Die Berechnung der Primfaktoren aus den Exponenten

Annie Yousar*

2023-04-01

Zusammenfassung

Wie man bei RSA den geheimen Schlüssel d aus dem Produkt $p \cdot q$ und dem öffentlichen Exponenten e bestimmt, weiß jeder. Wir zeigen hier den umgekehrten Weg, nämlich wie man aus den beiden Exponenten e und d und dem Modul m die Primfaktoren p und q berechnet und geben dafür einen *Einzeiler* in der Sprache dc an. Dass unter den üblichen RSA-Annahmen über die Primfaktoren die Kenntnis von e und d äquivalent zur Faktorisierung des Moduls ist, war wohl Folklore, und es gab auch einige randomisierte Algorithmen. Hier stellen wir den deterministischen Algorithmus des Annex C der NIST SP800-52B vor ([NIST]).

Wenn man den größten gemeinsamen Teiler GGT von $p-1$ und $q-1$ kennen würde, wäre alles so einfach.

Weil $e \cdot d - 1$ durch das kleinste gemeinsame Vielfache KGV von $p-1$ und $q-1$ teilbar ist, und $\mathrm{GGT} \cdot \mathrm{KGV} = (p-1) \cdot (q-1)$ ist, gilt

$$\mathrm{GGT} \cdot (e \cdot d - 1) = h \cdot (p-1) \cdot (q-1) = h \cdot p \cdot q - h \cdot (p+q-1)$$

und andererseits hat man die Division mit Rest für $m = p \cdot q$:

$$\mathrm{GGT} \cdot (e \cdot d - 1) = k \cdot m + r,$$

mit $0 \le r < m$.

Vergleicht man diese beiden Darstellungen, ergeben sich $k = h - 1$ und $r = m - h \cdot (p+q-1)$, woraus man

$$s = \frac{p+q}{2} = \frac{1 + (m-r)/(k+1)}{2}$$

erhält. Die Differenz

$$d = \frac{p-q}{2} = \sqrt{s^2 - m}$$

ist nach den binomischen Formeln die Quadratwurzel aus $s^2 - m$. Daraus ergeben sich die beiden Primfaktoren als $p = s + d$ und $q = s - d$.

*mailto:*a.yousar@informatik.hu-berlin.de*

Tatsächlich kann man aber statt des größten gemeinsamen Teilers GGT von $p-1$ und $q-1$ auch irgendein Vielfaches VGT des GGT nehmen, so lange nur der Wert $h \cdot (p+q-1)$ kleiner als m bleibt.

Die Rechnung bleibt die gleiche. Aus

$$\text{VGT} \cdot (e \cdot d - 1) = h \cdot (p-1) \cdot (q-1) = h \cdot m - h \cdot (p+q-1)$$

und der Division mit Rest

$$\text{VGT} \cdot (e \cdot d - 1) = k \cdot m + r, \text{ mit } 0 \le r < m.$$

bestimmt man $k = h - 1$ und $r = m - h \cdot (p+q-1)$ und so weiter.

Wie man leicht sieht, teilt jeder gemeinsame Teiler von $p-1$ und $q-1$ auch den größten gemeinsamen Teiler GCD von $e \cdot d - 1$ und $m - 1$.

Denn jeder gemeinsame Teiler vom $p-1$ und $q-1$ teilt sowohl

$$m - 1 = (p-1) \cdot (q-1) + p + q - 2 = (p-1) \cdot (q-1) + (p-1) + (q-1)$$

als auch das kleinste gemeinsame Vielfache KGV der beiden Zahlen und folglich auch $e \cdot d - 1$.

Insbesondere teilt dann auch der größte gemeinsame Teiler GGT von $p-1$ und $q-1$ den größten gemeinsamen Teiler GCD von $e \cdot d - 1$ und $m - 1$. GCD ist also das gesuchte Vielfache VGT.

In der Sprache dc reicht für die Eingabe m, e, d (in dieser Reihenfolge) eine Zeile:

```
dc << EOF
3566714233 23 852881305
*1-dSErdsm1-[dSarLa%d0<a]dsax+LE*lm~lmr-r1+/1+2/d2^Lm-vsddld-rld+f
EOF
```

Literatur

[NIST] Elaine Barker, Lily Chen, Allen Roginsky, Apostol Vassilev, Richard Davis, Scott Simon: Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography, NIST Special Publication 800-56B, Revision 2, 2019-03, https:/doi.org