KAPITEL 5

Public-Key-Verschlüsselung — RSA

1. Erinnerung

Viele unserer bisher betrachteten Verschlüsselungsverfahren funktionierten in etwa so:

(1) Man hat eine Menge M von Nachrichteneinheiten zur Verfügung, beispielsweise $M = \{\mathrm{A}, \ldots, \mathrm{Z}\}$ bei MASC, $M = \{\mathrm{AB}, \mathrm{AC}, \ldots, \mathrm{ZY}\}$ bei PLAYFAIR, $M = \{\mathrm{AA}, \ldots, \mathrm{ZZ}\}$ bei ALBC-2. Bei Bedarf kann M mit einem mathematischen Objekt identifiert werden, beispielsweise $\{0, 1, \ldots, 25\}$, $\mathbb{Z}/26\mathbb{Z}$ oder $\mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$.

(2) In Abhängigkeit von einem Parameter K, dem sogenannten Schlüssel, hat man bijektive Funktionen
$$f_K : M \to M.$$

(3) (a) Der zu verschlüsselnde Text wird in eine Folge von Nachrichteneinheiten $a_1, a_2, a_3, \ldots$ mit $a_i \in M$ umgewandelt.
(b) Für jedes a_i wird mit dem Schlüssel K und der Verschlüsselungsfunktion f_K nun $b_i = f_K(a_i)$ berechnet. Der Chiffretext ist die Folge $b_1, b_2, b_3, \ldots$.

(4) Die verwendeten Funktionen sind so, dass man bei Kenntnis von K auch f_K^{-1} kennt. Dann kann man mit Hilfe von $a_i = f_K^{-1}(b_i)$ aus dem Chiffretext den Klartext erhalten. Deshalb ist die Geheimhaltung des Schlüssels für die Sicherheit von zentraler Bedeutung.

(Für Stromchiffren wie STROM, VIGENERE oder AUTOKEY muss man obige Punkte etwas modifizieren.)

2. Eine Idee

Diffie und Hellman beschreiben 1976 in „New Directions in Cryptography“ die grundlegende Idee zu einem **Public-Key-Verschlüsselungsverfahren**:

M denken wir uns wieder als Menge von Nachrichteneinheiten. Abhängig von einem Parameter K gibt es bijektive Funktionen $f_K : M \to M$. Dabei sollen folgende Eigenschaften erfüllt sein:

1 Kennt man K, so lässt sich für alle $a \in M$ der Wert $f_K(a)$ schnell berechnen.

2 Auch wenn man K und damit f_K kennt, kann man zu (allgemeinem) $b \in M$ das Urbild $f_K^{-1}(b)$ praktisch nicht berechnen, d.h. in angemessener Zeit.

3 Man kann Parameter K und K' so finden/konstruieren, dass gilt $f_K^{-1} = f_{K'}$, dass man aber aus der Kenntnis von K allein das zugehörige K' praktisch nicht berechnen kann.

Was kann man damit anfangen?
Wir denken uns ein System mit vielen Teilnehmern, die verschlüsselt Nachrichten austauschen wollen.

(1) Jeder Teilnehmer A wählt sich Parameter K_A und K'_A, sodass $f_{K_A}^{-1} = f_{K'_A}$ gilt, was nach Eigenschaft 3 möglich ist.

(2) In einer Liste (Telefonbuch) werden die Daten (A, K_A) öffentlich zugänglich gemacht. K_A (und damit f_{K_A}) ist also allgemein bekannt, man nennt dies den **öffentlichen Schlüssel - public key** - von A. Allerdings ist K'_A nur A selbst bekannt; man nennt K'_A daher den **privaten Schlüssel - private key** - von A.

(3) Will ein Teilnehmer B eine Nachricht vertraulich an A schicken, wandelt er sie in eine Folge $a_1, a_2, a_3, \ldots$ von Nachrichteneinheiten um, besorgt sich den öffentlichen Schlüssel K_A von A,

Datei: ki_pkv_rsa_0.tex. Version vom 14.6.2018

berechnet $b_i = f_{K_A}(a_i)$, was wegen Eigenschaft $\boxed{1}$ praktisch schnell funktioniert, und schickt $b_1, b_2, b_3, \dots$ an A.

(4) Erhält A die Chiffretextfolge $b_1, b_2, b_3, \dots$ berechnet er mit seinem privaten Schlüssel K'_A

$$f_{K'_A}(b_i) = f^{-1}_{K_A}(b_i) = f^{-1}_{K_A}(f_{K_A}(a_i)) = a_i$$

und erhält damit die ursprüngliche Nachricht $a_1, a_2, a_3, \dots$.

(5) Was passiert, wenn ein Außenstehender C an die verschlüsselte Nachricht $b_1, b_2, b_3, \dots$ kommt? C kann sich den öffentlichen Schlüssel K_A von A besorgen und müsste dann nur

$$f^{-1}_{K_A}(b_i)$$

berechnen. Allerdings ist dies praktisch wegen der geforderten Eigenschaft $\boxed{2}$ im Allgemeinen nicht möglich. Daher kann ein Außenstehender den Chiffretext nicht entschlüsseln.

(6) Ein großer Vorteil eines solchen Verschlüsselungsverfahrens ist, dass man kein Problem mit dem Schlüsselaustausch hat, da die Schlüssel K_A öffentlich zugänglich sind. Außerdem können leicht neue Teilnehmer C dazu kommen; sie müssen nur ihre Daten (C, f_{K_C}) in die öffentliche Liste (Telefonbuch) eintragen lassen.

Natürlich stellt sich nun die Frage, ob man tatsächlich Funktionen f_K mit den oben geforderten Eigenschaften finden kann.

3. RSA

Das wohl bekannteste Public-Key-Verfahren geht auf Rivest, Shamir und Adleman (1977) zurück - daher die Bezeichnung RSA. Wir beginnen mit der Mathematik.

LEMMA. *Seien p und q verschiedene ungerade Primzahlen, $N = pq$, $e, d \in \mathbb{N}$ mit $ed \equiv 1 \bmod (p-1)(q-1)$. Dann gilt für $a, b \in \mathbb{Z}$ die Implikation*

$$b \equiv a^e \bmod N \quad \Longrightarrow \quad a \equiv b^d \bmod N.$$

Beweis: Wir müssen zeigen, dass für alle $a \in \mathbb{Z}$ gilt

$$a^{ed} \equiv a \bmod N.$$

Wegen $ed \equiv 1 \bmod (p-1)(q-1)$ gibt es ein $k \in \mathbb{N}_0$ mit $ed = 1 + k(p-1)(q-1)$. Sei $a \in \mathbb{Z}$ beliebig.

- Wir zeigen zunächst, dass $a^{ed} \equiv a \bmod p$ gilt.
  - Ist $a \equiv 0 \bmod p$, so gilt offensichtlich $a^{ed} \equiv 0 \equiv a \bmod p$.
  - Ist $a \not\equiv 0 \bmod p$, so ist $a^{p-1} \equiv 1 \bmod p$ nach dem kleinen Satz von Fermat und es folgt

$$a^{ed} \equiv a^{1+k(p-1)(q-1)} \equiv a \cdot \left(a^{p-1}\right)^{k(q-1)} \equiv a \cdot 1 \equiv a \bmod p.$$

- Genauso zeigt man $a^{ed} \equiv a \bmod q$.

Aus $a^{ed} \equiv a \bmod p$ und $a^{ed} \equiv a \bmod q$ folgt $p \mid a^{ed} - a$ und $q \mid a^{ed} - a$ und damit $pq \mid a^{ed} - a$, also $a^{ed} \equiv a \bmod N$, was gezeigt werden sollte. ■

Bemerkungen:

(1) Wegen $\varphi(pq) = (p-1)(q-1)$ für verschiedene Primzahlen p und q, lässt sich die Bedingung $ed \equiv 1 \bmod (p-1)(q-1)$ natürlich auch in der Form

$$ed \equiv 1 \bmod \varphi(N)$$

schreiben.

(2) Geht man den Beweis durch, so sieht man, dass die Folgerung auch gilt, wenn man nur $ed \equiv 1 \bmod \mathrm{kgV}(p-1, q-1)$ fordert. Wir werden aber meist die Beziehung $ed \equiv 1 \bmod (p-1)(q-1)$ benutzen, da sich dies einfacher handhaben lässt.

RSA-Verschlüsselung:

(1) **Schlüsselerzeugung:** Zur Erstellung eines Schlüssels geht eine Person A folgendermaßen vor:

(a) A wählt sich (mit Hilfe eines Primzahltests) verschiedene ungerade Primzahlen p_A und q_A und berechnet dann
$$N_A = p_A q_A.$$
Die Primzahlen p_A und q_A sollten so gewählt sein, dass N_A mit den gängigen Faktorisierungsmethoden praktisch nicht faktorisiert werden kann.

(b) A wählt sich eine natürliche Zahl $e_A > 1$ mit $\mathrm{ggT}(e_A, (p_A-1)(q_A-1)) = 1$ und berechnet sich (beispielsweise mit Hilfe des erweiterten euklidischen Algorithmus) eine natürliche Zahl d_A mit
$$e_A d_A \equiv 1 \bmod (p_A-1)(q_A-1),$$
also ein Inverses von e_A modulo $(p_A-1)(q_A-1)$.

A gibt (N_A, e_A) als seinen öffentlichen Schlüssel bekannt und hebt sich (N_A, d_A) als seinen privaten/geheimen Schlüssel auf.

(2) **Verschlüsselung:** Will eine Person B eine Nachricht verschlüsselt an A schicken, geht B folgendermaßen vor:

(a) B besorgt sich den öffentlichen Schlüssel (N_A, e_A) von A.

(b) Nach einem vereinbarten Verfahren wandelt B seine Nachricht in eine Zahlenfolge $a_1, a_2, a_3, \ldots$ mit $0 \le a_i \le N_A - 1$ um. (Nachfolgend werden Umwandlungsmöglichkeiten beschrieben.)

(c) B berechnet (mit der square-and-multiply-Methode)
$$b_i = a_i^{e_A} \bmod N_A.$$

(d) B schickt die Zahlenfolge $b_1, b_2, b_3, \ldots$ an B. (Die Zahlenfolge $b_1, b_2, b_3, \ldots$ ist also der Chiffretext.)

(3) **Entschlüsselung:** A erhält von B die Zahlenfolge $b_1, b_2, b_3, \ldots$

(a) A berechnet sich mit seinem privaten Schlüssel (N_A, d_A) unter Verwendung der square-and-multiply-Methode
$$a_i = b_i^{d_A} \bmod N_A.$$
(Das letzte Lemma garantiert die vorangegangene Gleichheit.)

(b) Die Zahlenfolge $a_1, a_2, a_3, \ldots$ wandelt A nach dem vereinbarten Schema in Text um und hat damit die Nachricht, die ihm B schicken wollte.

Bemerkungen:

(1) Mit den in der Vorlesung behandelten Methoden kann sich ein Teilnehmer A schnell passende Zahlen p_A, q_A, $N_A = p_A q_A$, e_A und d_A mit $e_A d_A \equiv 1 \bmod (p_A-1)(q_A-1)$ bestimmen. Wie groß N_A sein muss, dass es von Außenstehenden nicht faktorisiert werden kann, muss man testen. (Das BSI empfiehlt zur Zeit (2018) bis Ende 2022 eine Schlüssellänge von mindestens 2000 Bit, danach eine Schlüssellänge von 3000 Bit.)

(2) Ver- und Entschlüsselung funktionieren bei Kenntnis des öffentlichen bzw. privaten Schlüssels mit der square-and-multiply-Methode schnell.

(3) Es ist bis heute kein Verfahren bekannt, wie man bei Kenntnis von N und e für (allgemeines) b die Gleichung
$$x^e \equiv b \bmod N$$
lösen kann (Bestimmung der e-ten Wurzel modulo N), wenn man die Faktorisierung von N nicht kennt. Kennt man die Faktorisierung $N = pq$ von N, so kann man sich mit dem erweiterten euklidischen Algorithmus ein $d \in \mathbb{N}$ mit $ed \equiv 1 \bmod (p-1)(q-1)$ berechnen. Dann ist
$$b^d \bmod N$$
eine Lösung der Gleichung.

(4) Es ist auch kein Verfahren bekannt, wie man ohne Kenntnis der Faktorisierung den privaten Schlüssel bestimmen kann, wenn er nicht zu klein ist.

Umwandlung von Text in Zahlenfolgen – ein allgemeiner Ansatz:

(1) Es liege ein Alphabet zugrunde, dessen Zeichen wir mit einer Teilmenge von $\{0, 1, \ldots, n-1\}$ identifizieren.

(2) Ist eine große Zahl N gegeben und soll der Text in Zahlen a mit $0 \le a \le N-1$ umgewandelt werden, wählen wir k mit $n^k \le N$, z.B. das maximale k.
(3) Wir fassen nun jeweils k Zeichen unseres Textes zu einem Block zusammen, wobei man sich noch darauf einigen muss, was mit dem letzten Block passiert, wenn er nicht vollständig ist.
(4) Ist $c_1, c_2, \dots, c_k$ ein Block, wobei wir nun $c_i \in \{0, 1, \dots, n-1\}$ annehmen, so bilden wir

$$a = c_1 n^{k-1} + c_2 n^{k-2} + \cdots + c_{k-1} n + c_k,$$

was man leicht rekursiv durch

$$a = (\dots(((c_1 n + c_2)n + c_3)n + c_4)\dots)n + c_k$$

berechnen kann. Dann gilt $0 \le a \le n^k - 1 \le N - 1$, was wir haben wollten.

