RSA – Ein asymmetrisches Verschlüsselungs- und Entschlüsselungsverfahren

Übersicht

Das **RSA**-Verfahren ist nach seinen Urhebern Rivest, Shamir und Adleman aus dem Jahr 1978 benannt.

1. Anleitung zur Verschlüsselung und Entschlüsselung

1.1 Wähle zwei Primzahlen p und q (für nennenswerte Datensicherung jeweils größer als 512 Bit)
1.2 Berechne $n = p \cdot q$ und $z = \Phi(n) = (p-1)\cdot(q-1)$
1.3 Wähle Zahl d, die teilerfremd zu $z = \Phi(n)$ ist
1.4 Finde Zahl e, sodass $d \cdot e = 1 \pmod z$
1.5 Vernichte p und q
1.6 Verschlüssele: $C = P^d \pmod n$ mit P – Klartextnachricht, C – Chiffrat; d und n werden als öffentlicher Schlüssel (public key) bezeichnet
1.7 Entschlüssele: $P = C^e \pmod n$; e und n werden als privater Schlüssel (private key) bezeichnet

2. Einfaches noch unrealistisches Beispiel

2.1 p = 3, q = 11
2.2 $n = 33,\ z = \Phi(n) = 20$
2.3 d = 3, 7 und 20 haben keine gemeinsamen Faktoren außer 1
2.4 $7 \cdot 3 \equiv 1 \pmod{20}$ → e = 7
2.5 –
2.6 Der Klartext liegt als Bitkette vor und wird in Blöcke aufgeteilt, derart dass jede Klartextnachricht P im Intervall $0 \le P \le n$ liegt. Dazu wird der Klartext in Blöcke zu je k Bit angeordnet, k entspricht der größten ganzen Zahl mit $2^k < n$.

Ein zu übertragender Text sei „ZAUN“. Den Buchstaben werden Zahlen zugeordnet: A = 01; B = 02; …; Z = 26 mit k = 5 und 0 ≤ 26 ≤ 33.

Verschlüsselung durch den Sender

	P	P^3	$C = P^3 \pmod{33}$
Z	26	17576	20
A	01	1	1
U	21	9261	21
N	14	2744	5

2.7 Empfang: 20 1 21 5

Entschlüsselung durch den Empfänger

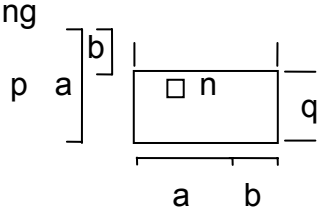
C^7	$P \equiv C^7 \pmod{33}$	
1280000000	26	Z
1	1	A
1801088541	21	U
78125	14	N

Erläuterungen:

- Die Reihenfolge der Berechnung bzw. Festlegung von d und e ist beliebig.
- P musste sehr klein gewählt werden (n = 33), sodass ein Klartextblock nur ein Zeichen enthält.
- Mit p und q im Bereich 2^{512} wäre $n \approx 2^{1024}$ und jeder Block könnte bis zu 1024 oder 128 Byte enthalten.
- Ohne p und q können – sofern sie genügend groß gewählt sind – $z = \Phi(n)$ sowie d und e derzeit nicht bestimmt werden. Es bestehen große Schwierigkeiten bei gegebenem n p und q zu bestimmen.
- Die Codierung von „A“ zu 01 ist denkbar ungünstig.

3. Einfache Faktorisierung einer Zahl n (Bestimmung zweier Primzahlen p und q aus ihrem Produkt n)

Deutung



$n = p\,q = (a + b)(a - b) = a^2 - b^2$

Näherung:

Aus n lässt sich $n_W = \sqrt{n}\uparrow$ bestimmen, d.i. die Wurzel aus n aufgerundet auf die nächste natürliche Zahl

Bsp.: n = 5.607.013; $n_W = \sqrt{n}\uparrow = 2.368$

es gilt: $q < n_W < p$

$a = \sqrt{n + b^2}$; $\qquad b = \sqrt{a^2 - n}$

$a = n_W + x$; $\qquad b = n_W - y$

$a = \sqrt{n + (n_W - y)^2}$; $\qquad b = \sqrt{(n_W + x)^2 - n}$

1. Beispiel:

n =33; $\qquad n_W = 6$

$b = \sqrt{(6+x)^2 - n} \quad \Rightarrow \quad x = 1 : \sqrt{49 - 33} = 4 = b$

$a = \sqrt{n + b^2} = 7$

$(a+b)(a-b) = 11 \cdot 3 = 33 = p \cdot q = n$

2. Beispiel:

a) n = 5.607.013 $\qquad n_W = 2.368$

$b = \sqrt{(2368+x)^2 - n} \quad \Rightarrow \quad x = 1 : \sqrt{2369^2 - n} = 71,...$

