
Fortgeschrittene Techniken der Kryptographie

Jürgen Fuß

Episode 3: Parameterwahl für das RSA-Verfahren

HAGENBERG | LINZ | STEYR | WELS



UNIVERSITY
OF APPLIED SCIENCES
UPPER AUSTRIA

Kettenbrüche

Erde überstreicht in 365 Tagen genau $359^\circ 45' 40'' 31'''$.

Saturn in der selben Zeit $12^\circ 13' 34'' 18'''$.

$$\text{Verhältnis } \rho = \frac{77708431}{2640858} \approx 29,4254484716709.$$

Lässt sich ρ (wenigstens näherungsweise) als Verhältnis kleinerer Zahlen darstellen?
Wie gut/schlecht wird dabei die Näherung?

$$\rho = \frac{77708431}{2640858} \approx 29,4254484716709$$

77708431 : 2640858 = 29



Astronomie (II)

$$\rho = \frac{77708431}{2640858} \approx 29,4254484716709$$

$$\frac{77708431}{2640858} = 29 + \frac{1123549}{2640858} \quad (\rho \approx 29)$$

Rest

$$29 + \frac{1}{\frac{2640858}{1123549}}$$

2640858 : 1123549 =

$$\rho = \frac{77708431}{2640858} \approx 29,4254484716709$$

$$\frac{77708431}{2640858} = 29 + \frac{1123549}{2640858} \quad (\rho \approx 29)$$

$$= 29 + \frac{1}{\frac{2640858}{1123549}} = 29 + \frac{1}{2 + \frac{393760}{1123549}} \quad (\rho \approx \frac{59}{2} = 29,5)$$

29 + $\frac{1}{2}$

Astronomie (II)

$$\rho = \frac{77708431}{2640858} \approx 29,4254484716709$$

$$\frac{77708431}{2640858} = 29 + \frac{1123549}{2640858}$$

($\rho \approx 29$)

$$= 29 + \frac{1}{\frac{2640858}{1123549}} = 29 + \frac{1}{2 + \frac{393760}{1123549}}$$

($\rho \approx \frac{59}{2} = 29,5$)

$$= 29 + \frac{1}{2 + \frac{1}{\frac{1123549}{393760}}} = 29 + \frac{1}{2 + \frac{1}{2 + \frac{336079}{393760}}}$$

($\rho \approx \frac{147}{5} = 29,4$)

29 + $\frac{1}{2 + \frac{1}{2}}$

$$\rho = \frac{77708431}{2640858} \approx 29,4254484716709$$

$$\frac{77708431}{2640858} = 29 + \frac{1123549}{2640858} \quad (\rho \approx 29)$$

$$= 29 + \frac{1}{\frac{2640858}{1123549}} = 29 + \frac{1}{2 + \frac{393760}{1123549}} \quad (\rho \approx \frac{59}{2} = 29,5)$$

$$= 29 + \frac{1}{2 + \frac{1}{\frac{1123549}{393760}}} = 29 + \frac{1}{2 + \frac{1}{2 + \frac{336029}{393760}}} \quad (\rho \approx \frac{147}{5} = 29,4)$$

$$= 29 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\frac{393760}{336029}}}} = 29 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{57731}{336029}}}}} \quad (\rho \approx \frac{206}{7} \approx 29,4286)$$

Notation

Ist $n \in \mathbb{N}$ und sind $a_0, \dots, a_n \in \mathbb{N}$, dann sei

$$[a_0; a_1, \dots, a_n] := a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{a_n}}}}.$$

Algorithmus

Ist $x = \frac{p}{q} \in \mathbb{Q}$, so kann die Kettenbruchentwicklung $x = [a_0; a_1, a_2, \dots]$ auf folgende Art berechnet werden.