Umwandlung von Text in Zahlenfolgen – ein Beispiel:
Das Alphabet bestehe aus den Großbuchstaben A,...,Z und dem Leerzeichen. In einem Text (oder Textblock) wird jedes A durch 01, jedes B durch 02, ..., jedes Z durch 26 und jedes Leerzeichen durch 00 ersetzt:

Leerzeichen	A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Besteht ein Text (oder Textblock) aus k Zeichen, so erhält man eine Zahl mit $2k$ Ziffern, die zwischen 0 (lauter Leerzeichen) und $262626\dots26$ (lauter Z) liegt.

Beispiel: Mit dem beschriebenen Verfahren wird „HEUTE IST FREITAG“ zu 8052120050009192000061805092001 07.
Soll man den Text zuerst in Blöcke der Länge 4 einteilen, so ergibt sich

HEUT	E IS	T FR	EITA	G
08052120	5000919	20000618	5092001	7000000

Also erhält man die Zahlenfolge 8052120, 5000919, 20000618, 5092001, 7000000.

Beispiel:
(1) Teilnehmer A wählt sich zunächst $p_A = 401$, $q_A = 503$ und damit $N_A = 201703$. Es ist $\mathrm{ggT}(3, (p_A-1)(q_A)-1)) = 1$, weswegen $e_A = 3$ als öffentlicher Exponent gewählt werden kann. Es $e_A d_A \equiv 1 \bmod (p_A-1)(q_A-1)$ erhält man den privaten Exponenten $d_A = 133867$. Der öffentliche Schlüssel ist also $(N_A, e_A) = (201703, 3)$, der private $(N_A, d_A) = (201703, 133867)$. Wenn wir obige Umwandlung von Text in Zahlenfolgen wählen, müssen wir den Text vorher in Blöcke der Länge 2 einteilen, damit die sich ergebenden Zahlen $< N_A$ sind.
(2) Wir wollen den Text „KRYPTOGRAPHIE“ verschlüsselt an A senden. Wir wandeln zunächst in eine Zahlenfolge a_i um, wobei wir wegen Blocklänge 2 ein Leerzeichen ergänzen. Dann berechnen wir $b_i = a_i^{e_A} \bmod N_A$.

Textblock	KR	YP	TO	GR	AP	HI	E
a_i	1118	2516	2015	0718	0116	0809	0500
$b_i = a_i^{e_A} \bmod N_A$	16648	51810	77992	21227	148975	4754	145843

Der Chiffretext besteht also aus der Zahlenfolge

$$16648, \quad 51810, \quad 77992, \quad 21227, \quad 148975, \quad 4754, \quad 145843.$$

(3) Wir nehmen an, A empfängt als Chiffretext die Zahlenfolge

$$121487, \quad 67566, \quad 50625,$$

die wir mit b_i bezeichen. Wir berechnen mit dem privaten Schlüssel (N_A, d_A) die Zahlenfolge $a_i = b_i^{d_A} \bmod N_A$ und erhalten

$$2601, \quad 812, \quad 514,$$

was der Folge 2601, 0812, 0514 entspricht und somit den Text ‘ZAHLEN’ ergibt.

Beispiel: Die Erfinder von RSA stellten im August 1977 im Scientific American folgende Aufgabe: Ein aus Großbuchstaben A,...,Z und Leerzeichen bestehender Text wurde nach obigem Verfahren in eine Zahl a umgewandelt. Dann wurde $b \equiv a^e \bmod N$ berechnet und die Zahlen N, e und b wie folgt angegeben:

$$\begin{aligned} N &= 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541, \\ e &= 9007, \\ b &= 968696137546220614771409222543558829057599911245743198746951209308162982251457083569314766228839896280133919905518299451578151 54. \end{aligned}$$

Aus diesen Angaben sollte der Ausgangstext rekonstruiert werden.
Die Aufgabe wurde erst nach Faktorisierung der Zahl N, die auch unter der Bezeichnung RSA-129 bekannt ist, im Jahre 1994 gelöst. Mit den Primfaktoren p und q berechnet man $d = \frac{1}{e} \bmod (p-1)(q-1)$, damit $a = b^d \bmod N$:

$$\begin{aligned} p &= 3490529510847650949147849619903898133417764638493387843990820577, \\ q &= 32769132993266709549961988190834461413177642967992942539798288533, \\ d &= 106698614368578024442868771328920154780709906633937862801226224496631063125911774470873340168597462306553968544513277109053606095, \\ a &= 200805001301070903002315180419000118050019172105011309190800151919090618010705. \end{aligned}$$

Wandelt man a nach obigem Verfahren in Text um, so erhält man als Lösung den Satz „THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE“.

Bemerkung: Unter einer RSA-Zahl verstehen wir eine natürliche Zahl N, die eine Primfaktorzerlegung $N = pq$ mit verschiedenen ungeraden Primzahlen p und q hat.

4. Ein Angriff auf RSA mit dem chinesischen Restsatz

Bemerkung: Die Wahl eines kleinen öffentlichen RSA-Exponenten e, beispielsweise $e = 3$, hat den Vorteil, dass die Verschlüsselung schnell geht. Verwenden aber mehrere Personen den gleichen kleinen öffentlichen Exponenten e, und wird der Text in Zahlenfolgen ungünstig umgesetzt, so kann das zur Entschlüsselung benutzt werden, wie folgendes Lemma zeigen wird:

LEMMA. *N_1, N_2, N_3 seien paarweise teilerfremde natürliche Zahlen, a eine ganze Zahl mit $0 \le a < N_i$ für $i = 1, 2, 3$ und*

$$b_i \equiv a^3 \bmod N_i \quad \text{für} \quad i = 1, 2, 3.$$

Es gibt ein $c \in \mathbb{Z}$ mit

$$c \equiv b_i \bmod N_i \text{ für } i = 1, 2, 3 \quad \text{und} \quad 0 \le c < N_1 N_2 N_3,$$

das man mit dem chinesischen Restsatz bestimmen kann. Dann gilt (in $\mathbb{Z}$)

$$c = a^3,$$

also $a = \sqrt[3]{c}$, d.h. a lässt sich aus b_1, b_2, b_3 und N_1, N_2, N_3 berechnen.

Beweis: Aus $0 \le a < N_i$ folgt $0 \le a^3 < N_1 N_2 N_3$. Die Kongruenzgleichungen liefern $c \equiv b_i \equiv a^3 \bmod N_i$ für $i = 1, 2, 3$, was wegen der Teilerfremdheit von N_1, N_2, N_3 zu $c \equiv a^3 \bmod N_1 N_2 N_3$ führt. Wegen $0 \le c, a^3 < N_1 N_2 N_3$ folgt dann aber sofort $a = c^3$, wie behauptet. ■

Angriff auf RSA bei gemeinsamem kleinen öffentlichen Verschlüsselungsexponenten: Wir nehmen an, B will an drei Personen A_1, A_2, A_3 mit öffentlichen RSA-Schlüsseln $(N_i, 3)$ ein und dieselbe Nachricht RSA-verschlüsselt schicken. Die Nachricht liege in Form einer Zahlenfolge a_i mit $0 \le a_i \le \min(N_1, N_2, N_3)$ vor, sodass B zur Chiffrierung die Zahlenfolgen

$$b_{1,i} = a_i^3 \bmod N_1, \quad b_{2,i} = a_i^3 \bmod N_2, \quad b_{3,i} = a_i^3 \bmod N_3$$

berechnet und an B_1 bzw. B_2 bzw. B_3 schickt.
Kommt ein Außenstehender C an die chiffrierten Zahlenfolgen $b_{1,i}$, $b_{2,i}$, $b_{3,i}$ und die öffentlichen Schlüssel $(N_1, 3)$, $(N_2, 3)$, $(N_3, 3)$, so berechnet er mit dem chinesischen Restsatz c_i mit $0 \leq c_i < N_1N_2N_3$ aus den Kongruenzgleichungen

$$c_i \equiv \begin{cases} b_{1,i} \bmod N_1, \\ b_{2,i} \bmod N_2, \\ b_{3,i} \bmod N_3. \end{cases}$$

Nach dem vorangegangenen Lemma gilt $c_i = a_i^3$, sodass C durch Kubikwurzelziehen die Ausgangsfolge erhält:

$$a_i = \sqrt[3]{c_i}.$$

Beispiel: Jemand sendet an drei Personen mit den RSA-Schlüsseln

$$(N_1, e_1) = (44929, 3), \quad (N_2, e_2) = (61423, 3), \quad (N_3, e_3) = (53491, 3)$$

eine verschlüsselte Zahlenfolge $(b_{j,1}, b_{j,2}, b_{j,3})$. Ein Unbefugter berechnet sich mit dem chinesischen Restsatz c_1, c_2, c_3 mit $c_1 \equiv b_{j,1} \bmod N_j$ für $j = 1, 2, 3$, und analog c_2 und c_3. Die c_i's sind dritte Potenzen, also $c_i = a_i^3$, was die ursprüngliche Nachricht 'GEHEIM' ergibt.

i	1	2	3
$b_{1,i}$	1354	34435	41095
$b_{2,i}$	45833	56009	17527
$b_{3,i}$	36575	15893	32040
c_i	350402625	521660125	761048497
$a_i = \sqrt[3]{c_i}$	0705	0805	0913
Text	GE	HE	IM

Bemerkung: Im letzten Angriff muss man die 3. Wurzel ziehen. Dafür kann man eventuell nachfolgendes Intervallschachtelungsverfahren benutzen. Es funktioniert, wenn k nicht zu groß ist.

Algorithmus $\lfloor \sqrt[k]{n} \rfloor$ - ganzzahliger Anteil der k-ten Wurzel aus n

Eingabe: $k, n \in \mathbb{N}$
Ausgabe: $\lfloor \sqrt[k]{n} \rfloor$

```
L, R ← 1, n                          ▷ Immer gilt L^k ≤ n < R^k
while R − L ≥ 2 do
    M ← ⌊(L+R)/2⌋
    if M^k ≤ n then
        L ← M
    else
        R ← M
    end if
end while
return L
```

5. Faktorisierung einer RSA-Zahl N bei Kenntnis des öffentlichen und privaten Schlüssels I

Bemerkungen:

(1) RSA-Situation: Es gibt verschiedene ungerade Primzahlen p, q, $N = pq$, Zahlen e, d mit $ed \equiv 1 \bmod (p-1)(q-1)$ und $1 < e, d < (p-1)(q-1)$.

(2) Sei $s = p + q$. Dann gilt

$$(x-p)(x-q) = x^2 - (p+q)x + pq = x^2 - sx + N,$$

d.h. die Nullstellen des Polynoms $x^2 - sx + N$ sind p und q. Da man die Nullstellen auch mit der bekannten Formel ausrechnen kann, erhält man

$$\{p,q\} = \left\{ \frac{s+\sqrt{s^2-4N}}{2}, \frac{s-\sqrt{s^2-4N}}{2} \right\}.$$

Kennt man also s (und N), so kann man auch p und q bestimmen.

(3) Es ist $\varphi(N) = (p-1)(q-1) = pq - (p+q) + 1 = N + 1 - s$. Kennt man also N und $\varphi(N)$, so kann man s und damit p und q bestimmen.

(4) Wegen $ed \equiv 1 \bmod (p-1)(q-1)$ gibt es ein $k \in \mathbb{Z}$ mit

$$ed = 1 + k(p-1)(q-1).$$

Schreiben wir wieder $s = p + q$, so lässt sich die letzte Gleichung auch in der Form

$$ed = 1 + k(N + 1 - s)$$

schreiben. Ist nur der öffentliche Schlüssel (N, e) bekannt, so ist dies eine Gleichung mit drei Unbekannten d, k, s. Im Folgenden werden wir voraussetzen, dass wir auch d kennen. Dann bleiben die beiden Unbekannten k und s. Wenn man ein paar Ungleichungen fordert, kann man praktisch k bestimmen und damit dann auch s, also die Primfaktorzerlegung von N.

