass p und q nicht teilerfremd sind:

$$\begin{aligned} 1 &= 31 \bmod 6 \\ 1 &= 31 \bmod 15 \\ \text{aber: } 1 &\neq 31 \bmod 90 \ (=31) \end{aligned}$$

Beweis. Aus $r \underset{p}{=} y$ folgt mit obigen Rechenregeln $0 \underset{p}{=} y - r$, d.h. dass die Division $(y-r)\colon p$ aufgeht, also

$$p \text{ teilt die Zahl } (y-r)$$

[Im obigen Beispiel: 3 teilt $(16-1)=15$]. Ähnlich folgt

$$q \text{ teilt die Zahl } (y-r)$$

Weil p und q teilerfremd sind, folgt

$$(p \cdot q) \text{ teilt die Zahl } (y-r)$$

Also gibt es einen Faktor k, sodass

$$(y-r) \underset{p \cdot q}{=} 0$$

Mit den Rechenregeln folgt

$$y \underset{p \cdot q}{=} r$$

□

Wir brauchen noch einen Hilfssatz über eine Kürzungsregel. Man kann nicht wie gewohnt aus der Gleichung $2 \cdot 7 \underset{6}{=} 2 \cdot 4$ den Faktor 2 auf beiden Seiten kürzen, denn es ist $7 \neq_6 4$. Primzahlreste kann man aber kürzen, wie der folgenden Satz zeigt.

Satz 16. (Kürzungsregel) *Es sei p ein Primzahl und $a \bmod p \neq 0$. Dann folgt aus*

$$a \cdot x \underset{p}{=} a \cdot y$$

auch

$$x \underset{p}{=} y$$

Beweis. Nach Voraussetzung ist

$$\begin{aligned} a \cdot x - a \cdot y &\underset{p}{=} 0 \\ a \cdot (x-y) &\underset{p}{=} 0 \end{aligned}$$

d.h. linke Seite dieser Gleichung ist durch p teilbar. Weil p die Zahl a nicht teilt und weil p eine Primzahl ist, sind p und a teilerfremd. Also bleibt nur die Möglichkeit, dass p die Zahl $(x-y)$ teilt.

$$\begin{aligned} (x-y) &\underset{p}{=} 0 \\ x &\underset{p}{=} y \end{aligned}$$

Wenn man die Folgerung $a \cdot x \underset{p}{=} a \cdot y \Rightarrow x \underset{p}{=} y$ umkehrt, erhält man

$$x \neq_p y \ \Rightarrow \ a \cdot x \neq_p a \cdot y$$

□

Beweis. (des kleinen Satzes von Fermat)
Voraussetzung: p ist Primzahl und $a \neq_p 0$.
Beispiel p=7, a=4. Wir betrachten die Gleichung

$$\begin{aligned} (1 \cdot 4) \cdot (2 \cdot 4) \cdot (3 \cdot 4) \cdot (4 \cdot 4) \cdot (5 \cdot 4) \cdot (6 \cdot 4) &\underset{7}{=} 1 \cdot 4 \cdot 2 \cdot 4 \cdot 3 \cdot 4 \cdot 4 \cdot 4 \cdot 5 \cdot 4 \cdot 6 \cdot 4 \\ 4 \cdot 8 \cdot 12 \cdot 16 \cdot 20 \cdot 24 &\underset{7}{=} 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \end{aligned}$$

Jetzt bilden wir auf der linken Seite der Gleichung die Reste bei der Divison durch 7.

$$4\cdot 1\cdot 5\cdot 2\cdot 6\cdot 3 \underset{7}{=} 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 4^6$$

Nun dividieren wir beide Seiten der Gleichung durch $1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6$.

$$1 \underset{7}{=} 4^6$$

Tatsächlich ist $4^6 = 4096 = 1 + 585\cdot 7$, d.h. der Rest bei der Division durch 7 ist 1. Funktioniert das bei jeder Primzahl? Anders gesagt, ergibt die Umformung der linken Seite immer bloß eine andere Reihenfolge der Zahlen $1, 2, 3, ..., (p-1)$?

Wir betrachten die Menge M der Zahlen

$$M = \{\, a\cdot 1 \bmod p,\ a\cdot 2 \bmod p,\ a\cdot 3 \bmod p, ...,\ a\cdot(p-1) \bmod p\}$$

Wir behaupten

$$M = \{1, 2, 3, ..., (p-1)\}$$

(die Reihenfolge der Zahlen spielt bei der Menge keine Rolle.) Die Behauptung wird in zwei Schritten bewiesen:

a) Jede Zahl x aus M ist Rest bei der Division durch p. Also $1 \leqslant x \leqslant p-1$

b) Die Zahlen im M sind alle verschieden. Wäre nämlich z.B.

$$a\cdot 2 \bmod p = a\cdot 3 \bmod p$$

dann hätten wir $a\cdot 2 \underset{p}{=} a\cdot 3$ und dürften a nach der Kürzungsregel weglassen, also $2 \underset{p}{=} 3$. Das ist ein Widerspruch, weil 2 und 3 kleiner als p sind.