1. Berechne mit dem Euklidschen Algorithmus den ggT von p und q .
2. Die Quotienten der Divisionen in den einzelnen Schritten sind genau die Werte a_0, a_1, \dots .

```
> from si import extended_gcd
> extended_gcd( 77708431, 2640858, verbose=1 )
    77708431          2640858
77708431           1           0
2640858           0           1         29
1123549           1          -29         2
393760            -2          59         2
336029            5          -147        1
57731             -7          206        5
47374              40         -1177       1
10357             -47          1383       4
5946              228         -6709       1
4411              -275          8092       1
1535              503         -14801      2
1341             -1281          37694      1
194               1784         -52495      6
177              -11985          352664     1
17               13769         -405159     10
7                -149675          4404254    2
3                 313119         -9213667    2
1                -775913          22831588   3
```

$$\frac{77708431}{2640858} = [29; 2, 2, 1, 5, 1, 4, 1, 1, 2, 1, 6, 1, 10, 2, 2, 3].$$

si.py

```
> import si
> kb = si.continued_fraction( 77708431, 2640858 ); list( kb )
[29, 2, 2, 1, 5, 1, 4, 1, 1, 2, 1, 6, 1, 10, 2, 2, 3]
> app = si.cf_approx( 77708431, 2640858 )
> [ a/b for (a,b) in app ]
[29.0, 29.5, 29.4, 29.428571428571427, 29.425, 29.425531914893618,
29.42543859649123, 29.425454545454546, 29.42544731610338,
29.42544886807182, 29.425448430493272, 29.425448477263245,
29.425448471203428, 29.425448471688657, 29.42544847166732,
29.425448471671437, 29.42544847167095]
> list( si.cf_approx_from_cf( [29, 2, 2, 1, 5, 1, 4, 1, 1, 2, 1, 6, 1, 10, 2, 2, 3] ) )
[(29, 1), (59, 2), (147, 5), (206, 7), (1177, 40), (1383, 47), (6709, 228), (8092, 275),
(14801, 503), (37694, 1281), (52495, 1784), (352664, 11985), (405159, 13769),
(4404254, 149675), (9213667, 313119), (22831588, 775913), (77708431, 2640858)]
```

$$29 + \frac{1}{2+1} \xrightarrow{\text{?}} \frac{59}{2}$$

(59,2)

Satz v. Wiener (1)

Es seien $x \in \mathbb{R}$ und $[a_0; a_1, a_2, \dots]$ die Kettenbruchentwicklung von x . Weiterhin seien r und s ganze Zahlen. Dann gilt:

Ist $\left| x - \frac{r}{s} \right| < \frac{1}{2s^2}$, dann gibt es ein $n \in \mathbb{N}$, sodass $\frac{r}{s} = [a_0; a_1, \dots, a_n]$.

Sind alle Näherungen durch Kettenbrüche so gut?

n	r/s	$x - r/s$	$1/2s^2$	$ x - r/s < 1/2s^2$
0	29	$4,3 \cdot 10^{-1}$	$5,0 \cdot 10^{-1}$	✓
1	$59/2$	$-7,5 \cdot 10^{-2}$	$1,3 \cdot 10^{-1}$	✓
2	$147/5$	$2,5 \cdot 10^{-2}$	$2,0 \cdot 10^{-2}$	
3	$206/7$	$-3,1 \cdot 10^{-3}$	$1,0 \cdot 10^{-2}$	✓
4	$1177/40$	$4,5 \cdot 10^{-4}$	$3,1 \cdot 10^{-4}$	
5	$1383/47$	$-8,3 \cdot 10^{-5}$	$2,3 \cdot 10^{-4}$	✓
6	$6709/228$	$9,9 \cdot 10^{-6}$	$9,6 \cdot 10^{-6}$	
7	$8092/275$	$-6,1 \cdot 10^{-6}$	$6,6 \cdot 10^{-6}$	✓
8	$14801/503$	$1,2 \cdot 10^{-6}$	$2,0 \cdot 10^{-6}$	✓
9	$37694/1281$	$-4,0 \cdot 10^{-7}$	$3,0 \cdot 10^{-7}$	
10	$52495/1784$	$4,1 \cdot 10^{-8}$	$1,6 \cdot 10^{-7}$	✓
11	$352664/11985$	$-5,6 \cdot 10^{-9}$	$3,5 \cdot 10^{-9}$	
12	$405159/13769$	$4,7 \cdot 10^{-10}$	$2,6 \cdot 10^{-9}$	✓

Wieners Angriff auf RSA

Satz v. Wiener (2)

Seien $p, q \in \mathbb{P}$ mit $q < p < 2q$. Es sei $n := pq$ und $d, e \in \mathbb{N}$ seien so gewählt, dass $\underbrace{ed = 1 \pmod{\varphi(n)}}$. Ist $\boxed{d < \frac{1}{3}\sqrt[4]{n}}$, dann lässt sich d aus dem RSA Public Key (n, e) einfach berechnen.