(5) Ist $ed = 1 + k(p-1)(q-1)$ und $1 < e, d < (p-1)(q-1)$, so folgt

$$k = \frac{ed-1}{(p-1)(q-1)}.$$

Wegen $e, d > 1$ ist $k \in \mathbb{N}$. Wegen $d < (p-1)(q-1)$ ist

$$k = \frac{ed-1}{(p-1)(q-1)} < \frac{ed}{(p-1)(q-1)} = e \cdot \frac{d}{(p-1)(q-1)} < e, \quad \text{und ganz analog} \quad k < d.$$

Insgesamt:

$$1 \le k < e \quad \text{und} \quad 1 \le k < d.$$

LEMMA. *Ist $N = pq$ eine RSA-Zahl mit $p < q < \lambda p$, so gilt*

$$2\sqrt{N} < p + q < (\sqrt{\lambda} + \frac{1}{\sqrt{\lambda}})\sqrt{N}.$$

Im Fall $p < q < 2p$ erhalten wir

$$2\sqrt{N} < p + q < \frac{3}{\sqrt{2}}\sqrt{N}.$$

Beweis: Wir schreiben $p = \frac{1}{u}\sqrt{N}$, $q = u\sqrt{N}$. Nun gelten die Äquivalenzen

$$p < q < \lambda p \quad \Longleftrightarrow \quad \frac{1}{u}\sqrt{N} < u\sqrt{N} < \lambda\frac{1}{u}\sqrt{N} \quad \Longleftrightarrow \quad 1 < u^2 < \lambda \quad \Longleftrightarrow \quad 1 < u < \sqrt{\lambda}.$$

Da die Funktion $x \mapsto x + \frac{1}{x}$ (mit Ableitung $1 - \frac{1}{x^2}$) für $x \ge 1$ streng monoton wachsend ist, folgt

$$2\sqrt{N} = (1 + \frac{1}{1})\sqrt{N} < (u + \frac{1}{u})\sqrt{N} < (\sqrt{\lambda} + \frac{1}{\sqrt{\lambda}})\sqrt{N},$$

woraus die allgemeine Behauptung folgt. Für $\lambda = 2$ ist

$$\sqrt{\lambda} + \frac{1}{\sqrt{\lambda}} = \sqrt{2} + \frac{1}{\sqrt{2}} = \frac{3}{\sqrt{2}},$$

was den Rest beweist. ■

SATZ. *Seien p und q verschiedene ungerade Primzahlen, $N = pq$, seien $e, d \in \mathbb{N}$ mit $ed \equiv 1 \bmod (p-1)(q-1)$ und $3 \leq e, d < (p-1)(q-1)$. Dann gibt es $k \in \mathbb{N}$ mit $ed = 1 + k(p-1)(q-1)$. ((N, e) ist also ein öffentlicher RSA-Schlüssel, (N, d) ein zugehöriger privater RSA-Schlüssel.) Es gebe ein $\lambda \in \mathbb{R}_{>1}$ mit $p < q < \lambda p$. Dann gilt*

$$\left\lfloor \frac{ed}{N} \right\rfloor + 1 \leq k < \left\lfloor \frac{ed}{N} \right\rfloor + 1 + \frac{e}{\sqrt{N}} \left(\sqrt{\lambda} + \frac{1}{\sqrt{\lambda}} \right).$$

Insbesondere gilt im Fall $p < q < 2p$ und $e \leq 0.47\sqrt{N}$

$$k = \left\lfloor \frac{ed}{N} \right\rfloor + 1.$$

Beweis:

(1) Die Voraussetzung $ed \equiv 1 \bmod (p-1)(q-1)$ liefert sofort, dass eine ganze Zahl k existiert mit $ed = 1 + k(p-1)(q-1)$. Wegen $e, d \geq 3$ ist $k \geq 1$. Auflösung nach k ergibt

$$k = \frac{ed - 1}{(p-1)(q-1)}.$$

(2) Mit $k(p+q-1) - 1 \geq (p+q-1) - 1 \geq 3 + 5 - 2 \geq 6 > 0$ ergibt sich

$$ed = 1 + k(p-1)(q-1) = 1 + k(N + 1 - p - q) = kN - \Big(k(p+q-1) - 1 \Big) < kN,$$

also

$$k > \frac{ed}{N}.$$

(3) Weiter gilt

$$\begin{aligned} k - \frac{ed}{N} &= \frac{ed-1}{(p-1)(q-1)} - \frac{ed}{N} < \frac{ed}{(p-1)(q-1)} - \frac{ed}{N} = \\ &= \frac{ed(N - (p-1)(q-1))}{(p-1)(q-1)N} = \frac{d}{(p-1)(q-1)} \cdot \frac{e(N - (N+1-p-q))}{N} < \\ &< \frac{e(p+q-1)}{N} < \frac{e(p+q)}{N}. \end{aligned}$$

Die Voraussetzung $p < q < \lambda q$ liefert mit dem vorangegangenen Lemma $p + q < (\sqrt{\lambda} + \frac{1}{\sqrt{\lambda}})\sqrt{N}$, sodass nun

$$k - \frac{ed}{N} < \frac{e}{\sqrt{N}} (\sqrt{\lambda} + \frac{1}{\sqrt{\lambda}})$$

folgt.

(4) Insgesamt ergibt sich

$$\frac{ed}{N} < k < \frac{ed}{N} + \frac{e}{\sqrt{N}} \left(\sqrt{\lambda} + \frac{1}{\sqrt{\lambda}} \right)$$

und damit

$$\left\lfloor \frac{ed}{N} \right\rfloor + 1 \leq k < \left\lfloor \frac{ed}{N} \right\rfloor + 1 + \frac{e}{\sqrt{N}} \left(\sqrt{\lambda} + \frac{1}{\sqrt{\lambda}} \right).$$

(5) Ist $\lambda = 2$, so ist

$$\frac{e}{\sqrt{N}} \left(\sqrt{\lambda} + \frac{1}{\sqrt{\lambda}} \right) = \frac{e}{\sqrt{N}} \cdot \frac{3}{\sqrt{2}}.$$

Ist $e \leq 0.47\sqrt{N}$, so folgt

$$\frac{e}{\sqrt{N}} \left(\sqrt{\lambda} + \frac{1}{\sqrt{\lambda}} \right) = \frac{e}{\sqrt{N}} \cdot \frac{3}{\sqrt{2}} \leq 0.47 \cdot \frac{3}{\sqrt{2}} < 1,$$

damit

$$\left\lfloor \frac{ed}{N} \right\rfloor + 1 \leq k < \left\lfloor \frac{ed}{N} \right\rfloor + 1 + 1$$

und damit

$$k = \left\lfloor \frac{ed}{N} \right\rfloor + 1.$$

Dies war zu zeigen. ■

Bemerkung: Die Idee ist bei A. May, „Computing the RSA Secret Key is Deterministic Polynomial Time Equivalent to Factoring“ zu finden. Allerdings findet sich dort die Bedingung $ed \leq N^{\frac{3}{2}}$.

Anwendung:

(1) Wir nehmen an, wir sind in der Situation des Satzes. Wir definieren für $i = 1, 2, 3, \ldots$

$$k_i = \left\lfloor \frac{ed}{N} \right\rfloor + i.$$

(2) Sei wie früher $s = p + q$ und $\Delta = q - p$.

(3) Ist i der Index mit $k = k_i$, so folgt aus $ed - 1 = k(N - s + 1)$ zunächst

$$k \mid ed - 1,$$

dann

$$s = N + 1 - \frac{ed - 1}{k}.$$

Außerdem gilt

$$s^2 - 4N = \Delta^2$$

und

$$p = \frac{s - \Delta}{2}, \quad q = \frac{s + \Delta}{2}.$$

Verfahren zur Faktorisierung einer RSA-Zahl bei Kenntnis des öffentlichen und privaten Schlüssels: Gegeben sei ein öffentlicher RSA-Schlüssel (N, e) und ein zugehöriger privater RSA-Schlüssel (N, d) (mit $3 \leq e, d < \varphi(N)$ und $e \leq \sqrt{N}$). Außerdem werde angenommen, dass die Primteiler p und q nicht zu weit auseinanderliegen.

(1) Setze

$$k := \left\lfloor \frac{ed}{N} \right\rfloor.$$

(2) Setze $k := k + 1$.

(3) Teste, ob $k \mid ed - 1$ gilt. Wenn nicht, gehe zu (2).

(4) Berechne $s = N + 1 - \frac{ed-1}{k}$ und damit $\Delta = \left\lfloor \sqrt{s^2 - 4N} \right\rfloor$.

(5) ist $s^2 - 4N \neq \Delta^2$, gehe zu (2).

(6) Gib $\frac{s-\Delta}{2}$ und $\frac{s+\Delta}{2}$ als die Primteiler von N aus.

Beispiele: Bei den folgenden Beispielen bleibt e in der Größenordnung von $\sqrt{N}$.

(1)

$$\begin{aligned}
N &= 139010512803754921786716297874540281597289220705030553510293 \\
e &= 49824531331703126978755621230 5 \\
d &= 456793879093180769335771109895173853501633355042644882742 13 \\
\frac{e}{\sqrt{N}} &= 1.33635 \\
\left\lfloor \frac{ed}{N} \right\rfloor &= 163725321790148949313930547142 \\
k - \left\lfloor \frac{ed}{N} \right\rfloor &= 1 \\
p &= 255920363387062222749920110667 \\
q &= 543178787979098532151264702879
\end{aligned}$$

(2)

$$\begin{aligned}
N &= 1403819239748557680296696997961634668083663028611248409117 11\\
e &= 55098316257792105416155572703 1\\
d &= 113149403655116265863410427029423248037917480092315666421767\\
\frac{e}{\sqrt{N}} &= 1.47056\\
\left\lfloor \frac{ed}{N} \right\rfloor &= 444098602615449682560506277165\\
k - \left\lfloor \frac{ed}{N} \right\rfloor &= 3\\
p &= 205326473383705743094294669273\\
q &= 6837010428388148046202404316 07
\end{aligned}$$

(3)

$$\begin{aligned}
N &= 3669988547980685723732436000102132000912701786107516511734 79\\
e &= 67666251299650967652078225318 89\\
d &= 323044359824672524832888467234714984077389072847622408016009\\
\frac{e}{\sqrt{N}} &= 11.16966\\
\left\lfloor \frac{ed}{N} \right\rfloor &= 595620409901785934554628956690 5\\
k - \left\lfloor \frac{ed}{N} \right\rfloor &= 22\\
p &= 908834098512114777456086162251\\
q &= 403812814020617944494374518229
\end{aligned}$$

(4)

$$\begin{aligned}
N &= 3369679260748236735952710920310966005950441951852641517263 17\\
e &= 54939858859780228709091566648759\\
d &= 183235530174935013282400285407603688739743612618871676152999\\
\frac{e}{\sqrt{N}} &= 94.64404\\
\left\lfloor \frac{ed}{N} \right\rfloor &= 298750515610573859891757424750 09\\
k - \left\lfloor \frac{ed}{N} \right\rfloor &= 106\\
p &= 714621781372694505117493885189\\
q &= 471533242980017460391941911753
\end{aligned}$$

(5)

$$\begin{aligned}
N &= 728008782790287075032737418240952516312144219193225419022193\\
e &= 83898705771529586918972087414687\\
d &= 67083650229737107647915911820012528139856989599236751356276 3\\
\frac{e}{\sqrt{N}} &= 98.33021\\
\left\lfloor \frac{ed}{N} \right\rfloor &= 773099386402073958082916063481 03\\
k - \left\lfloor \frac{ed}{N} \right\rfloor &= 182\\
p &= 92230738148052993600869876887 9\\
q &= 78933422566959631659095494876 7
\end{aligned}$$

(6)

$$\begin{aligned}
N &= 450304253127936195502465221742026279990135117178097812675349\\
e &= 84298487326332209917557744587273\\
d &= 28717030706461216723832189572866038792881286041594939315564 1\\
\frac{e}{\sqrt{N}} &= 125.62230\\
\left\lfloor \frac{ed}{N} \right\rfloor &= 537592579293435697010041012054 99\\
k - \left\lfloor \frac{ed}{N} \right\rfloor &= 173\\
p &= 45498350651303665166225903635 7\\
q &= 98971555382092431647867227905 7
\end{aligned}$$

Beispiele: Die folgenden Beispiele sollen zeigen, dass der vorangegangene Algorithmus nicht mehr brauchbar ist, wenn e deutlich größer als $\sqrt{N}$ wird. Dann wird nämlich auch die Schrittzahl $k - \left\lfloor \frac{ed}{N} \right\rfloor$ schnell groß.

(1)

$$\begin{aligned}
N &= 429021855963920931789425735034459318819961363547086133857163\\
e &= 43347812661715330707142559755637 1397\\
d &= 10821265403882398090407999294086644875890459909047963632481 3\\
\frac{e}{\sqrt{N}} &= 661801.09154\\
\left\lfloor \frac{ed}{N} \right\rfloor &= 109336664081198494359454886256463166\\
k - \left\lfloor \frac{ed}{N} \right\rfloor &= 352190\\
p &= 47092580599342653725421124952 3\\
q &= 91101793637936561551473108468 1
\end{aligned}$$

(2)

$$\begin{aligned}
N &= 1465982127791040759259035723796218141287596343051605076222 17\\
e &= 92182802090453171717562164384822014043810485720807\\
d &= 10687880867325546252433281259279000803863329419586877579 9583\\
\frac{e}{\sqrt{N}} &= 240760683410862866432.00000\\
\left\lfloor \frac{ed}{N} \right\rfloor &= 67206740660855213245179209361738934947581129123870\\
k - \left\lfloor \frac{ed}{N} \right\rfloor &= 354604328365283507208\\
p &= 33218730976583659635214631 2847\\
q &= 44131189985084972832128740 4711
\end{aligned}$$

6. Faktorisierung einer RSA-Zahl bei Kenntnis eines „Exponenten“ für $(\mathbb{Z}/N\mathbb{Z})^*$

Im Folgenden skizzieren wir ein Verfahren, das praktisch sehr schnell ist, von dem aber keine gute Laufzeitabschätzung existiert.