$x = 2 : \sqrt{2370^2 - n} = 99,...$ Iteration 2
…
$x = 915 : \sqrt{3283^2 - n} = 2274,00 = b$ Iteration 915

$a = \sqrt{n + b^2} = 3283$

$(a+b)(a-b) = 5557 \cdot 1009 = 5607013 = p \cdot q = n$

oder

b) $a = \sqrt{n + (2368 - y)^2} \quad \Rightarrow \quad y = 1 : \sqrt{n + 2367^2} = 3348,...$

$y = 2 : \sqrt{n + 2366^2} = 3347,...$ Iteration 2
…
$x = 94 : \sqrt{n + 2274^2} = 3283,00 = a$ Iteration 94

$b = \sqrt{a^2 - n} = 2274$

$(a+b)(a-b) = 5557 \cdot 1009 = 5607013 = p \cdot q = n$

Offensichtlich führt der Weg nach 2b) schneller zum Ergebnis.

4. Realistischeres Beispiel

Text: „*RSA works!*“ als ASCII: „82 83 65 32 119 111 114 107 115 33“

Primzahlen: p = 509, q = 503 → n = 256.027
z = 255.016

d = 65.537 65.537 = 65.536 + 1 = $2^{16} + 2^0$!
in der Bitfolge kommen nur zwei Einsen vor → schnelle Multiplikation (Exponentiation)

es sollte sein: max(p, q) < d < Φ(n) = z;
es muss sein: d und z relativ prim, d.h. teilerfremd

$$\frac{d \cdot e}{z} = x \,\text{Rest}\, 1 \quad \leftrightarrow \quad d \cdot e \equiv 1 \,(\text{mod}\, z)$$

e = 231.953 mit dem Euklidschen Algorithmus bestimmt (s. Abschnitt 7, S. 10)

d e = 65.537 231.953 = 15.201.503.761 ≡ 1 (mod 255.016)

Codierung mit 2er-Blockbildung (Zahlen < n)

Zwei Zahlen werden als 8-stellige Binärzahlen hintereinander geschrieben[1]:

[1] die Zahlen können auch als 3-stellige Dezimalzahlen hintereinander geschrieben werden (082083065032119usw.)

82 83	01010010 01010011	≡	$2^{14} + 2^{12} + 2^9 + 2^6 + 2^4 + 2^1 + 2^0$
Bitstelle	15. . . . 10 . . . . 5 1	≡	21.075
65 32	01000001 00100000	≡	$2^{14} + 2^8 + 2^5$ ≡ 16.672
119 111	01110111 01101111	≡	$2^{14} + 2^{13} + 2^{12} + 2^{10} + 2^9 + 2^8 + 2^6 + 2^5 + 2^3 + 2^2 + 2^1 + 2^0$ ≡ 30.575
114 107	01110010 01101011	≡	$2^{14} + 2^{13} + 2^{12} + 2^9 + 2^6 + 2^5 + 2^3 + 2^1 + 2^0$ ≡ 29.291
115 33	01110011 00100001	≡	$2^{14} + 2^{13} + 2^{12} + 2^9 + 2^8 + 2^5 + 2^0$ ≡ 29.473

Verschlüsselung $C = P^d \ (mod\ n)$ $21.075^{65.537}$ (mod 256.027)

Exponentenzerlegung: 65.537 = 65.536 + 1
(andere Exponenten werden nur für Zwischenergebnisse benötigt)

$P^1 \pmod n \equiv 21.075 \pmod n \equiv 21.075$ ← 21.075 wird zur Chiffrierung benötigt

(Rechnen mit dem Rest vereinfacht wesentlich das weitere Vorgehen; s. Abschnitt 5, S. 7)