Sei k jene positive ganze Zahl, für die

$$ed = k\varphi(n) + 1$$

$$\boxed{ed - 1 = k\varphi(n)}$$

$$n \approx 2^{2000}$$

$$\sqrt[4]{n} \approx \sqrt[4]{2^{2000}} \cdot 2^{\frac{2000}{4}} \approx 2^{250}$$

$$k = \frac{ed-1}{\varphi(n)}$$

Dann ist $\frac{k}{d}$ ein Bruch, so dass

$$\left| \frac{e}{n} - \frac{k}{d} \right| < \frac{1}{2d^2}.$$

$p^2 < 2n \rightarrow$ Da $p < 2q$, ist $\underline{p^2 < 2pq}$, also $p < \sqrt{2n}$. Weiterhin ist $\underline{q < p < \sqrt{2n}}$. Daneben ist $\underline{p^2 < 2pq}$

$$n - \varphi(n) = p + q - 1 < p + q < 2q + q = 3q < 3\sqrt{2n}$$

und

$$\boxed{p < d}$$

$$p \cdot q - (p-1)(q-1)$$

$$pq - pq + p + q - 1$$

$$k = \frac{ed - 1}{\varphi(n)} < \frac{ed}{\varphi(n)} < d,$$

$$\boxed{n - \varphi(n) < 3\sqrt{2n}}$$

$$\frac{ed}{\varphi(n)} = \frac{e}{\varphi(n)} \cdot d < 1$$

denn $e < \varphi(n)$. Schließlich folgt aus $d < \frac{1}{3}\sqrt[4]{n}$, dass $9d^2 < \sqrt{n}$. Somit ist

$$\boxed{d < \frac{1}{3}\sqrt[4]{n}} \\ \boxed{d^2 < \frac{1}{9}\sqrt{2n}}$$

$$qd^2 < \sqrt{n}$$

$$\begin{aligned} \left| \frac{e}{n} - \frac{k}{d} \right| &= \left| \frac{k}{d} - \frac{e}{n} \right| = \left| \frac{kn - ed}{nd} \right| \checkmark \\ &= \left| \frac{kn - (1 + k\varphi(n))}{nd} \right| = \left| \frac{k(n - \varphi(n)) - 1}{nd} \right| \\ &= \frac{k(n - \varphi(n)) - 1}{nd} < \frac{k(n - \varphi(n))}{nd} < \frac{d(n - \varphi(n))}{nd} \\ &= \frac{n - \varphi(n)}{n} < \frac{3\sqrt{2n}}{n} = \frac{3\sqrt{2}}{\sqrt{n}} < \frac{3\sqrt{2}}{9d^2} = \frac{\sqrt{2}}{3d^2} < \frac{1}{2d^2}. \end{aligned}$$

$$\frac{3\sqrt{2n}}{n}, \quad \frac{3\sqrt{2}}{\sqrt{n^2}}$$

$$\frac{\sqrt{2}}{3} < \frac{1}{2}$$

Wieners Attacke

Mit den folgenden Schritten lassen sich aus einem Public Key (n, e) die Primfaktoren von n berechnen, wenn d ausreichend klein ist.

1. Setze $i := 1$.
2. Berechne die Kettenbruchentwicklung $K/D = [a_0; a_1, \dots, a_i]$ des Bruchs e/n .
3. Ist D gerade, setze $i := i + 2$. Weiter bei Schritt 2.
4. Berechne $\Phi := (e \cdot D - 1)/K$.
5. Ist Φ keine ganze Zahl, setze $i := i + 2$. Weiter bei Schritt 2.
6. Berechne die beiden Lösungen der Gleichung

$$x^2 - (n - \Phi + 1)x + n = 0.$$

$n, \varphi(n)$

Sind die beiden Lösungen ganzzahlig, so handelt es sich um die beiden Primfaktoren von n .