Sei $N = pq$ eine RSA-Zahl, (N, e) ein öffentlicher und (N, d) ein zugehöriger privater RSA-Schlüssel. Dann gilt

$$a^{ed} \equiv a \bmod N \text{ für alle } a \in \mathbb{Z},$$

und damit

$$a^{ed-1} \equiv 1 \bmod N \text{ für alle } a \in \mathbb{Z} \text{ mit } \mathrm{ggT}(N, a) = 1.$$

Wir betrachten nun allgemeiner den Fall, dass wir eine Zahl $m \in \mathbb{N}$ kennen mit der Eigenschaft

$$a^m \equiv 1 \bmod N \text{ für alle } a \in \mathbb{Z} \text{ mit } \mathrm{ggT}(N, a) = 1.$$

Unter einem „Exponenten“ für die Gruppe $(\mathbb{Z}/N\mathbb{Z})^*$ verstehen wir eine solche Zahl m.
Wir zerlegen

$$m = 2^\ell u \text{ mit } u \equiv 1 \bmod 2.$$

Ist nun $a \in \mathbb{Z}$ mit $\mathrm{ggT}(N, a) = 1$, so gilt

$$a^{2^\ell u} \equiv 1 \bmod N.$$

Wie beim Miller-Rabin-Test berechnen wir zuerst $a^u \bmod N$ und quadrieren wir dann sukzessive. Wir unterscheiden zwei Fälle:

- *Fall $a^u \equiv 1 \bmod N$:* Auch alle Potenzen $a^{2^i u}$ sind dann 1 modulo N.
- *Fall $a^u \not\equiv 1 \bmod N$:* Wegen $a^{2^\ell u} \equiv 1 \bmod N$ gibt es (genau) eine Zahl $i \in \{0, 1, \ldots, \ell - 1\}$ mit

  $$a^{2^i u} \not\equiv 1 \bmod N \text{ und } a^{2^{i+1} u} \equiv 1 \bmod N.$$

  Es gilt dann

  $$\left(a^{2^i u}\right)^2 \equiv a^{2^{i+1} u} \equiv 1 \bmod N,$$

  d.h. $a^{2^i u} \bmod N$ ist eine Quadratwurzel von 1 modulo N.

Satz. *Sei $N = pq$ eine RSA-Zahl und*

$$Q_N = \{a \in \mathbb{Z} : 0 \le a \le N - 1, a^2 \equiv 1 \bmod N\},$$

d.h. Q_N ist die Menge der Quadratwurzeln von 1 modulo N.

(1) *Es gibt Zahlen* $\alpha, \beta \in \mathbb{Z}$ *mit* $0 \le \alpha \le N-1$, $0 \le \beta \le N-1$ *und*

$$\alpha \equiv \begin{cases} 1 \bmod p, \\ -1 \bmod q \end{cases} \quad \textit{und} \quad \beta \equiv \begin{cases} -1 \bmod p, \\ 1 \bmod q. \end{cases}$$

(Kennt man p *und* q *kann man sie mit dem chinesischen Restsatz bestimmen.) Es gilt*

$$\beta = N - \alpha.$$

(2) *Es ist*

$$Q_N = \{1, \alpha, \beta, N-1\}.$$

(3) *Es gilt*

$$\mathrm{ggT}(N, \alpha - 1) = p \quad \textit{und} \quad \mathrm{ggT}(N, \beta - 1) = q.$$

Beweis:

(1) Die Existenz und Eindeutigkeit der Zahlen α und β folgt sofort aus dem chinesischen Restsatz. Aus $1 \le \alpha \le N-1$ folgt

$$1 \le N - \alpha \le N - 1 \quad \text{und} \quad N - \alpha \equiv \begin{cases} -1 \bmod p, \\ 1 \bmod q, \end{cases}$$

sodass die Eindeutigkeit von β sofort $\beta = N - \alpha$ liefert.

(2) $\Longleftarrow$: Natürlich gilt $1, N-1 \in Q_N$. Nun ist $\alpha^2 \equiv 1 \bmod p$ und $\alpha^2 \equiv 1 \bmod q$, und somit $\alpha^2 \equiv 1 \bmod N$, was $\alpha \in Q_N$ zeigt. Genauso folgt $\beta \in Q_N$.
$\Longrightarrow$: Sei $a \in Q_N$. Dann ist $a^2 \equiv 1 \bmod N$, also auch $a^2 \equiv 1 \bmod p$ und $a^2 \equiv 1 \bmod q$. Es folgt $a \equiv \pm 1 \bmod p$ und $a \equiv \pm 1 \bmod q$. Nach dem chinesischen Restsatz ist durch diese Kongruenzen $a \in \{0, 1, \ldots, N-1\}$ eindeutig bestimmt. Wir kennen aber bereits vier Lösungen: $1, N-1, \alpha, \beta$. Daher folgt $a \in \{1, N-1, \alpha, \beta\}$, und damit die Behauptung.

(3) Aus $\alpha \equiv 1 \bmod p$, $\alpha \equiv -1 \bmod q$ folgt $p \mid \alpha - 1$ und $q \nmid \alpha - 1$, woraus sofort

$$\mathrm{ggT}(N, \alpha - 1) = p$$

folgt, da $\mathrm{ggT}(N, *) \in \{1, p, q, N\}$ gilt. Genauso sieht man $\mathrm{ggT}(N, \beta - 1) = q$. ■

Der letzte Teil des Satzes besagt, dass man N sofort faktorisieren kann, falls man ein nichttriviales Element von Q_N kennt.

Wir definieren nun für eine RSA-Zahl

$$E_N = \{a \in \mathbb{Z} : 0 \le a \le N-1, \mathrm{ggT}(N, a) = 1\} \text{ und } Q_N = \{a \in \mathbb{Z} : 0 \le a \le N-1, a^2 \equiv 1 \bmod N\}.$$

Kennt man ein $m \in \mathbb{N}$ mit $a^m \equiv 1 \bmod N$ für alle $a \in E_N$, zerlegt man $m = 2^\ell u$ mit $u \equiv 1 \bmod 2$, so erhält man eine Abbildung

$$\omega_{N,m} : E_N \to Q_N$$

wie folgt:

$$\omega_{N,m}(a) = \begin{cases} 1, & \text{falls } a^u \equiv 1 \bmod N, \\ (a^{2^i u} \bmod N), & \text{falls } a^{2^i u} \not\equiv 1 \bmod N \text{ und } a^{2^{i+1} u} \equiv 1 \bmod N \text{ für ein } i \in \{0, \ldots, \ell - 1\}. \end{cases}$$

Kennt man N und m, so lässt sich die Funktion $\omega_{N,m}$ schnell berechnen:

Beispiele:

Algorithmus Berechnung von $\omega_{N,m}(a)$

Eingabe: RSA-Zahl N und „Exponent“ m und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(N,a)=1$
Ausgabe: $\omega_{N,m}(a)$

Zerlege $m = 2^\ell u$ mit $u \equiv 1 \bmod 2$.
$b \leftarrow a^u \bmod N$
$c \leftarrow b^2 \bmod N$
while $c \neq 1$ **do**
    $b, c \leftarrow c, c^2 \bmod N$
end while
Return b

Algorithmus Faktorisierung einer RSA-Zahl N bei Kenntnis eines „Exponenten“ m

Eingabe: RSA-Zahl N und „Exponent“ m
Ausgabe: Primteiler p und q von N

loop
    Wähle eine Zahl a mit $2 \le a \le N-2$
    $g \leftarrow \mathrm{ggT}(N,a)$
    if $g > 1$ **then**
        return g und $\frac{N}{g}$
    end if
    $b \leftarrow \omega_{N,m}(a)$
    if $b \neq 1$ und $b \neq N-1$ **then**
        $p \leftarrow \mathrm{ggT}(N, b-1)$, $q \leftarrow \frac{N}{p}$
        return p, q
    end if
end loop

(1)

$$
\begin{aligned}
N &= 658850937607612312657108729964086148561591553611592953539163\\
e &= 40466174908060971462730501706070178797340086412410089175463\\
d &= 600215686412710000793685165190665098070891768564314249573527\\
b = \omega_{N,ed-1}(2) &= 45266689311243494615575325986192871169632540116124386387489 3\\
p = \mathrm{ggT}(N, b-1) &= 760801809769495963836523488923\\
q = \frac{N}{p} &= 865995492054925275315978626881
\end{aligned}
$$

(2)

$$
\begin{aligned}
N &= 46546851894325084602092237706885949582368837402171533173 2623\\
e &= 93608747617068567585642475755500722832809300680245060528099\\
d &= 37262442651107110055637373279362507638362523401659573988 3211\\
b = \omega_{N,ed-1}(2) &= 43658929576064996111266688243446783064451496462474193128 6638\\
p = \mathrm{ggT}(N, b-1) &= 97635568401102920082761979 3559\\
q = \frac{N}{p} &= 476740727345417673418618858697
\end{aligned}
$$

(3)

$$\begin{aligned}
N &= 37388644834546359634094205853067376638990751540080450301049 1\\
e &= 53823987848248649184362565680045891916317023988095620290597\\
d &= 23220117209802032821211265332941881990837240901914933396341\\
b = \omega_{N,ed-1}(2) &= 23556540915941854585472091573989950139892742484417911029608 2\\
p = \mathrm{ggT}(N, b-1) &= 539142308141712937848124637407\\
q = \frac{N}{p} &= 69348378470640811193797204061 3
\end{aligned}$$

(4)

$$\begin{aligned}
N &= 17439385030978486029840444742737597209326018790923692283157 3\\
e &= 10459642789522067294426923000731927200344415102206826686331\\
d &= 88937872060992539022149504348421314191397212636547650476371\\
b = \omega_{N,ed-1}(2) &= 17439385030978486029840444742737597209326018790923692283157 2\\
b = \omega_{N,ed-1}(3) &= 16245130393424450200099858566308528911303793634788321207180 3\\
p = \mathrm{ggT}(N, b-1) &= 343123274892454611365733445069\\
q = \frac{N}{p} &= 50825421377913013112935749661 7
\end{aligned}$$

(5)

$$\begin{aligned}
N &= 71375034993669948719210549518309745603976059727313805987037 7\\
e &= 57577882717649755841973632675391201384626507250621727527867\\
d &= 41280532130309536426687165686150681367814280251156106557545 1\\
b = \omega_{N,ed-1}(2) &= 1\\
b = \omega_{N,ed-1}(3) &= 1\\
b = \omega_{N,ed-1}(4) &= 1\\
b = \omega_{N,ed-1}(5) &= 68555492068572342483530503862566487139339268906606707593791 0\\
p = \mathrm{ggT}(N, b-1) &= 80116217607188750460758722559 9\\
q = \frac{N}{p} &= 89089371821848883804370135842 3
\end{aligned}$$

(6)

$$\begin{aligned}
N &= 71712230867899052149100889184713449360254934951694151507197 7\\
e &= 36735148844054725254772716027254853158351833396211305306189\\
d &= 16125014850717153172575319083180840684731481236524611378723 7\\
b = \omega_{N,ed-1}(2) &= 71712230867899052149100889184713449360254934951694151507197 6\\
b = \omega_{N,ed-1}(3) &= 71712230867899052149100889184713449360254934951694151507197 6\\
b = \omega_{N,ed-1}(4) &= 71712230867899052149100889184713449360254934951694151507197 6\\
b = \omega_{N,ed-1}(5) &= 38077173596841147805762995943284068766223568512147545786040 7\\
p = \mathrm{ggT}(N, b-1) &= 72080504644772562873854293202 9\\
q = \frac{N}{p} &= 99489079913232518203444593641 3
\end{aligned}$$

(7)

$$\begin{aligned} N &= 189580281920426592313884873849725782683400953490504693950157 \\ e &= 958527555852979973625040812427282862883531801585015872376 29 \\ d &= 845329199991863435274862061245632721514583766210801619006 9 \\ b = \omega_{N,ed-1}(2) &= 140339446022480228540873499274570633707481267270584197033651 \\ p = \mathrm{ggT}(N, b-1) &= 641335467395011597881871375417 \\ q = \frac{N}{p} &= 295602366559372318577236199221 \end{aligned}$$

(8)

$$\begin{aligned} N &= 316859844888580235451867414074397000717227161459285848386261 \\ e &= 107139059593840482731404673254939951436162457994739161314 53 \\ d &= 573967109765097015664954279624165741531925776039328069128 37 \\ b = \omega_{N,ed-1}(2) &= 174558624547716908378347975215270468461185106255868404723840 \\ p = \mathrm{ggT}(N, b-1) &= 998159603487929411852111829487 \\ q = \frac{N}{p} &= 317444067843817496321669569403 \end{aligned}$$

(9)

$$\begin{aligned} N &= 128209040405267970958313647589379209822409712093217015930407 \\ e &= 297384790343349561505632550434081197865489962510518575372 11 \\ d &= 910245611843521004162460207754445605170781727642256754172 67 \\ b = \omega_{N,ed-1}(2) &= 1 \\ b = \omega_{N,ed-1}(3) &= 377904538543971439875746338397411488929761047870265050357 97 \\ p = \mathrm{ggT}(N, b-1) &= 1297211126596637662089082951 19 \\ q = \frac{N}{p} &= 988343668787648567930280678953 \end{aligned}$$

(10)

$$\begin{aligned} N &= 740487387346319629923532976400393683412143964316240041451463 \\ e &= 476534789078022308996959151085590320935901685173509742028 33 \\ d &= 413657525528592871406786957206046367177978362374366831690289 \\ b = \omega_{N,ed-1}(2) &= 147185214636969670500853972690566099053589218931784580279490 \\ p = \mathrm{ggT}(N, b-1) &= 835340196204452124095645121119 \\ q = \frac{N}{p} &= 886450084302040491396653818777 \end{aligned}$$

(11)

$$\begin{aligned} N &= 259952166396552591383599626119555804704643234051976151244287 \\ e &= 455456560596032577979710011960049370944484943661344583906 81 \\ d &= 116403010265702586190601481492025699574225459950108042479529 \\ b = \omega_{N,ed-1}(2) &= 218757507724792282523646249789515931362188848533837560053 13 \\ p = \mathrm{ggT}(N, b-1) &= 624892154529282346895309162183 \\ q = \frac{N}{p} &= 415995247359712649814701070089 \end{aligned}$$