$P^2 \pmod n \equiv 21.075^2 \pmod n \equiv 204.807$

$P^4 \pmod n \equiv 204.807^2 \pmod n \equiv 235.758$

$P^8 \pmod n \equiv 235.758^2 \pmod n \equiv 165.053$

$P^{16} \pmod n \equiv 165.053^2 \pmod n \equiv 195.901$

$P^{32} \pmod n \equiv 195.901^2 \pmod n \equiv 34.636$

$P^{64} \pmod n \equiv 34.636^2 \pmod n \equiv 166.001$

$P^{128} \pmod n \equiv 166.001^2 \pmod n \equiv 145.991$

$P^{256} \pmod n \equiv 145.991^2 \pmod n \equiv 148.439$

$P^{512} \pmod n \equiv 148.439^2 \pmod n \equiv 197.074$

$P^{1024} \pmod n \equiv 197.074^2 \pmod n \equiv 145.711$

$P^{2048} \pmod n \equiv 145.711^2 \pmod n \equiv 144.492$

$P^{4096} \pmod n \equiv 144.492^2 \pmod n \equiv 216.349$

$P^{8192} \pmod n \equiv 216.349^2 \pmod n \equiv 33.661$

$P^{16384} \pmod n \equiv 33.661^2 \pmod n \equiv 143.446$

$P^{32768} \pmod n \equiv 143.446^2 \pmod n \equiv 120.953$

$P^{65536} \pmod n \equiv 120.953^2 \pmod n \equiv 245.429$ ← wird zur Chiffrierung benötigt

$C \equiv P^d \pmod n \equiv [P^{65536} \pmod n \;\; P^1 \pmod n] \pmod n \equiv [245.429 \;\; 21.075] \pmod n$

$C \equiv 5.172.416.175 \pmod n \equiv 158.721$

Übertragen wird: 158.721 137.346 37.058 240.130 112.898
(hier wurde nur die erste Zahl berechnet)

Entschlüsselung $P = C^e \pmod n$ $158.721^{231.953} \pmod{256.027}$

Exponentenzerlegung:
231.953 = 131.072 + 65.536 + 32.768 + 2.048 + 512 + 16 + 1

C^{1} (mod n) ≡ 158.721 (mod n) ≡ 158.721 ←

C^{2} (mod n) ≡ 158.721^{2} (mod n) ≡ 67.122

C^{4} (mod n) ≡ 67.122^{2} (mod n) ≡ 55.765

C^{8} (mod n) ≡ 55.765^{2} (mod n) ≡ 31.283

C^{16} (mod n) ≡ 31.283^{2} (mod n) ≡ 90.895 ←

C^{32} (mod n) ≡ 90.895^{2} (mod n) ≡ 165.762

C^{64} (mod n) ≡ 165.762^{2} (mod n) ≡ 223.004

C^{128} (mod n) ≡ 223.004^{2} (mod n) ≡ 99.536

C^{256} (mod n) ≡ 99.536^{2} (mod n) ≡ 194.504

C^{512} (mod n) ≡ 194.504^{2} (mod n) ≡ 232.388 ←

C^{1024} (mod n) ≡ 232.388^{2} (mod n) ≡ 151.407

C^{2048} (mod n) ≡ 151.407^{2} (mod n) ≡ 190.150 ←

C^{4096} (mod n) ≡ 190.150^{2} (mod n) ≡ 121.479

C^{8192} (mod n) ≡ 121.479^{2} (mod n) ≡ 7.188

C^{16384} (mod n) ≡ 7.188^{2} (mod n) ≡ 205.917

C^{32768} (mod n) ≡ 205.917^{2} (mod n) ≡ 155.311 ←

C^{65536} (mod n) ≡ 155.311^{2} (mod n) ≡ 178.943 ←

C^{131072} (mod n) ≡ 178.943^{2} (mod n) ≡ 68.440 ←

$$[68440 \cdot 178943 \cdot 155311 \cdot 190150 \cdot 232388 \cdot 90895 \cdot 158721] (\mathrm{mod}\, 256027) \equiv 21075$$

Mit einem Taschenrechner gerechnet:
[(68440 178943) (155311 190150) (232388 90895) (158721)](mod 256027) →

(68440 178943) ≡ 63402 (mod 256027)
(155311 190150) ≡ 184254 (mod 256027)
(232388 90895) ≡ 167706 (mod 256027)
(158721) ≡ 158721 (mod 256027)

(63402 184254) ≡ 72152 (mod 256027)
(167706 158721) ≡ 104917 (mod 256027)

(72152 104917) ≡ 21075 (mod 256027)

21075 ≡ 01010010 01010011 ≡ $2^{14} + 2^{12} + 2^9 + 2^6 + 2^4 + 2^1 + 2^0$

Bitstelle 15. . . . 10 . . . . 5 1

bzw. 01010010 ≡ $2^6 + 2^4 + 2^1 = 64 + 16 + 2$ ≡ 82 ≡ R und

01010011 ≡ $2^6 + 2^4 + 2^1 + 2^0 = 64 + 16 + 2 + 1$ ≡ 83 ≡ S

5. Modulo-Berechnung für große Zahlen

Im vorherigen Abschnitt wurde die vereinfachte Modulo-Berechnung verwendet. Hier soll eine Begründung für deren Richtigkeit gegeben werden.

