Zahlentheorie

Marvin Baeumer **2023-12-06 10:23**

Grundlagen - Rechenregeln

$$\begin{aligned} a_1 &\equiv b_1 \mod m \\ a_2 &\equiv b_2 \mod m \\ \implies a_1 + a_2 &\equiv b_1 + b_2 \mod m \end{aligned}$$

"Wir duerfen zwei Kongruenzen modulo m addieren"

$$\begin{aligned} a_1 &\equiv b_1 \mod m \\ \implies a_1 \cdot c &\equiv b_2 \cdot c \mod m \end{aligned}$$

"Wir duerfen beide Seiten einer Kongruenz mit der gleichen ganzen Zahl multiplizieren"

$$\begin{aligned} a_1 &\equiv b_1 \mod m \\ a_2 &\equiv b_2 \mod m \\ \implies a_1 \cdot a_2 &\equiv b_1 \cdot b_2 \mod m \end{aligned}$$

"Wir duerfen zwei Kongruenzen Modulo m multiplizieren"

Pruefzifferverfahren

RSA-Verfahren

Vorgehen

- Waehlen zweier Primzahlen p und q
- Berechnung von n mit $p \cdot q$
- Berechnung von $\varphi(n)$ mit $(p-1) \cdot (q-1)$
- Waehlen von $e \rightarrow$ teilerfremd zu $\varphi(n)$ und $1 < e < \varphi(n)$
- Berechnung von d mit erweiterter euklidischer algorythmus mit $\varphi(n)$ und e
    - fuer d gillt $e \cdot d \equiv 1 \mod \varphi(n)$
- Bilden des Public Key (n, e)
- Bilden des Private Key (n, d)
- Eine Nachricht m verschluesseln mit $m^e \mod n$
- Die verschluesselte Nachricht c entschluesseln mit $c^d \mod n$

Beispiel

$$\begin{array}{ccccccccccc}
p & = & 19, & q & = & 23 & & & & & \\
n & = & p & \cdot & q & \Leftrightarrow & 19 & \cdot & 23 & = & 437 \\
\varphi(n) & = & (p-1) & \cdot & (q-1) & \Leftrightarrow & 18 & \cdot & 22 & = & 396 \\
e & = & 23 & & & & & & & & \\
d & = & ? & & & & & & & &
\end{array}$$

Berechnung von d

Euklidischer Algorytmus

$$\begin{array}{ccccccccc}
 & \varphi(n) & = & e & \cdot & n & + & r \\
\Leftrightarrow & 396 & = & 23 & \cdot & 17 & + & 5 \\
 & 23 & = & 5 & \cdot & 4 & + & 3 \\
 & 5 & = & 3 & \cdot & 1 & + & 2 \\
 & 3 & = & 2 & \cdot & 1 & + & 1 \\
 & 2 & = & 1 & \cdot & 2 & + & 0
\end{array}$$

Umstellen nach Rest

$$\begin{array}{ccccccc}
5 & = & 396 & - & 23 & \cdot & 17 \\
3 & = & 23 & - & 5 & \cdot & 4 \\
2 & = & 5 & - & 3 & \cdot & 1 \\
1 & = & 3 & - & 2 & \cdot & 1
\end{array}$$

Erweiterter Euklidischer Algorithms

$$
\begin{array}{rcccccccccccccc}
 & 1 & = & 3 & - & 2 & \cdot & 1 & & & & & & & \\
\Leftrightarrow & 1 & = & 3 & - & 1 & \cdot & (5 & - & 1 & \cdot & 3) & & & \\
 & 1 & = & 3 & - & 1 & \cdot & 5 & + & 3 & & & & & \\
 & 1 & = & & - & 5 & + & 2 & \cdot & 3 & & & & & \\
\Leftrightarrow & 1 & = & & - & 5 & + & 2 & \cdot & (23 & - & 4 & \cdot & 5) & \\
 & 1 & = & & - & 5 & + & 2 & \cdot & 23 & - & 8 & \cdot & 5 & \\
 & 1 & = & & - & 9 & \cdot & 5 & + & 2 & \cdot & 23 & & & \\
\Leftrightarrow & 1 & = & & - & 9 & \cdot & (396 & - & 17 & \cdot & 23) & + & 2 & \cdot 23 \\
 & 1 & = & & - & 9 & \cdot & 396 & + & 153 & \cdot & 23 & + & 2 & \cdot 23 \\
final\ form & 1 & = & & - & 9 & \cdot & 396 & + & 155 & \cdot & 23 & & &
\end{array}
$$

Nach d aufloesen

$$
\begin{array}{cccccccccccl}
- & 9 & \cdot & 396 & + & 155 & \cdot & 23 & \equiv & 1 & \bmod & 396 \mid -9\cdot 396 \text{ faellt weg} \\
 & & & & & 155 & \cdot & 23 & \equiv & 1 & \bmod & 396 \mid 23 = e
\end{array}
$$

$$d \rightarrow 155 \quad e \rightarrow 23$$

Ver- und entschluesselung

Public Key $(437, 23)$

Private Key $(437, 155)$

$Verschluesselung: m^e \mod n \mid m = 420 = 420^{23} \mod 437 = 374$

$Entschluesselung: c^d \mod n \mid c = 374 = 374^{155} \mod 437 = 420$

[Zum Code]