(12)

$$\begin{aligned} N &= 65826428594628984276926501279061584443063885616183913263891 9 \\ e &= 60374725490612135284983488483325147846287084514106078068851 \\ d &= 32763470575666358700726581558780009095426311851360422591153 1 \\ b = \omega_{N,ed-1}(2) &= 1 \\ b = \omega_{N,ed-1}(3) &= 27033644812682842340813816230545699293497633136857007708175 2 \\ p = \mathrm{ggT}(N, b-1) &= 71154253970312142459925441823 9 \\ q = \frac{N}{p} &= 92512288333588460704633708812 1 \end{aligned}$$

(13)

$$\begin{aligned} N &= 39353925647268408144794006225922662720885171594795131362290 9 \\ e &= 96877296410282126934427736746730119843905050084437401785003 \\ d &= 37534008427437390269523600516687031299391825631523983703545 9 \\ b = \omega_{N,ed-1}(2) &= 19659332481970834688738279573289612467422613280169335298749 6 \\ p = \mathrm{ggT}(N, b-1) &= 71857375770755549354978195467 3 \\ q = \frac{N}{p} &= 54766717021253416930337188193 3 \end{aligned}$$

(14)

$$\begin{aligned} N &= 30244686328890515777518858017315440960949251580630797150662 3 \\ e &= 74339830669821871983785525476591882673217131615102261198207 \\ d &= 20679159543298303614229627542594506918742732540090076639252 7 \\ b = \omega_{N,ed-1}(2) &= 20334850366351386942905542534448470685895886972108107788160 8 \\ p = \mathrm{ggT}(N, b-1) &= 77954894002789252388900364616 7 \\ q = \frac{N}{p} &= 38797674880820632895822771336 9 \end{aligned}$$

(15)

$$\begin{aligned} N &= 30360043278245134702631417267815977203330272746746545602227 3 \\ e &= 52992020208133229068701327164097876931044880613899618130885 \\ d &= 16675908192568914105266959561694107550691210120133036684558 1 \\ b = \omega_{N,ed-1}(2) &= 30360043278245134702631417267815977203330272746746545602227 2 \\ b = \omega_{N,ed-1}(3) &= 28802207883540878981289454244023361760584916534508588093644 1 \\ p = \mathrm{ggT}(N, b-1) &= 55471539581176730509418263551 7 \\ q = \frac{N}{p} &= 54730846678261782853702757486 9 \end{aligned}$$

Wie schnell findet man durch Berechnung von $\omega_{N,m}(a)$ eine nichttriviale Quadratwurzel von 1 modulo N? Der folgende Satz macht eine Aussage über die Verteilung:

Satz. *Sei $N = pq$ eine RSA-Zahl, E_N und Q_N wie oben, $m \in \mathbb{N}$ eine Zahl mit $a^m \equiv 1 \bmod N$ für alle $a \in E_N$ und $\omega_{N,m} : E_N \to Q_N$ wie oben. Sei*

$$Q_N = \{1, \alpha, \beta, N-1\}$$

mit $\alpha \equiv 1 \bmod p$ wie oben. Sei $p-1 = 2^{\ell_p} u_p$ und $q-1 = 2^{\ell_q} u_q$ mit $u_p \equiv u_q \equiv 1 \bmod 2$. Sei o.E. $\ell_p \le \ell_q$. Dann gilt:

$$\begin{aligned}
\#\omega_{N,m}(1) &= u_p u_q, \\
\#\omega_{N,m}(\alpha) &= u_p u_q \cdot \left(2^{\ell_p + \ell_q} - 1 - 2 \cdot \frac{4^{\ell_p} - 1}{3} \right), \\
\#\omega_{N,m}(\beta) &= u_p u_q \cdot \frac{4^{\ell_p} - 1}{3}, \\
\#\omega_{N,m}(N-1) &= u_p u_q \cdot \frac{4^{\ell_p} - 1}{3}.
\end{aligned}$$

Den Satz kann man mit etwas Gruppentheorie beweisen.

7. Angriffe auf RSA mit Kettenbrüchen

Bemerkungen:

(1) Beim RSA-Kryptosystem hat man einen öffentlichen Schlüssel (N, e) und dazu einen passenden privaten Schlüssel (N, d). Dabei ist $N = pq$ das Produkt zweier verschiedener ungerader Primzahlen, außerdem gilt

$$ed \equiv 1 \bmod \varphi(N) \quad (\text{und } \varphi(N) = \varphi(pq) = (p-1)(q-1)).$$

Ein Text wird (nach einem vereinbarten Schema) in eine Zahlenfolge a_i (mit $0 \le a_i < N$) umgewandelt, dann

$$b_i = a_i^e \bmod N$$

berechnet. Der Chiffretext ist die Zahlenfolge $b_1, b_2, b_3, \ldots$
Aus $b_1, b_2, b_3, \ldots$ berechnet man mit dem privaten Schlüssel (N, d)

$$a_i = b_i^d \bmod N,$$

dann wandelt man die Zahlenfolge $a_1, a_2, a_3, \ldots$ in den Ausgangstext um.

(2) Für die Sicherheit des RSA-Verschlüsselungssystems ist es wesentlich, dass man aus dem (allgemein zugänglichen) öffentlichen Schlüssel (N, e) den privaten Schlüssel (N, d) praktisch nicht herleiten kann. Dies führt zu einigen unmittelbaren Konsequenzen:
   (a) N sollte nicht faktorisiert werden können, da man wegen sonst mittels der Gleichung

$$ed \equiv 1 \bmod (p-1)(q-1)$$

   sofort (N, d) berechnen könnte.
   (b) d sollte nicht zu klein sein, sodass man durch Probieren von $d = 3, 5, 7, \ldots$ auf d schließen kann. (Man kann beispielsweise testen, ob $2^{ed} \equiv 2 \bmod N$ gilt. Wenn ja, kann man versuchen, ob man mit (N, d) entschlüsseln kann.)
   (c) Im Folgenden werden wir sehen, dass im Fall von $d \lessapprox N^{\frac{1}{4}}$ (und ein paar Voraussetzungen an p und q) die Zahl N mit Hilfe von Kettenbruchentwicklungen faktorisiert werden kann. Die Idee geht auf M. Wiener (1990) zurück.

Sei (N, e) ein öffentlicher RSA-Schlüssel, $N = pq$, dazu d mit $ed \equiv 1 \bmod (p-1)(q-1)$ und k mit $ed = 1 + k(p-1)(q-1)$. Wir können $1 < e, d < (p-1)(q-1)$ annehmen. Aus $ed - k(p-1)(q-1) = 1$ folgt durch Division

$$\frac{e}{(p-1)(q-1)} - \frac{k}{d} = \frac{1}{d(p-1)(q-1)}.$$

Gilt nun $d < \frac{1}{2}(p-1)(q-1)$, so folgt sofort

$$\left| \frac{e}{(p-1)(q-1)} - \frac{k}{d} \right| < \frac{1}{2d^2}.$$

Nach unseren Vorkenntnissen über Kettenbrüche tritt dann $\frac{k}{d}$ als Näherungsbruch in der Kettenbruchentwicklung von $\frac{e}{(p-1)(q-1)}$ auf. Die folgenden Beispiele illustrieren dieses Phänomen.

Beispiel: Wir wählen $N = 15333921635029117607$ mit $N = pq$ und $p = 2397845293$, $q = 6394875299$. Es ist $\varphi(N) = (p-1)(q-1) = 15333921626236397016$. Wir haben verschiedene d mit $\mathrm{ggT}(e,(p-1)(q-1)) = 1$ und $1 < d < (p-1)(q-1)$ gewählt, dazu e mit $ed \equiv 1 \bmod (p-1)(q-1)$ und k mit $ed = 1+k(p-1)(q-1)$ berechnet. Anschließend wurden die Kettenbruchentwicklungen von $\frac{e}{\varphi(N)}$ und $\frac{k}{d}$ bestimmt:

(1) $d = 15333921626236384673$, $e = 12394599049255491617$, $k = 12394599049255481640$,

$$\begin{aligned}\frac{e}{\varphi(N)} &= [0,1,4,4,1,1,1,1,2,1,2,2,3,1,1242317234565048],\\ \frac{k}{d} &= [0,1,4,4,1,1,1,1,2,1,2,2,3,1,1242317234565047].\end{aligned}$$

Hier ist $\frac{k}{d}$ kein Näherungsbruch von $\frac{e}{\varphi(N)}$.

(2) $d = 7666960813118192335$, $e = 8687897438484010783$, $k = 4343948719242001894$,

$$\begin{aligned}\frac{e}{\varphi(N)} &= [0,1,1,3,3,1,12,10,1,2,621007679662902,2],\\ \frac{k}{d} &= [0,1,1,3,3,1,12,10,1,2,621007679662902].\end{aligned}$$

(3) $d = 233977075595647$, $e = 12129298342629271663$, $k = 185078404886310$,

$$\begin{aligned}\frac{e}{\varphi(N)} &= [0,1,3,1,3,1,1,1,5,1,12,6,1,1,3110404599,65536],\\ \frac{k}{d} &= [0,1,3,1,3,1,1,1,5,1,12,6,1,1,3110404599].\end{aligned}$$

(4) $d = 116988537797825$, $e = 12110973441548388737$, $k = 92399394543064$,

$$\begin{aligned}\frac{e}{\varphi(N)} &= [0,1,3,1,3,7,1,5,43,1,2,963788783,1,131071],\\ \frac{k}{d} &= [0,1,3,1,3,7,1,5,43,1,2,963788784].\end{aligned}$$

(5) $d = 57123309473$, $e = 10293840884799985673$, $k = 38347545583$,

$$\begin{aligned}\frac{e}{\varphi(N)} &= [0,1,2,23,1,1,2,2,1,2,2,1,1,1,1,16,6,25,3,150,1,268435455],\\ \frac{k}{d} &= [0,1,2,23,1,1,2,2,1,2,2,1,1,1,1,16,6,25,3,151].\end{aligned}$$

(6) $d = 13619$, $e = 11116220590045667651$, $k = 9873$,

$$\begin{aligned}\frac{e}{\varphi(N)} &= [0,1,2,1,1,1,2,1,10,3,1,6,1,1125921258993787],\\ \frac{k}{d} &= [0,1,2,1,1,1,2,1,10,3,1,7].\end{aligned}$$

(7) $d = 425$, $e = 5917089756947692025$, $k = 164$,

$$\begin{aligned}\frac{e}{\varphi(N)} &= [0,2,1,1,2,4,3,1,1,36079815591144463],\\ \frac{k}{d} &= [0,2,1,1,2,4,3,2].\end{aligned}$$

(8) $d = 11$, $e = 5575971500449598915$, $k = 4$,

$$\begin{aligned}\frac{e}{\varphi(N)} &= [0,2,1,2,1,1393992875112399728],\\ \frac{k}{d} &= [0,2,1,3].\end{aligned}$$

(9) $d = 5$, $e = 12267137300989117613$, $k = 4$,

$$\begin{aligned}\frac{e}{\varphi(N)} &= [0,1,4,3066784325247279403],\\ \frac{k}{d} &= [0,1,4].\end{aligned}$$

In den Fällen (2) bis (9) ist $\frac{k}{d}$ Näherungsbruch in der Kettenbruchentwicklung von $\frac{e}{(p-1)(q-1)}$.

Schreiben wir $s = p + q$, so gilt

$$\varphi(N) = (p-1)(q-1) = N - (p+q) + 1 = N + 1 - s$$

und damit

$$\frac{e}{\varphi(N)} = \frac{e}{N+1-s}.$$

Kennen wir nur den öffentlichen Schlüssel (N, e), so kennen wir nicht $s = p+q$, also können wir auch nicht $\frac{k}{d}$ als Näherungsbruch von $\frac{e}{N+1-s}$ suchen. Aber wir können beispielsweise fragen, ob $\frac{k}{d}$ als Näherungsbruch von $\frac{e}{N}$ vorkommt.

Wir haben zuvor gezeigt: Ist $N = pq$ eine RSA-Zahl mit $p < q < 2p$, so gilt

$$2\sqrt{N} < p + q < \frac{3}{\sqrt{2}}\sqrt{N}.$$

Diese Abschätzungen benötigen wir im Folgenden.

Satz. *Sei (N, e) öffentlicher RSA-Schlüssel, $N = pq$ mit verschiedenen ungeraden Primzahlen p und q, $1 < e < (p-1)(q-1)$, $d \in \mathbb{N}$ mit $ed \equiv 1 \bmod (p-1)(q-1)$ und $1 < d < (p-1)(q-1)$, sei $k \in \mathbb{N}$ mit $ed = 1 + k(p-1)(q-1)$. Außerdem gelte $p < q < 2p$. Dann gelten die Implikationen*

$$kd \le 0.2357\sqrt{N} \quad \Longrightarrow \quad kd \le \sqrt{\frac{N}{18}} \quad \Longrightarrow \quad |\frac{e}{N} - \frac{k}{d}| < \frac{1}{2d^2}$$

und

$$d \le 0.4854 \cdot N^{0.25} \quad \Longrightarrow \quad d \le (\frac{N}{18})^{0.25} \quad \Longrightarrow \quad |\frac{e}{N} - \frac{k}{d}| < \frac{1}{2d^2},$$

also ist $\frac{k}{d}$ (in beiden Fällen) Näherungsbruch in der Kettenbruchentwicklung von $\frac{e}{N}$.