Wie lässt sich beispielsweise $31^{792} (\mathrm{mod} 851)$ möglichst einfach berechnen?

Wenn die Rechnung auch nicht allzu schwierig ist, so ist sie doch – für diese Ausführungen – recht umfangreich, weshalb hier mit kleineren Zahlen, die auch auf einfachen Taschenrechnern handhabbar sind, gerechnet wird.

Es seien: $m < n; a, b, m, n, x \in N; m^2 = a + b \wedge a(\mathrm{mod}\, n) = 0.$

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

$$m^2 (\mathrm{mod}\, n) = x$$

$$m^4 (\mathrm{mod}\, n) = [(a+b)(a+b)](\mathrm{mod}\, n) = \left[a^2 + 2ab + b^2\right](\mathrm{mod}\, n) \equiv b^2 (\mathrm{mod}\, n)$$

1. Beispiel:

$$31^4 (\mathrm{mod} 851) = \left[31^2 \cdot 31^2\right](\mathrm{mod} 851) = [961 \cdot 961](\mathrm{mod} 851) =$$

$$[(851+110)(851+110)](\mathrm{mod} 851) = \left[851^2 + 2 \cdot 851 \cdot 110 + 110^2\right](\mathrm{mod} 851) \equiv$$

zu $b^2 = 110^2$ wird eine Zahl addiert (oder zwei oder mehr), die durch 851 ohne Rest dividierbar ist, d.h. sie kann bei der Modulo-Rechnung auch weggelassen werden.

$$\left[110^2\right](\mathrm{mod} 851) = 186$$

entsprechend höhere Potenzen:

$$m^8 (\mathrm{mod}\, n) = \left[m^4 m^4\right](\mathrm{mod}\, n) = \left\{[(a+b)(a+b)]^2 [(a+b)(a+b)]^2\right\}(\mathrm{mod}\, n) =$$

$$\left\{a^4 + 4a^3 b + 6a^2 b^2 + 4ab^3 + b^4\right\}(\mathrm{mod}\, n) \equiv b^4 (\mathrm{mod}\, n)$$

2. Beispiel:

$$31^8 \,(\mathrm{mod}\, 851) = [(851+110)(851+110)]^2 \,(\mathrm{mod}\, 851) =$$

$$\left[851^4 + 4\cdot 851^3 \cdot 110 + 6\cdot 851^2 \cdot 110^2 + 4\cdot 851\cdot 110^3 + 110^4\right](\mathrm{mod}\, 851) \equiv$$

$$\left[110^4\right](\mathrm{mod}\, 851) = \left[110^2 \cdot 110^2\right](\mathrm{mod}\, 851) = [(11914+186)(11914+186)](\mathrm{mod}\, 851) \equiv$$

$$186^2 \,(\mathrm{mod}\, 851) = 556$$

und eine letzte Potenz

$$m^{16} \,(\mathrm{mod}\, n) = \left[m^8 m^8\right](\mathrm{mod}\, n) = \left\{[(a+b)(a+b)]^4 [(a+b)(a+b)]^4\right\}(\mathrm{mod}\, n) =$$

$$\left\{\ldots \quad + b^8\right\}(\mathrm{mod}\, n)$$

3. Beispiel:

$$31^{16} \,(\mathrm{mod}\, 851) = [(851+110)(851+110)]^4 \,(\mathrm{mod}\, 851) =$$

$$\left[\ldots \quad + 110^8\right](\mathrm{mod}\, 851) \equiv$$

$$\left[110^4 \cdot 110^4\right](\mathrm{mod}\, 851) = \left[(11914+186)^2 (11914+186)^2\right](\mathrm{mod}\, 851) \equiv$$

$$\left[186^2 \cdot 186^2\right](\mathrm{mod}\, 851) \equiv 556^2 \,(\mathrm{mod}\, 851) \equiv 223$$

6. Berechnung der modularen Inversen nach der Vielfachsummendarstellung

In diesem Abschnitt wird e bestimmt, sodass

$\frac{d \cdot e}{\Phi(n)} = x \text{ Rest } 1 \Leftrightarrow (d \cdot e) \equiv 1 (\mathrm{mod}\ \Phi(n))$.

Vorgegeben wird d. Es sollte sein: max(p, q) < d < Φ(n)
d und Φ(n) müssen teilerfremd sein

Zunächst allgemeine Darstellung.