7. Andernfalls, setze $i := i + 2$. Weiter bei Schritt 2.

Brechen des RSA Public Key (n, e) = (19452881344027252501, 11591841614497619999)
(Lösung mit Generatoren anstatt Listen, um unnötige Berechnungen zu vermeiden.)

```
> n, e = 19452881344027252501, 11591841614497619999
> # Jede zweite Kettenbruchnäherung berechnen
> app = si.cf_approx( e, n ); app = itertools.islice( app, 1, None, 2 )
> # Zu jeder Näherung die resultierenden Werte für D und Phi berechnen
> # und die gültigen auswählen
> DPhis = ( ( D, (e*D-1)//K ) for (K,D) in app if D%2==1 and (e*D-1)%K==0 )
> # Zu den passenden D und Phi die Lösungen der quadratischen Gleichung
> pqss = ( ( -(n-Phi+1), n ) for (D,Phi) in DPhis )
> xs = ( ( -p + math.sqrt( p**2 - 4*q ) ) // 2 for (p,q) in pqss )
> # Den ersten Teiler von n finden
> next( x for x in xs if n%x == 0 )
5218623757
```

Fermat-Faktorisierung

Differenzen von Quadraten

Wenn sich Zahlen $a, b \in \mathbb{N}$ finden lassen, so dass

$$n = a^2 - b^2,$$

dann lässt sich n einfach faktorisieren, denn dann ist

$$n = \underbrace{a^2 - b^2}_{(a+b) \cdot (a-b)} = \underbrace{(a+b) \cdot (a-b)}.$$

Ist $a - b \neq 1$, dann sind $p := a + b$ und $q := a - b$ die Primfaktoren von n .

p und q sind nah beieinander

1. Das lineare Gleichungssystem

$$p+q = 2a$$

$$+ \begin{cases} p = a + b \\ q = a - b \end{cases}$$

$$p-q = 2b$$

lässt sich nach a und b auflösen und man erhält

$$\begin{cases} a = \frac{p+q}{2} \\ b = \frac{p-q}{2} \end{cases}$$

$$n = \underline{q^2 - b^2}$$

$$q^2 = n + b^2$$

$$q_1 = \sqrt{n+b^2}$$

Liegen also p und q nahe beieinander, dann ist b klein.

2. Ist $\underline{n = a^2 - b^2}$, dann ist $\underline{b^2 = a^2 - n}$. Damit b klein ist, muss a^2 ein wenig größer als n sein, also a ein wenig größer als \sqrt{n} . Wir können also mit $\underline{a := \lceil \sqrt{n} \rceil}$ beginnen und dann immer größere a probieren.

Angenommen, $p - q < 2\sqrt[4]{n}$. Dann ist

$$\begin{aligned}a - \sqrt{n} &= \frac{(a - \sqrt{n})(a + \sqrt{n})}{a + \sqrt{n}} = \frac{a^2 - n}{a + \sqrt{n}} = \\&= \frac{b^2}{a + \sqrt{n}} < \frac{b^2}{2\sqrt{n}} = \frac{(p-q)^2/4}{2\sqrt{n}} = \frac{(p-q)^2}{8\sqrt{n}} < \frac{4\sqrt{n}}{8\sqrt{n}} = 1/2.\end{aligned}$$

Es unterscheidet sich dann also a von \sqrt{n} maximal um $1/2$. In diesem Fall ist also der Startwert $a = \lceil \sqrt{n} \rceil$ bereits der richtige.

Für ein 3000 Bit langes n wäre die Zahl $\sqrt[4]{n}$ etwa 750 Bit lang, der Unterschied zwischen p und q ist also riesig, im Vergleich zu p und q aber doch zu klein.

```
> import math, si
> q = si.next_prime( 2**1000 + 2**500 )
> p = si.next_prime( q + 2**200 )
> n = p*q
> a = math.sqrt( n ) + 1
> b = math.sqrt( a**2 - n )
> n % (a-b)
0
> a-b
1071508607186267320948425049060001810561404811705533607443750388370\\
3510511249361224931983788156958581275946729175531468251871452856923\\
1404359845775747018481945424639166942441751179022042145877839239972\\
4694252976635167807506380344211404881403840296707172208316181410223\\
8669647088198509779890534195659079
```