Beweis: Es gilt mit $s = p + q$

$$|\frac{e}{N} - \frac{k}{d}| = |\frac{ed - kN}{dN}| = |\frac{1 + k(N+1-s) - kN}{dN}| = |\frac{1 + k - ks}{dN}| = \frac{ks - k - 1}{dN}.$$

Aus $p < q < 2p$ folgt $s < \frac{3}{\sqrt{2}}\sqrt{N}$ und damit

$$\begin{aligned} |\frac{e}{N} - \frac{k}{d}| &= \frac{ks - k - 1}{dN} < \frac{ks}{dN} < \frac{k \cdot \frac{3}{\sqrt{2}}\sqrt{N}}{dN} = \frac{3\sqrt{2}k}{2d\sqrt{N}} = \frac{1}{2d^2} \cdot \frac{\sqrt{18}kd}{\sqrt{N}} = \\ &= \frac{1}{2d^2} \cdot \frac{kd}{\sqrt{\frac{N}{18}}}. \end{aligned}$$

Daraus folgt die erste Abschätzung (mit der numerischen Auswertung $\sqrt{\frac{1}{18}} = 0.235702\ldots$). Der erste Teil der zweiten Implikation folgt aus $(\frac{1}{18})^{0.25} = 0.485491\ldots$. Gilt $d \le (\frac{N}{18})^{0.25}$, so folgt aus $k < d$

$$kd < d^2 \le \sqrt{\frac{N}{18}},$$

und mit der ersten Implikation folgt auch diese Aussage. ■

Bemerkung: Die Aussage, dass aus einer Abschätzung wie $d \le 0.4854 \cdot N^{0.25}$ folgt, dass $\frac{k}{d}$ Näherungsbruch von $\frac{e}{N}$ ist, wird oft als Satz von Wiener bezeichnet.

Beispiele:

(1) $e = 3593613806987181353$

$$\begin{aligned} d &= 79129 \approx 1.5000 \cdot N^{0.25} \\ k &= 36718 \\ kd &= 2905458622 \approx 1.0440 \cdot N^{0.5} \\ \frac{e}{N} &= [0, 2, 6, 2, 4, 2, 7, 4, 7, 3, 1, 10, 1, 98, 3, 9, 3, 4, 10, 1, 1, 1, 5, 2, 26, 3, 3, 8, 1, 1, 3, 10] \\ \frac{k}{d} &= [0, 2, 6, 2, 4, 2, 7, 4, 9] \end{aligned}$$

(2) $e = 688891786930255313$

$$\begin{aligned} d &= 71217 \approx 1.3500 \cdot N^{0.25} \\ k &= 6335 \\ kd &= 451159695 \approx 0.1621 \cdot N^{0.5} \\ \frac{e}{N} &= [0, 11, 4, 7, 2, 2, 40, 1, 2, 53, 1, 13, 10, 7, 2, 2, 1, 1, 1, 1, 10, 1, 8, 2, 9, 2, 6, 1, 56, 3, 1, 2] \\ \frac{k}{d} &= [0, 11, 4, 7, 2, 2, 41] \end{aligned}$$

(3) $e = 369084120139393017$

$$\begin{aligned} d &= 63305 \approx 1.2000 \cdot N^{0.25} \\ k &= 3017 \\ kd &= 190991185 \approx 0.0686 \cdot N^{0.5} \\ \frac{e}{N} &= [0, 20, 1, 57, 51, 1, 6, 10, 1, 4, 28, 2, 1, 2, 1, 1, 7, 2, 29, 2, 1, 11, 1, 13, 11, 1, 1, 49, 2] \\ \frac{k}{d} &= [0, 20, 1, 57, 52] \end{aligned}$$

(4) $e = 5824276941050460833$

$$\begin{aligned} d &= 55393 \approx 1.0500 \cdot N^{0.25} \\ k &= 41659 \\ kd &= 2307616987 \approx 0.8292 \cdot N^{0.5} \\ \frac{e}{N} &= [0, 1, 3, 30, 19, 25, 1, 5, 4, 1, 59, 1, 1, 2, 4, 1, 23, 9, 6, 3, 1, 1, 3, 1, 45, 1, 1, 1, 1, 1, 11, 2, 6] \\ \frac{k}{d} &= [0, 1, 3, 30, 19, 24] \end{aligned}$$

(5) $e = 347251289678534089$

$$\begin{aligned} d &= 47481 \approx 0.9001 \cdot N^{0.25} \\ k &= 2129 \\ kd &= 101087049 \approx 0.0363 \cdot N^{0.5} \\ \frac{e}{N} &= [0, 22, 3, 3, 4, 1, 1, 1, 6, 2, 12, 1, 8, 1, 11, 1, 2, 6228, 1, 5, 3, 1, 3, 1, 6, 2, 5, 1, 1, 6, 4, 9] \\ \frac{k}{d} &= [0, 22, 3, 3, 4, 1, 1, 1, 6, 2] \end{aligned}$$

(6) $e = 1268454839300612977$

$$\begin{aligned} d &= 39569 \approx 0.7501 \cdot N^{0.25} \\ k &= 6481 \\ kd &= 256446689 \approx 0.0922 \cdot N^{0.5} \\ \frac{e}{N} &= [0, 6, 9, 2, 22, 3, 1, 3, 5, 675, 1, 1, 1, 1, 1, 1, 1, 3, 1, 13, 2, 30, 1, 13, 2, 4, 1, 1, 1, 2, 3, 1, 1, 2, 3, 1, 3] \\ \frac{k}{d} &= [0, 6, 9, 2, 22, 3, 1, 3] \end{aligned}$$

(7) $e = 1056577871634580377$

$$\begin{aligned} d &= 31657 \approx 0.6001 \cdot N^{0.25} \\ k &= 4319 \\ kd &= 136726583 \approx 0.0491 \cdot N^{0.5} \\ \frac{e}{N} &= [0, 7, 3, 30, 3, 2, 1, 4, 9, 1, 2, 91, 2, 2, 5, 2, 1, 1, 1, 1, 1, 67, 1, 2, 1, 2, 2, 1, 8, 2, 1, 3, 5, 8, 2, 1, 1, 2] \\ \frac{k}{d} &= [0, 7, 3, 30, 3, 2, 1, 4] \end{aligned}$$

(8) $e = 5479953451499670849$

$$\begin{aligned} d &= 23745 \approx 0.4501 \cdot N^{0.25} \\ k &= 16802 \\ kd &= 398963490 \approx 0.1434 \cdot N^{0.5} \\ \frac{e}{N} &= [0, 1, 2, 2, 2, 1, 1, 1, 1, 1, 45, 1, 1, 1, 2, 1, 2, 1, 1, 2, 8, 1, 1, 1, 2, 3, 4, 1, 99, 1, 6, 1, 4, 1, 3, 3, 19, 3, 2, 2, 4, 2, 21] \\ \frac{k}{d} &= [0, 1, 2, 2, 2, 1, 1, 1, 1, 1, 45, 1, 2] \end{aligned}$$

(9) $e = 52336976383084905$

$$\begin{aligned} d &= 15833 \approx 0.3001 \cdot N^{0.25} \\ k &= 107 \\ kd &= 1694131 \approx 0.0006 \cdot N^{0.5} \\ \frac{e}{N} &= [0, 147, 1, 34, 1, 2, 797, 10, 1, 5, 4, 15, 1, 2, 2, 7, 1, 1, 6, 1, 22, 2, 1, 1, 4, 1, 12, 1, 8, 2] \\ \frac{k}{d} &= [0, 147, 1, 34, 1, 2] \end{aligned}$$

(10) $e = 1336523392153255185$

$$\begin{aligned} d &= 7921 \approx 0.1502 \cdot N^{0.25} \\ k &= 1367 \\ kd &= 10828007 \approx 0.0039 \cdot N^{0.5} \\ \frac{e}{N} &= [0, 5, 1, 3, 1, 6, 2, 1, 1, 7, 124, 1, 1, 1, 2, 1, 1, 2, 12, 1, 18, 13, 1, 4, 1, 1, 4, 1, 1, 2, 2, 5, 2, 3, 4, 47, 1, 1, 1, 2] \\ \frac{k}{d} &= [0, 5, 1, 3, 1, 6, 2, 1, 1, 7] \end{aligned}$$

In den Fällen (1) und (4) ist $\frac{k}{d}$ kein Näherungsbruch in der Kettenbruchentwicklung von $\frac{e}{N}$, sonst schon.

Wir zeigen jetzt, wie man von der Kenntnis von $\frac{k}{d}$ zu einer Faktorisierung von N kommt.

LEMMA. *Sei $N = pq$ mit ungeraden Primzahlen $p < q$, seien e, d natürliche Zahlen mit $1 < e, d < (p-1)(q-1)$ und $ed \equiv 1 \bmod (p-1)(q-1)$.*

(1) *Setzt man nacheinander*

$$k = \frac{ed-1}{(p-1)(q-1)}, \quad s = N + 1 - \frac{ed-1}{k}, \quad D = s^2 - 4N,$$

so sind k, s und D natürliche Zahlen und es gilt

$$ed \equiv 1 \bmod k, \quad D \text{ ist ein Quadrat} \quad \text{und} \quad p = \frac{s - \sqrt{D}}{2}, \quad q = \frac{s + \sqrt{D}}{2}.$$

(2) *Sind umgekehrt k', d' natürliche Zahlen, sodass gilt $ed' \equiv 1 \bmod k'$, so sind*

$$s' = N + 1 - \frac{ed'-1}{k'}, \quad \text{und} \quad D' = s'^2 - 4N$$

ganze Zahlen. Setzt man außerdem voraus, dass $s' > 0$ gilt und dass D' ein Quadrat (in $\mathbb{Z}$) ist, so ist

$$p = \frac{s' - \sqrt{D'}}{2} \quad \textit{und} \quad q = \frac{s' + \sqrt{D'}}{2}.$$

Beweis:

(1) Die Voraussetzung $ed \equiv 1 \bmod (p-1)(q-1)$ bedeutet, dass $k = \frac{ed-1}{(p-1)(q-1)}$ eine ganze Zahl ist. Wegen $e, d > 1$ ist $k > 0$. Dann ist

$$s = N + 1 - \frac{ed-1}{k} = N + 1 - (p-1)(q-1) = pq + 1 - (p-1)(q-1) = p + q,$$

und damit

$$D = s^2 - 4N = (p+q)^2 - 4pq = (q-p)^2$$

ein Quadrat und

$$\frac{s - \sqrt{D}}{2} = \frac{(p+q) - (q-p)}{2} = p \quad \text{und} \quad \frac{s + \sqrt{D}}{2} = \frac{(p+q) + (q-p)}{2} = q,$$

was die erste Behauptung beweist.

(2) Wegen $ed' \equiv 1 \bmod k'$ sind s' und D' ganze Zahlen und damit wegen $D' \equiv s' \bmod 2$ auch

$$p' = \frac{s' - \sqrt{D'}}{2} \quad \text{und} \quad q' = \frac{s' + \sqrt{D'}}{2}.$$

Wegen $D' = s'^2 - 4N$ ist $D' < s'^2$, also $\sqrt{D'} < s'$, weil $s' > 0$ vorausgesetzt war. Daher gilt $1 \le p' \le q'$. Aus

$$p'q' = \frac{s' - \sqrt{D'}}{2} \cdot \frac{s' + \sqrt{D'}}{2} = \frac{s'^2 - D'}{4} = N$$

sieht man, dass es nur die beiden Möglichkeiten

$$p' = 1, q' = N \quad \text{oder} \quad p' = p, q' = q$$

gibt. Wäre $p' = 1, q' = N$, so wäre $s' = p' + q' = N + 1$ und damit $ed' = 1$ wegen $s' = N + 1 - \frac{ed'-1}{k}$, was der Voraussetzung $e > 1$ widerspricht. Also bleibt nur die zweite Möglichkeit, womit die Behauptung bewiesen ist. ■

Algorithmus Kettenbruchangriff auf RSA

Eingabe: (N, e) öffentlicher RSA-Schlüssel (mit $1 < e < N$)
Ausgabe: Nichts oder die Primteiler p, q von N und den privaten Exponenten d

Bestimme die Näherungsbrüche $\frac{k_0}{d_0}, \frac{k_1}{d_1}, \ldots, \frac{k_n}{d_n}$ der Kettenbruchentwicklung von $\frac{e}{N}$
for $i = 1, \ldots, n$ **do** ▷ Beginn mit $i = 1$ wegen $k_0 = 0$, $d_0 = 1$
  if $ed_i \equiv 1 \bmod k_i$ **then**
    $s \leftarrow N + 1 - \frac{ed_i - 1}{k_i}$, $D \leftarrow s^2 - 4N$
    if $s > 0$ and $D \ge 0$ **then**
      $w \leftarrow \left\lfloor \sqrt{D} \right\rfloor$
      if $w^2 = D$ **then**
        $p \leftarrow \frac{s-w}{2}$, $q \leftarrow \frac{s+w}{2}$
        return p, q, d_i
      end if
    end if
  end if
end for

Beispiel: s_i und D_i sind nur angegeben, wenn $ed_i \equiv 1 \bmod k_i$ gilt. p_i und q_i werden genau dann angegeben, wenn D_i eine Quadratzahl ist. $N = 3070389953$, $e = 1160418943$. Dann ist

$$\frac{e}{N} = [0, 2, 1, 1, 1, 4, 1, 2, 4, 31, 2, 3, 1, 6, 1, 1, 1, 14, 1, 1, 1, 5, 1, 2].$$

i	k_i	d_i	s_i	D_i	p_i	q_i
1	1	2				
2	1	3				
3	2	5	169342597	28676902877144597		
4	3	8				
5	14	37				
6	17	45	-1307248	1696615773692		
7	48	127	114834	905287744	42373	72461
8	209	553				
9	6527	17270				
10	13263	35093				
11	46316	122549				
12	59579	157642				
13	403790	1068401				
14	463369	1226043				
15	867159	2294444				
16	1330528	3520487				
17	19494551	51581262				
18	20825079	55101749				
19	40319630	106683011				
20	61144709	161784760				
21	346043175	915606811				
22	407187884	1077391571	1	-12281559811		
23	1160418943	3070389953				

Bemerkungen:

(1) Der dargestellte Kettenbruchangriff auf RSA ist sicher erfolgreich, wenn (im Fall $p < q < 2p$) für den privaten Exponenten die Abschätzung $d \leq 0.4854N^{0.25}$ gilt.
(2) Der Kettenbruchangriff funktioniert (im Fall $p < q < 2p$) auch, wenn $kd \leq 0.2357\sqrt{N}$ ist. Ist also k klein, so kann d in der Größenordnung von $\sqrt{N}$ sein. Die folgenden Beispiele illustrieren diesen Sachverhalt.