Sei m der größte gemeinsame Teiler von a und b, dann gibt es ganze Zahlen s und t mit der Eigenschaft

$$m = s \cdot a + t \cdot b \qquad \text{(Vielfachsummendarstellung des ggT)}$$

1. Beispiel: a = 37, b = 16;

$$a = r_0 = q_1 r_1 + r_2 \qquad r_0 = 37 = \left\lfloor \frac{37}{16} \right\rfloor \cdot 16 + 5 \qquad q_1 = 2,\ r_2 = 5, \text{mit } q_1 = \left\lfloor \frac{a}{b} \right\rfloor \cdot b$$

$$r_1 = q_2 r_2 + r_3 \qquad r_1 = 16 = \left\lfloor \frac{16}{5} \right\rfloor \cdot 5 + 1 \qquad q_2 = 3,\ r_3 = 1$$

$r_2 = q_3 r_3 + r_4$ $\qquad r_2 = 5 = \left\lfloor \frac{5}{1} \right\rfloor \cdot 5 + 0 \qquad q_3 = 5,\ r_4 = 0$

d.h.

$r_3 = r_1 - q_2 r_2 = r_1 - q_2 (r_0 - q_1 r_1) = -r_0 q_2 + r_1 (1 + q_1 q_2)$

$r_3 = 1 = -37 \cdot 3 + 16 \cdot 7$ s.o.: a =37, b = 16, → s = -3, t = 7,

letzter Rest r_3 ($r_4 = 0$) ist nur von r_0, r_1 und q_i abhängig.

Anwendbar zur Bestimmung von e für die Gleichung: $1 = x \cdot \Phi(n) + d \cdot e$

2. Beispiel: p = 47; q = 79; n = p q = 3713; Φ(n) = z = 3588;

gewählt d = 37 es sollte sein: max(p, q) < d < Φ(n) ; trifft hier nicht zu;
d und Φ(n) müssen teilerfremd sein ; trifft zu;
(37 e) ≡ 1 (mod 3588).

$a = r_0 = q_1 r_1 + r_2 \qquad r_0 = 3588 = \left\lfloor \frac{3588}{37} \right\rfloor \cdot 37 + r_2 = 96 \cdot 37 + 36$

$r_1 = q_2 r_2 + r_3 \qquad r_1 = 37 = \left\lfloor \frac{37}{36} \right\rfloor \cdot 36 + r_3 = 1 \cdot 36 + 1$

$r_2 = q_3 r_3 + r_4 \qquad r_2 = 36 = \left\lfloor \frac{36}{1} \right\rfloor \cdot 1 + r_4 = 36 \cdot 1 + 0$

$r_3 = 1 = -r_0 q_2 + r_1 (1 + q_1 q_2)$

$r_3 = 1 = -3588 \cdot 1 + 37 \cdot 97$

daraus e = 97 Probe: $\frac{37 \cdot 97}{3588} = 1 \text{ Rest } 1$; oder $(37 \cdot 97) \equiv 1 \pmod{3588}$

Vgl. jeweils die Kettenbruchdarstellung:

$$\frac{37}{16} = 2 + \frac{1}{3 + \frac{1}{5}}$$

2, 3, 5 sind die q_i aus Beispiel 1.

$$\frac{3588}{37} = 96 + \frac{1}{1 + \frac{1}{36}}$$

96, 1, 36 sind die q_i aus dem letzten Beispiel.

Die Vielfachsummendarstellung kann zu unnötig großen e führen. Da die e Exponenten sind, ist dies umso problematischer. Deshalb folgt anschließend im Kapitel 7 die Berechnung mit dem (erweiterten) Euklidschen Algorithmus.

7. Berechnung der modularen Inversen mit dem Euklidschen Algorithmus

Da es u. U. wichtig ist zu wissen, dass der größte gemeinsame Teiler (ggT) zweier natürlicher Zahlen Eins ist, wird zunächst eine Vorgehensweise zu Bestimmung dieses ggT vorgestellt.

s.o. Vielfachsummendarstellung

$ggT(a,b) = m = s \cdot a + t \cdot b \qquad Bsp.: ggT(37,16) = 1 = (-3) \cdot 37 + 7 \cdot 16$

Algorithmus:

1. Setze m := a, n: = b, s = 1, t = 0, u = 0, v = 1

$$a = 1 \cdot a + 0 \cdot b \qquad 37 = 1 \cdot 37 + 0 \cdot 16$$
$$b = 0 \cdot a + 1 \cdot b \qquad 16 = 0 \cdot 37 + 1 \cdot 16$$

$$m = s \cdot a + t \cdot b \qquad m = 37$$
$$n = u \cdot a + v \cdot b \qquad n = 16$$

