Zwei inverse Funktionen (siehe Skript S. 11.3/63)

In der Kryptographie wird eine Funktion zum Verschlüsseln und eine zum Entschlüsseln verwendet. Bei symmetrischen Verfahren wird zum Ver- und Entschlüsseln dieselbe Funktion verwendet. Bei asymmetrischen Verfahren wird eine Funktion f zum Verschlüsseln eine Funktion f' zum Entschlüsseln verwendet. Eine Möglichkeit ist es, f' als f^{-1} zu wählen. Dies wird beim RSA-Algorithmus gemacht.

Mit Hilfe des erweiterten Euklidischen Algorithmus und den Theoremen von Fermat und Euler kann unter bestimmten Voraussetzungen die inverse Funktion f^{-1} einfach berechnet werden.

Zwei inverse Funktionen sind E(x) und D(x), die im folgenden definiert werden.

Seien p und q zwei Primzahlen und seinen *d* und *e* zwei positive Zahlen, die für $k \in N$ die Gleichung

$$\mathbf{d \cdot e = 1 + k(p-1)(q-1)}$$

erfüllen.

Dann sind die beiden Funktionen invers:

$$\mathbf{E(x) = x^e \mod pq,\ 1 \le x \le pq - 1}$$

$$\mathbf{D(x) = x^d \mod pq,\ 1 \le x \le pq - 1}$$

$E(x) = x^e \mod pq, \quad 1 \le x \le pq - 1$

$D(x) = x^d \mod pq, \quad 1 \le x \le pq - 1$

Beweis:

$$\begin{aligned} E(D(x)) &= E(x^d \bmod pq) \\ &= \left(x^d \bmod pq\right)^e \bmod pq \\ &= \left(x^d\right)^e \bmod pq \\ &= x^{de} \bmod pq \\ &= x^{1+k(p-1)(q-1)} \bmod pq \\ &= x^1 \end{aligned}$$

Jeder, der den Exponenten e und das Produkt pq kennt, kann einen Text x verschlüsseln; e heißt öffentlicher Schlüssel.

Nur, wer den Exponenten d und das Produkt pq kennt, kann aus der Nachricht y = D(x) den Text x wieder entschlüsseln; d heißt privater Schlüssel.

Für große p, q, e, d ist es schwierig, aus dem Produkt pq und e den Faktor d, also den privaten Schlüssel, zu ermitteln.

Die Zahlen d und e werden durch die Definition

$$\mathbf{d \cdot e = 1 + k(p-1)(q-1)}$$

gerade so gewählt, dass das Eulersche Theorem erfüllt ist. Dividiert man das Produkt d · e durch n = (p-1)(q-1), so bleibt als Rest 1, d.h. $\mathbf{d \cdot e \equiv 1 \pmod{n}}$.

Spalte 2 der Tabelle zeigt solche Produkte (Skript S. 11.3/59):

k	1 + 24k	Faktorisierung von 1 + 24k
0	1	1
1	25	52
2	49	72
3	73	731
4	97	971
5	121	112
6	145	5 · 29
7	169	13 · 13
8	193	193

Damit ist d das multiplikative Inverse von e (mod n). Wir erinnern uns, dass der erweiterte euklidische Algorithmus das multiplikative Inverse x von a (mod b) berechnet:

$$\mathbf{gcd(a, b) = (1, x, y)}$$

Wir wählen ein a = e und b = n, so dass e und n relativ prim.

Dann folgt: $\mathbf{gcd(e, n) = (1, d, y)}$

Der Algorithmus liefert **d** als multiplikatives Inverses zu **e**.