Beispiel: Wir betrachten $N = 8702995822830039013 = pq$ mit $p = 2384654143$ und $q = 3649584091$. Weiter wählen wir $e = 11794298623$. Damit berechnen wir d und k zu

$$d = 737898547 \approx 0.25\sqrt{N} \quad \text{und} \quad k = 1.$$

Für die Kettenbruchentwicklungen finden wir

$$\begin{aligned} \frac{k}{d} &= [0, 737898547], \\ \frac{e}{N} &= [0, 737898547, 1, 1, 21, 117, 1, 8, 248, 1, 1, 1, 1, 10, 1, 17]. \end{aligned}$$

Also ist $\frac{k}{d}$ Näherungsbruch von $\frac{e}{N}$, der Kettenbruchangriff funktioniert.

Beispiel:

$$
\begin{aligned}
N &= 413053273800953303783069058320630345085099293294199582370432504690849224502636 19,\\
p &= 584514203302800799212975968606678797801 3,\\
q &= 706660798774424047898958355605020575766 3,\\
e &= 129356067306964459878364469952233112675 05,\\
d &= 319314959398672706517982323145854674408 9,\\
k &= 1,\\
\frac{k}{d} &= [0, 319314959398672706517982323145854674408 9],\\
\frac{e}{N} &= [0, 319314959398672706517982323145854674408 9, 1, 541, 4, 1, 1, 8, 1, 3, 1, 1, 1, 1, 6, 1, 5, 2, 3, 1, 7, 2,\\
&\quad 1, 4, 56, 1, 1, 4, 1, 1, 1, 33, 46, 8, 1, 1, 3, 7, 1, 1, 8, 1, 1, 1, 2, 1, 3, 12, 3, 7, 2, 8, 1, 1, 5, 1, 1, 21, 4, 1, 1, 3, 1,\\
&\quad 3, 1, 1, 1, 1, 5, 1, 2, 1, 1, 6, 1, 2, 3, 5, 8, 1, 1, 1, 4, 3, 1, 11],\\
&\quad \frac{d}{\sqrt{N}} = 0.4968, \quad \frac{q}{p} = 1.21.
\end{aligned}
$$

Hier ist $\frac{k}{d}$ Näherungsbruch in der Kettenbruchentwicklung von $\frac{e}{N}$ und $d \approx 0.5N^{0.5}$. Auch hier funktioniert der Kettenbruchangriff.

Beispiel:

$$
\begin{aligned}
N &= 87457631035059056586824477565086269119644439363792185584227133465350538824102469,\\
p &= 89633296164601257726260659466717906348 59,\\
q &= 97572704315652029671803905500606507317 91,\\
e &= 16165252083317784532017867671353906319699,\\
d &= 54102237678875156678021844782954244004 79,\\
k &= 1,\\
\frac{k}{d} &= [0, 54102237678875156678021844782954244004 79],\\
\frac{e}{N} &= [0, 54102237678875156678021844782954244004 80, 6, 3, 14, 1, 10, 1, 52, 6, 13, 1, 14, 5, 1, 3, 5, 2, 1, 45,\\
&\quad 6, 2, 2, 1, 1, 3, 1, 2, 3, 4, 4, 8, 1, 1, 163, 1, 3, 3, 1, 1, 1, 2, 3, 7, 2, 18, 5, 1, 3, 2, 4, 10, 5, 2, 9, 3, 10, 6, 2, 2, 1,\\
&\quad 2, 1, 1, 1, 1, 1, 16, 1, 6, 3, 1, 1, 1, 1, 3, 2],\\
&\quad \frac{d}{\sqrt{N}} = 0.5785, \quad \frac{q}{p} = 1.09.
\end{aligned}
$$

Hier ist $\frac{k}{d}$ kein Näherungsbruch in der Kettenbruchentwicklung von $\frac{e}{N}$ und $d \approx 0.58N^{0.25}$. Der Kettenbruchangriff funktioniert nicht.

SATZ. *Sei (N, e) öffentlicher RSA-Schlüssel, $N = pq$ mit verschiedenen ungeraden Primzahlen p und q, $1 < e < (p-1)(q-1)$, $d \in \mathbb{N}$ mit $ed \equiv 1 \bmod (p-1)(q-1)$ und $1 < d < (p-1)(q-1)$, sei $k \in \mathbb{N}$ mit $ed = 1 + k(p-1)(q-1)$. Dann gelten die Implikationen*

$$kd \geq 0.68\sqrt{N} \quad \Longrightarrow \quad |\frac{e}{N} - \frac{k}{d}| > \frac{1}{d^2}$$

und

$$d \geq 0.68 \cdot N^{0.5} \quad \Longrightarrow \quad |\frac{e}{N} - \frac{k}{d}| > \frac{1}{d^2},$$

also ist $\frac{k}{d}$ (in beiden Fällen) kein Näherungsbruch in der Kettenbruchentwicklung von $\frac{e}{N}$.

Beweis: Mit $s = p + q$ und $s > 2\sqrt{N}$ folgt

$$\begin{aligned}\left|\frac{e}{N} - \frac{k}{d}\right| &= \left|\frac{ed - kN}{dN}\right| = \left|\frac{1 + k(N + 1 - s) - kN}{dN}\right| = \left|\frac{1 - k(s-1)}{dN}\right| = \left|\frac{k(s-1) - 1}{dN}\right| = \\ &= \frac{k(s-1) - 1}{dN} \geq \frac{k(s-1) - k}{dN} = \frac{k(s-2)}{dN} > \frac{k(2\sqrt{N} - 2)}{dN} = \\ &= 2(1 - \frac{1}{\sqrt{N}}) \cdot \frac{kd}{\sqrt{N}} \cdot \frac{1}{d^2} \overset{N \geq 15}{\geq} \frac{kd}{0.68\sqrt{N}} \cdot \frac{1}{d^2}.\end{aligned}$$

Ist also $kd \geq 0.68\sqrt{N}$, so folgt

$$|\frac{e}{N} - \frac{k}{d}| > \frac{1}{d^2},$$

weswegen $\frac{k}{d}$ nicht als Näherungsbruch in der Kettenbruchentwicklung von $\frac{e}{N}$ auftritt. Die zweite Aussage folgt natürlich sofort aus der ersten Implikation, da $k \geq 1$ gilt. ■

Bemerkung: Aus den vorangegangenen Sätzen folgt (im Fall $p < q < 2p$), dass der Kettenbruchangriff im Fall $d \leq 0.4854 \cdot N^{0.25}$ Erfolg hat, dass er aber im Fall $d \geq 0.68 \cdot N^{0.5}$ sicher nicht mehr erfolgreich ist.

Zurück zur allgemeinen Situation. Wir haben gesehen, dass $2\sqrt{N} < p+q$ gilt. Dies impliziert $\left\lfloor \sqrt{4N} \right\rfloor + 1 \leq p + q$ und damit

$$(p-1)(q-1) = N + 1 - (p+q) \leq N + 1 - (\left\lfloor \sqrt{4N} \right\rfloor + 1) = N - \left\lfloor \sqrt{4N} \right\rfloor.$$

Also gilt

$$\frac{e}{N} < \frac{e}{N - \left\lfloor \sqrt{4N} \right\rfloor} < \frac{e}{(p-1)(q-1)}.$$

Was passiert, wenn wir die Kettenbruchentwicklung von $\frac{e}{N - \lfloor \sqrt{4N} \rfloor}$ statt die Kettenbruchentwicklung von $\frac{e}{N}$ verwenden?

Beispiel: Wir nehmen die 20-stellige Zahl

$$N = 32758596115823463 61 = 4072951217 \cdot 8042978633$$

und

$$d = 118575 \approx N^{0.260}, \quad e = 30770071517687295567 \approx N^{0.999}, \quad k = 111377$$

$$\begin{aligned}\frac{k}{d} &= [0, 1, 15, 2, 8, 1, 6, 1, 5, 8] \\ \frac{e}{\varphi(N)} &= [0, 1, 15, 2, 8, 1, 6, 1, 5, 7, 1, 276269530672286] \\ \frac{e}{N} &= [0, 1, 15, 2, 8, 1, 6, 1, 5, 20, \\ &\quad 6, 1, 6, 1, 1, 1, 15, 5, 2, 1, 1, 1, 1, 4, 22, 3, 2, 1, 1, 22, 2, 6, 1, 3, 1, 2, 2, 3, 1, 1, 1, 2] \\ \frac{e}{N - \left\lfloor \sqrt{4N} \right\rfloor} &= [0, 1, 15, 2, 8, 1, 6, 1, 5, 8, \\ &\quad 3, 1, 1, 2, 2, 2, 4, 3, 1, 7, 6, 1, 4, 1, 1, 3, 1, 1, 1, 2, 4, 1, 1, 1, 2, 2, 1, 1, 4, 1, 1, 1, 2, 1, 8, 2, 28]\end{aligned}$$

Wir sehen, dass $\frac{k}{d}$ Näherungsbruch in der Kettenbruchentwicklung von $\frac{e}{N - \lfloor \sqrt{4N} \rfloor}$, nicht jedoch Näherungsbruch in der Kettenbruchentwicklung von $\frac{e}{N}$ ist.

Satz. *Sei $N = pq > 3000$ mit $p < q < 3.9p$, seien e, d natürliche Zahlen mit $1 < e, d < \varphi(N)$ und $ed \equiv 1 \bmod \varphi(N)$, sowie $k = \frac{ed-1}{\varphi(N)}$. Dann gilt die Implikation*

$$d \leq N^{\frac{1}{4}} \quad \Longrightarrow \quad |\frac{e}{N - \left\lfloor \sqrt{4N} \right\rfloor} - \frac{k}{d}| < \frac{1}{2d^2},$$

ist also $d \leq N^{0.25}$, so kommt $\frac{k}{d}$ als Näherungsbruch in der Kettenbruchentwicklung von $\frac{e}{N - \lfloor \sqrt{4N} \rfloor}$ vor.

Beweis:

(1) Aus $p < q < 3.9p$ folgt mit einem vorangegangenen Lemma mit $s = p + q$

$$2\sqrt{N} < s < (\sqrt{3.9} + \frac{1}{\sqrt{3.9}})\sqrt{N} < 2.48121145\sqrt{N}.$$

Da $2\sqrt{N}$ keine ganze Zahl ist, gilt $\left\lfloor \sqrt{4N} \right\rfloor + 1 \leq s$.

(2) Im Fall $s = \left\lfloor \sqrt{4N} \right\rfloor + 1$ ist $\varphi(N) = N + 1 - s = N - \left\lfloor \sqrt{4N} \right\rfloor$ und damit

$$|\frac{e}{N - \left\lfloor \sqrt{4N} \right\rfloor} - \frac{k}{d}| \quad = \quad |\frac{e}{\varphi(N)} - \frac{k}{d}| = |\frac{e}{\varphi(N)} - \frac{e - \frac{1}{d}}{\varphi(N)}| = \frac{1}{d\varphi(N)}$$

Für $N \geq 10$ ist $2N^{\frac{1}{4}} + 2\sqrt{N} < N$, also

$$2d \leq 2N^{\frac{1}{4}} < N - 2\sqrt{N} \leq N - \left\lfloor \sqrt{4N} \right\rfloor = \varphi(N)$$

und damit

$$|\frac{e}{N - \left\lfloor \sqrt{4N} \right\rfloor} - \frac{k}{d}| = \frac{1}{d\varphi(N)} < \frac{1}{2d^2},$$

was gezeigt werden sollte.