Aus a) und b) zusammen genommen ergibt sich, dass M alle Zahlen von 1 bis $(p-1)$ enthält. Nun multiplizieren wir alle Zahlen aus M.

$$1\cdot 2\cdot 3\cdot ...\cdot(p-1) \underset{p}{=} a\cdot 1\cdot a\cdot 2\cdot a\cdot 3\cdot ...\cdot a\cdot(p-1) = 1\cdot 2\cdot 3\cdot ...\cdot(p-1)\cdot a^{p-1}$$

Weil die Zahlen aus M alle nicht von p geteilt werden, darf man sie nach Satz 16 der Reihe nach aus dieser Gleichung kürzen und es bleibt

$$1 \underset{p}{=} a^{p-1}$$

Das ist der Satz von Fermat. □

Beweis. (zum RSA-Verfahren)

Damit das RSA-Verfahren funktioniert, war folgende Behauptung zu zeigen

$$T = (T^s \bmod k)^t \bmod k$$

Wegen Bemerkung 7 ist T kleiner als k, d.h. wenn man T duch k dividiert, bleibt T als Rest.

$$T \bmod k = (T^s \bmod k)^t \bmod k$$

Mit Definition 11 kann man das schreiben als

$$T \underset{k}{=} (T^s \bmod k)^t$$

Mit der Rechenregel 3 wird das zu

$$T \underset{k}{=} (T^s)^t = T^{s\cdot t}$$

Es bleibt also zu zeigen

$$T^{s\cdot t} \underset{k}{=} T$$

Nach Konstruktion war $s\cdot t \bmod m = 1$, mit anderen Worten: Die Division $(s\cdot t - 1) : m$ geht auf, es gibt einen Faktor f mit $s\cdot t - 1 = f\cdot m$, $s\cdot t = 1 + f\cdot m$. Also

$$T^{s\cdot t} = T^{1+m\cdot f} = T\cdot T^{m\cdot f} = T\cdot (T^m)^f \tag{5}$$

Wegen der Gleichung (2) wären wir fertig, wenn wir zeigen könnten, dass

$$(T^m)^f \underset{k}{=} 1$$

Wir untersuchen jetzt den Term T^m. Dazu erinnern wir uns an $m = (p-1)\cdot(q-1)$ und erhalten

$$T^m = T^{(p-1)\cdot(q-1)} = (T^{p-1})^{q-1}$$

Nun wenden wir zweimal den kleinen Satz von Fermat an:

$$\begin{aligned} T^m = (T^{q-1})^{p-1} &\underset{p}{=\!=} 1^{q-1} = 1 \\ (T^{p-1})^{q-1} &\underset{q}{=\!=} 1 \end{aligned}$$

Der Chinesische Restzahlsatz liefert hier

$$T^m \underset{p\cdot q}{=\!=} 1$$

Weil $p \cdot q = k$ ist, erhalten wir für jedes beliebige f

$$(T^m)^f \underset{k}{=\!=} 1^f = 1$$

was zu zeigen war.

□

Bemerkung 17. Damit man den kleinen Satz von Fermat anwenden darf, muss T^{q-1} teilerfremd zu p sein. Das erreicht man z.B. dadurch, dass $T < p$ gewählt wird. Größere Nachrichten muss man in kleinere Stücke aufteilen und einzeln verschlüsseln. Nun darf man p und q nicht verraten und deshalb auch die maximale Größe der Nachricht nicht genau verraten. Ein Ausweg ist, wenn p und q von ähnlicher Größe gewählt werden. Dann ist $q \approx p \approx \sqrt{p \cdot q} = \sqrt{k}$ und man empfiehlt, T ordentlich kleiner als $\sqrt{k}$ zu wählen.

4 Dank

An Marcel Schubert fürs Korrekturlesen.

5 Literatur

- Simon Singh: The Code Book, Forth Estate, London
- François Fricker: Datenschutz durch Verschlüsselung, Neue Zürcher Zeitung, 17.3.1982
- http://pajhome.org.uk/crypt/index.html
- http://www.cypherspace.org/adam/rsa/
- https://chorgiessen.altervista.org/jab/code/