2. Berechne q und r mit $m = q \cdot n + r, \quad q = \left\lfloor \frac{m}{n} \right\rfloor$

$$q = \left\lfloor \frac{m}{n} \right\rfloor \qquad q = 2$$

$$r = m - q \cdot n = sa + tb - q(ua + vb) \qquad r = 37 - 2 \cdot 16 = 5$$

$$r = (s - qu)a + (t - qv)b$$

3. Setze m := n, n: = r, berechne r neu; Abbruch bei r = 0 bzw. n = 1 sonst Punkt 2 und 3 wiederholen

$$37 = 1 \cdot 37 + 0 \cdot 16$$

$$m := n = 16 = 0 \cdot 37 + 1 \cdot 16$$

$$n := r = 5 = 1 \cdot 37 - 2 \cdot 16$$

Zur Berechnung der rechten Seite von n = r zieht man von der vorletzten Zeile (37 = …) das entsprechende Vielfache der letzten Zeile ab.

Deshalb:
$r = m - q \cdot n$ mit q = 2

$$37 = 1 \cdot 37 + 0 \cdot 16$$

$-2 \quad (16 = 0 \cdot 37 + 1 \cdot 16)$

$\Rightarrow \quad 5 = 1 \cdot 37 - 2 \cdot 16$

$m := n = 16 = 0 \cdot 37 + 1 \cdot 16$ 2. Runde

$n := r = 5 = 1 \cdot 37 - 2 \cdot 16$

$q = \left\lfloor \frac{m}{n} \right\rfloor = \left\lfloor \frac{16}{5} \right\rfloor = 3$

$r = m - q \cdot n = 16 - 3 \cdot 5 = 1$ (q = 3)

$16 = 0 \cdot 37 + 1 \cdot 16$

$-3 \quad (5 = 1 \cdot 37 - 2 \cdot 16)$

$\Rightarrow \quad 1 = (-3) \cdot 37 + 7 \cdot 16$

$m := n = 5 = 1 \cdot 37 - 2 \cdot 16$ 3. Runde

$n := r = 1 = (-3) \cdot 37 + 7 \cdot 16$

$q = \left\lfloor \frac{m}{n} \right\rfloor = \left\lfloor \frac{5}{1} \right\rfloor = 5$

$r = m - q \cdot n = 5 - 5 \cdot 1 = 0$ (q = 5)

$5 = 1 \cdot 37 - 2 \cdot 16$

$-5 \quad (1 = (-3) \cdot 37 + 7 \cdot 16)$

$\Rightarrow \quad 0 = 16 \cdot 37 - 37 \cdot 16$ Abbruch: r = 0 und rechte Seite trivial
Zeile r = 1 bedeutet: ggT(37,16) = 1

1. Beispiel: $m = 124, n = 30$

$124 = 1 \cdot 124 + 0 \cdot 30$

$-4 \quad (30 = 0 \cdot 124 + 1 \cdot 30)$ $q = \left\lfloor \frac{124}{30} \right\rfloor = 4, r = 4$

$\Rightarrow \quad 4 = 1 \cdot 124 - 4 \cdot 30$ $r = m - qn$

$30 = 0 \cdot 124 + 1 \cdot 30$

$-7 \quad (4 = 1 \cdot 124 - 4 \cdot 30)$ $q = \left\lfloor \frac{30}{4} \right\rfloor = 7, r = 2$

$\Rightarrow \quad 2 = (-7) \cdot 124 + 29 \cdot 30$ $r = m - qn$

$$4 = 1 \cdot 124 - 4 \cdot 30$$

$-2 \quad (2 = (-7) \cdot 124 + 29 \cdot 30) \qquad q = \left\lfloor \frac{4}{2} \right\rfloor = 2,\ r = 0$

$\Rightarrow \quad 0 = 15 \cdot 124 - 58 \cdot 30$ Abbruch: ggT(124,30) = 2

Der erweiterte Euklidsche Algorithmus kann so zur Bestimmung des Exponenten e beim Empfänger herangezogen werden

$$\frac{d \cdot e}{\Phi(n)} \equiv x \quad \text{Rest } 1 \quad \Leftrightarrow \quad (d \cdot e) \equiv 1 \left(\bmod \Phi(n)\right)$$

2. Beispiel: $p = 47,\ q = 79 \Rightarrow n = 3713, \Phi(n) = 46 \cdot 78 = 3588;$ gewählt $d = 37$

$$3588 = 1 \cdot 3588 + 0 \cdot 37$$

$-96 \quad (37 = 0 \cdot 3588 + 1 \cdot 37) \qquad q = \left\lfloor \frac{3588}{37} \right\rfloor = 96,\ r = 36$