(3) Im Fall $s > \left\lfloor \sqrt{4N} \right\rfloor + 1$ gilt

$$\begin{aligned} k(N - \left\lfloor \sqrt{4N} \right\rfloor) - ed &= k(N - \left\lfloor \sqrt{4N} \right\rfloor) - (1 + k\varphi(N)) \geq \\ &\geq k(N - \left\lfloor \sqrt{4N} \right\rfloor) - k - k\varphi(N) = \\ &= k(N - \left\lfloor \sqrt{4N} \right\rfloor - 1 - (N + 1 - s)) = k(s - \left\lfloor \sqrt{4N} \right\rfloor - 2) \geq 0 \end{aligned}$$

und damit

$$\frac{k}{d} \geq \frac{e}{N - \left\lfloor \sqrt{4N} \right\rfloor}.$$

Dann ist

$$\begin{aligned} |\frac{e}{N - \left\lfloor \sqrt{4N} \right\rfloor} - \frac{k}{d}| &= \frac{k}{d} - \frac{e}{N - \left\lfloor \sqrt{4N} \right\rfloor} < \frac{k}{d} - \frac{e}{N + 1 - 2\sqrt{N}} = \\ &= \frac{e - \frac{1}{d}}{\varphi(N)} - \frac{e}{N + 1 - 2\sqrt{N}} < \frac{e}{\varphi(N)} - \frac{e}{N + 1 - 2\sqrt{N}} = \\ &= \frac{e((N + 1 - 2\sqrt{N}) - (N + 1 - s))}{\varphi(N)(N + 1 - 2\sqrt{N})} < \frac{s - 2\sqrt{N}}{N + 1 - 2\sqrt{N}} < \\ &< \frac{(2.48121145 - 2)\sqrt{N}}{N + 1 - 2\sqrt{N}} = \frac{0.48121145\sqrt{N}}{N + 1 - 2\sqrt{N}} \end{aligned}$$

Nun gilt

$$\begin{aligned} \frac{0.48121145\sqrt{N}}{N + 1 - 2\sqrt{N}} \leq \frac{1}{2\sqrt{N}} \quad &\iff \quad 0.9624229N \leq N + 1 - 2\sqrt{N} \\ &\iff \quad 2\sqrt{N} - 1 \leq 0.0375771N \quad \iff \quad N \geq 2780 \end{aligned}$$

Damit folgt für $N \geq 3000$ und $d \leq N^{\frac{1}{4}}$ zunächst $d^2 \leq \sqrt{N}$ und damit

$$|\frac{e}{N - \left\lfloor \sqrt{4N} \right\rfloor} - \frac{k}{d}| < \frac{1}{2d^2},$$

was gezeigt werden sollte. ■

Den zuvor angegebenen Algorithmus kann man nun natürlich auch mit $\frac{e}{N-\lfloor\sqrt{4N}\rfloor}$ statt mit $\frac{e}{N}$ durchführen.

Beispiele: In den folgenden Beispielen ist $\frac{\ln(d)}{\ln(N)} \approx 0.25$. Manchmal ist der Algorithmus erfolgreich, manchmal nicht.

1. Beispiel:

$$
\begin{aligned}
N &= 82257510389380447225013058328054960189274459591361757147434743211245 63\\
p &= 63642133071342787856743220237688643\\
q &= 12925008389830339920376935931753144 1\\
\frac{q}{p} &= 2.030889\\
e &= 65798253881547077561033458280194449501897084997263138289422141262 4333\\
d &= 1111235133951504677\\
\frac{\ln(d)}{\ln(N)} &= .258110\\
\frac{e}{N-\left\lfloor\sqrt{4N}\right\rfloor} &= [0, 12, 1, 1, 169, 4, 1, 7, 3, 2, 1, 1, 1, 1, 1, 1, 1, 1, 1, 7, 1, 1, 6, 24, 1, 8, 1, 2, 1, 8, 3, 1, 2, 1, 1, 2,\\
&\quad 211, 1, 6, 4, 15, 5, 6, 14, 2, 1, 32, 1, 5, 1, 1, 7, 7, 17, 1, 1, 2, 1, 1, 2, 21, 1, 2, 1, 32, 2, 4, 3, 37, 4,\\
&\quad 6, 9, 2, 2, 1, 1, 3, 5, 1, 7, 1, 4, 8, 2, 2, 3, 1, 40, 2, 1, 7, 10, 1, 1, 54, 1, 24, 1, 1, 5, 1, 1, 4, 3, 3, 1, 10,\\
&\quad 1, 5, 1, 61, 1, 5, 3, 2, 1, 10, 1, 1, 4, 3, 2, 2, 2, 8, 1, 1, 1, 7, 1, 3, 2, 4]\\
\frac{k}{d} &= [0, 12, 1, 1, 169, 4, 1, 7, 3, 2, 1, 1, 1, 1, 1, 1, 1, 1, 1, 7, 1, 1, 6, 24, 1, 8, 1, 2, 1, 8, 3, 1, 2, 1, 1, 2,\\
&\quad 212]
\end{aligned}
$$

Der Algorithmus hat Erfolg.

2. Beispiel:

$$
\begin{aligned}
N &= 16267828224447286944047076614006829226087184613526395634552214561790 97\\
p &= 24257763286132280790960960610552741\\
q &= 67062358687238516099099348034732517\\
\frac{q}{p} &= 2.764573\\
e &= 93287748061254136097346812144579989544445924143659894076836187483092 3\\
d &= 489467349331406467\\
\frac{\ln(d)}{\ln(N)} &= .255590\\
\frac{e}{N-\left\lfloor\sqrt{4N}\right\rfloor} &= [0, 1, 1, 2, 1, 9, 2, 1, 1, 2, 12, 63, 1, 6, 3, 1, 2, 2, 1, 2, 5, 5, 1, 1, 1, 104, 34, 1, 1, 2, 1, 18, 1, 1, 1, 7,\\
&\quad 24, 1, 6, 1, 13, 2, 9, 63, 4, 15, 2, 2, 1, 22, 3, 5, 3, 9, 3, 1, 2, 1, 2, 4, 1, 1, 54, 1, 1, 1, 4, 70, 1, 6, 2, 1,\\
&\quad 29, 1, 2, 1, 2, 42, 4, 4, 3, 9, 5, 2, 1, 2, 17, 1, 20, 1, 2, 2, 3, 8, 1, 2, 1, 4, 4, 3, 2, 2, 6, 5, 2, 1, 5, 1, 2,\\
&\quad 3, 8, 29, 1, 2, 1, 22, 2, 24, 1, 1, 4, 3, 1, 4, 6]\\
\frac{k}{d} &= [0, 1, 1, 2, 1, 9, 2, 1, 1, 2, 12, 63, 1, 6, 3, 1, 2, 2, 1, 2, 5, 5, 1, 1, 1, 104, 34, 1, 1, 2, 1, 18, 1, 1, 1, 6]
\end{aligned}
$$

Der Algorithmus hat keinen Erfolg.

3. Beispiel:

$$
\begin{aligned}
N &= 584848245832818966184145525652796528482850386898810478316658617713489 9\\
p &= 469363413326147222407077485288784 77\\
q &= 124604566361124665250581388345956287\\
\frac{q}{p} &= 2.654757\\
e &= 43142442550884520582247716941939330380060285181477518135142620108715 1\\
d &= 699303130395894943\\
\frac{\ln(d)}{\ln(N)} &= .255775\\
\frac{e}{N - \left\lfloor \sqrt{4N} \right\rfloor} &= [0, 13, 1, 1, 3, 1, 17, 1, 13, 1, 1, 34, 4, 21, 2, 3, 3, 1, 3, 1, 1, 1, 2, 1, 1, 2, 1, 11, 1, 2, 62, 1, 17, 2, 3, 1,\\
&\quad 7, 1, 16, 1, 4, 1, 8, 1, 1, 1, 4, 1, 2, 1, 1, 3, 3, 4, 6, 2, 1, 2, 2, 1, 1, 15, 1, 1, 1, 14, 1, 9, 1, 3, 2, 56,\\
&\quad 2, 49, 1, 6, 1, 3, 1, 2, 4, 2, 4, 4, 1, 938, 1, 1, 22, 4, 2, 1, 11, 10, 2, 1, 1, 6, 2, 1, 1, 15, 249, 1, 1,\\
&\quad 22, 1, 1, 4, 1, 1, 1, 1, 2, 2, 3, 1, 5, 2, 12, 22, 4, 4, 2, 1, 5, 1, 1, 12, 2, 3, 1, 2, 1, 16]\\
\frac{k}{d} &= [0, 13, 1, 1, 3, 1, 17, 1, 13, 1, 1, 34, 4, 21, 2, 3, 3, 1, 3, 1, 1, 1, 2, 1, 1, 2, 1, 11, 1, 2, 62, 1, 17, 2, 4]
\end{aligned}
$$

Der Algorithmus hat Erfolg.

4. Beispiel:

$$
\begin{aligned}
N &= 628132752154033093821256475001725389032356982878193434482485231932719 1\\
p &= 546258460653743701757467628764631 51\\
q &= 114988196503593738651573799794638041\\
\frac{q}{p} &= 2.105014\\
e &= 26722347180210576408089314460079188881804027372274115107185929368163 41\\
d &= 885468195135947261\\
\frac{\ln(d)}{\ln(N)} &= .257130\\
\frac{e}{N - \left\lfloor \sqrt{4N} \right\rfloor} &= [0, 2, 2, 1, 5, 1, 3, 2, 1, 1, 3, 12, 1, 1, 1, 2, 3, 1, 4, 1, 1, 5, 19, 65, 168, 1, 3, 1, 1, 1, 5, 1, 4, 3, 1, 1,\\
&\quad 2, 1, 2, 2, 27, 3, 8, 1, 2, 1, 1, 1, 1, 3, 4, 3, 1, 1, 2, 1, 5, 2, 1, 2, 7, 3, 1, 3, 1, 1, 8, 1, 1, 2, 1, 2, 1, 2,\\
&\quad 2, 2, 4, 2, 3, 1, 2, 1, 37, 1, 3, 1, 2, 1, 5, 20, 15, 1, 3, 1, 117, 1, 1, 1, 1, 1, 2, 6, 1, 2, 19, 1, 3, 2, 1, 2,\\
&\quad 1, 2, 20, 1, 3, 2, 9548, 3, 8, 1, 27, 1, 1, 1, 19, 12, 2, 1, 18, 2, 9, 1, 1, 1, 1, 1, 7, 2, 2, 2, 2, 1, 1, 1, 2, 4]\\
\frac{k}{d} &= [0, 2, 2, 1, 5, 1, 3, 2, 1, 1, 3, 12, 1, 1, 1, 2, 3, 1, 4, 1, 1, 5, 19, 65, 168, 1, 3, 1, 1, 1, 5, 1, 4, 3, 1, 1,\\
&\quad 2, 1, 3]
\end{aligned}
$$

Der Algorithmus hat keinen Erfolg.

5. Beispiel:

$$
\begin{aligned}
N &= 44153262380073646954383015297853068889355406107977111244330514010805 63\\
p &= 469376055532583386868408327057109 67\\
q &= 940679906007872470706034261592635 89\\
\frac{q}{p} &= 2.004107\\
e &= 939878508601349839923620992908733807690086968342232503417680162545 5\\
d &= 7189884310724546759\\
\frac{\ln(d)}{\ln(N)} &= .270755\\
\frac{e}{N-\left\lfloor\sqrt{4N}\right\rfloor} &= [0, 469, 1, 3, 2, 7, 1, 3, 3, 1, 3, 1, 608, 58, 1, 60, 6, 36, 1, 1, 11, 2, 1, 3, 1, 2, 2, 2, 4, 1, 1, 6,\\
&\quad 1, 1, 1, 1, 1, 1, 95, 1, 7, 3, 2, 6, 2, 4, 2, 1, 8, 1, 1, 90, 1, 1, 1, 5, 1, 24, 4, 2, 13, 1, 2, 1, 5, 6, 6,\\
&\quad 1, 3, 21, 27, 1, 9, 1, 9, 216, 1, 1, 8, 6, 5, 1, 6, 1, 1, 3, 1, 2, 6, 2, 1, 1, 11, 4, 2, 1, 23, 1, 1, 1, 1,\\
&\quad 6, 1, 124, 7, 3, 6, 57, 4, 13, 2, 1, 13, 1, 74]\\
\frac{k}{d} &= [0, 469, 1, 3, 2, 7, 1, 3, 3, 1, 3, 1, 608, 58, 1, 60, 6, 36, 1, 1, 11, 2, 1, 3, 1, 2, 2, 2]
\end{aligned}
$$

Der Algorithmus hat Erfolg. (Dies ist ein interessantes Beispiel.)

6. Beispiel:

$$
\begin{aligned}
N &= 59814262581111495012520362949654103505409384361061312972576470421892 69\\
p &= 52855629701729781274727756693095853\\
q &= 11316535801134156545705016789726407 3\\
\frac{q}{p} &= 2.141028\\
e &= 86786843645279280511129693026396951865865848025826625695467692956779 1\\
d &= 775134741803520975\\
\frac{\ln(d)}{\ln(N)} &= .256380\\
\frac{e}{N-\left\lfloor\sqrt{4N}\right\rfloor} &= [0, 6, 1, 8, 3, 1, 2, 1, 20, 1, 26, 1, 2, 1, 37, 1, 1, 4, 2, 1, 4, 1, 1, 1, 3, 5, 1, 1, 134, 1, 3, 4, 6, 1, 25,\\
&\quad 1, 5, 11, 1, 1, 13, 41, 1, 3, 1, 3, 2, 3, 1, 9, 1, 1, 10, 1, 2, 1, 4, 3, 2, 5, 3, 1, 1, 2, 10, 1, 1, 1, 1, 1, 1,\\
&\quad 35, 2, 1, 3, 1, 1, 6, 1, 2, 1, 3, 1, 151, 5, 1, 1, 2, 1, 2, 13, 1, 1, 96, 2, 1, 1, 7, 1, 1, 3, 3, 7, 9, 2, 4, 1,\\
&\quad 1, 5, 2, 1, 1, 1, 9, 9, 14, 5, 5, 3, 1, 3, 3, 4, 517, 1, 1, 1, 2, 22, 3, 3, 1, 2, 1, 3, 1, 4, 4]\\
\frac{k}{d} &= [0, 6, 1, 8, 3, 1, 2, 1, 20, 1, 26, 1, 2, 1, 37, 1, 1, 4, 2, 1, 4, 1, 1, 1, 3, 5, 1, 1, 134, 1, 3, 4, 6, 1, 26]
\end{aligned}
$$

Der Algorithmus hat Erfolg.