$\Rightarrow \quad 36 = 1 \cdot 3588 - 96 \cdot 37$

$$37 = 0 \cdot 3588 + 1 \cdot 37$$

$-1 \quad (36 = 1 \cdot 3588 - 96 \cdot 37) \qquad q = \left\lfloor \frac{37}{36} \right\rfloor = 1,\ r = 1$

$\Rightarrow \quad 1 = (-1) \cdot 3588 + 97 \cdot 37$ damit ist zu d = 37 der Faktor e = 97 gefunden (ggT(3588,37) = 1)

$$36 = 1 \cdot 3588 - 96 \cdot 37$$ der Vollständigkeit halber weiter

$-36 \quad (1 = (-1) \cdot 3588 + 97 \cdot 37) \qquad q = \left\lfloor \frac{36}{1} \right\rfloor = 36,\ r = 0$

$\Rightarrow \quad 0 = 37 \cdot 3588 - 3588 \cdot 37$

Die berechneten Quotienten q_i lauten: 96, 1, 36 vergleiche Kettenbruchdarstellung:

$$\frac{3588}{37} = 96 + \frac{1}{1 + \frac{1}{36}}$$

3. Beispiel: $p = 59,\ q = 83 \Rightarrow n = 4897, \Phi(n) = 4756;$ gewählt $d = 7$

$$4756 = 1 \cdot 4756 + 0 \cdot 7$$

$-679 \ (7 = 0 \cdot 4756 + 1 \cdot 7) \qquad q = \left\lfloor \frac{4756}{7} \right\rfloor = 679,\ r = 3$

$-2 \quad (3 = 1 \cdot 4756 - 679 \cdot 7) \qquad q = \left\lfloor \frac{7}{3} \right\rfloor = 2,\ r = 1$

$-3 \quad (1 = (-2) \cdot 4756 + 1359 \cdot 7) \qquad q = \left\lfloor \frac{3}{1} \right\rfloor = 3,\ r = 0$

$$\Rightarrow \quad 0 = 7 \cdot 4756 - 4756 \cdot 7$$

vergleiche Kettenbruchdarstellung: $$\frac{4756}{7} = 679 + \frac{1}{2 + \frac{1}{3}}$$

8. Literatur und weitere Informationen

- http://www.cryptool.com/
- Beutelspacher, Albrecht: „Kryptologie“, 2. Auflage, vieweg, Braunschweig, 1991.
- Beutelspacher, Albrecht: „Geheimsprachen“, 2. Auflage, C.H. Beck, München, 2000.

Anhang Primzahlkennzeichen (aus den Weiten des Internets)

Die Anzahl von Primzahlen in einem Bereich x lässt sich abschätzen nach: $P_z = \frac{x}{\ln x - 1.08366}$

Bereich	exakt	P_z
$10^0 – 10^1$ $10^1 – 10^2$ $10^2 – 10^3$ $10^3 – 10^4$ → $10^0 – 10^4$	4 21 143 1061 → 1229	8 20 143 1059 → 1230
$10^0 – 10^{45}$ 10^0 -10^{46} → $10^{45} – 10^{46}$		$9{,}75\ 10^{42}$ $9{,}54\ 10^{43}$ → $8{,}56\ 10^{43}$
10^{153} $1{,}34\ 10^{154} \approx 2^{512}$ → $10^{153} – 1{,}34\ 10^{154} \approx 2^{512}$		$2{,}85\ 10^{150}$ $3{,}79\ 10^{151}$ $3{,}5\ 10^{151}$

Wie kann man systematisch alle Primzahlen finden?

Das bekannteste Verfahren ist das *Sieb des Eratosthenes*, benannt nach dem griechischen Mathematiker Eratosthenes von Kyrene. Hier sein Vorschlag, um alle Primzahlen zu finden:

Schreibe die natürlichen Zahlen, beginnend mit 2, hintereinander hin: 2, 3, 4, 5, 6, 7, 8, 9, ... Streiche alle echten Vielfachen von 2, also 4, 6, ... 2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, 9, ... Streiche alle echten Vielfachen von 3, also 6, 9, ... (die 6 ist schon in der ersten Runde ausgeschieden): 2, 3, 4, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~, 11, ~~12~~, ... Und so weiter: Als nächstes werden die Vielfachen von 5 gestrichen, dann die von 7 usw. Genauer: Im k-ten Durchgang streiche die Vielfachen der k-ten Zahl, die bis dahin noch ,,überlebt" hat; das ist dann die k-te Primzahl.
Die Begründung für den Erfolg des Verfahrens ist leicht: Jede Nicht-Primzahl n hat einen echten Primteiler p, und damit wird n bei der zu p gehörigen Streichungsrunde gestrichen.

Primzahltests

Es ist für eine große Zahl m auch mit Computerhilfe sehr mühsam, die Primzahleigenschaft festzustellen. Eigentlich sind *alle* Zahlen n, die kleiner als m sind, zu testen: Teilt n die Zahl m? Man kann sich aber schnell klar machen, dass man nur Zahlen bis zur Wurzel von m testen muss, denn ist n ein Teiler von m, so ist eine der Zahlen n oder m/n höchstens so groß wie die Wurzel. Das kann immer noch eine Menge sein. Hat zum Beispiel m 100 Stellen im Dezimalsystem, so hat die Wurzel 50 Stellen. Könnte ein Computer pro Sekunde eine Million Zahlen testen (lässt sich m durch n teilen?), so hätte er immer noch mehr Jahre zu tun, als das Weltall voraussichtlich bestehen wird. Es gibt aber bessere Tests, hier der bekannteste:

Ausgangspunkt des Tests ist ein Ergebnis, das schon von Fermat gefunden wurde. Es setzt voraus, dass man weiß, was für zwei Zahlen a und b die Zahl ,,a modulo b'' bedeutet: Damit ist die Zahl gemeint, die beim Teilen von a durch b als Rest übrig bleibt. (Zum Beispiel ist 15 modulo 2 gleich 1, und 139 modulo 4 ist gleich 3.). Fermat konnte nun zeigen: Startet man mit einer Primzahl p und einer Zahl a, die zwischen 1 und p-1 liegt und rechnet man dann a hoch p-1 aus, so gilt: Diese Zahl modulo p ist gleich 1. Hier ein Test für p = 5 und a = 3. Es ist 3 hoch 4 gleich 81, und wenn man 81 modulo 5 rechnet, kommt wirklich 1 heraus. Und warum ist das ein Primzahltest? Soll man m auf Primzahleigenschaft testen, so wähle man ein a kleiner m und prüfe, ob a^{m-1}(modulo m) = 1 ist. Kommt etwas von 1 Verschiedenes heraus, war m bestimmt keine Primzahl, obwohl damit noch lange kein Teiler bekannt ist. Es ist nun so, dass man üblicherweise mit diesem Test sehr schnell herausfinden kann, ob eine Zahl eine Primzahl ist oder nicht. Es gibt einige Ausnahmezahlen, die so genannten *Carmichael-Zahlen*, bei denen der Test versagt: Der Test ergibt immer 1, obwohl es sich *nicht* um eine Primzahl handelt. Das kleinste Beispiel ist die Zahl 561. Seit 1992 weiß man, dass es unendlich viele derartige ,,Versager'' gibt, sie sind aber sehr dünn gesät. Glücklicherweise gibt es – leider aber etwas komplizierter zu beschreibende - Tests, die immer anwendbar sind.

Einige besondere Primzahlen

Für Zahlen besonders einfacher Bauart gibt es Tests, die viel wirkungsvoller sind, damit können dann viel größere Kandidaten untersucht werden als mit den üblichen Verfahren.
Berühmtes Beispiel dafür sind die *Mersenne-Primzahlen*, das sind Primzahlen der Form „2^r – 1“. So sind zum Beispiel 7 und 31 Mersenne-Primzahlen. 2^r - 1 ist allerdings nicht für jedes r eine Primzahl; setzt man etwa r = 4, so kommt als 2^4 - 1 die Zahl 15 heraus, und die ist sicher nicht prim. Ob es für ein großes r klappt, kann man mit Computerhilfe relativ schnell ermitteln. Daher ist es kein Wunder, dass alle Primzahlrekorde der letzten Zeit von Mersenne-Primzahlen aufgestellt wurden. Bemerkenswert sind auch Primzahlen der Form 2^r+1, man nennt sie *Fermat-Primzahlen*. Einfache Beispiele sind 5 und 17, es ist unbekannt, ob es unendlich viele Beispiele gibt. Die sind für die Geometrie wichtig: Man kann ein gleichseitiges n-Eck genau dann mit Zirkel und Lineal konstruieren, wenn n ein Produkt von verschiedenen Fermat-Primzahlen - und möglicherweise noch einer Zweierpotenz - ist. Ein 17-Eck kann man also konstruieren, ebenso ein 80-Eck (denn 80 = 5· 2^4), ein 7-Eck aber nicht.