1 Grundlagen

Allgemeines

$$x^k \bmod p \equiv (x \bmod p)^{k \bmod \varphi(p)} \bmod p$$

$$\gcd(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \bmod m$$

Berechnung der Stellenzahl

Die Anzahl a der Ziffern der b-adischen Darstellung einer natürlichen Zahl $n \in \mathbb{N}_0$ berechnet sich wie folgt:

$$a = \begin{cases} 1, & \text{wenn } n = 0, \\ \lfloor \log_b n \rfloor + 1, & \text{wenn } n \geq 1. \end{cases}$$

1.1 Phi-Funktion

Die Eulersche Phi-Funktion gibt an, wie viele ganze Zahlen teilefremd zu n sind.

1. $\varphi(\text{prime}) = \text{prime} - 1$
2. $\varphi(\text{prime}^k) = \text{prime}^{k-1} \cdot (\text{prime} - 1)$
3. $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Wobei p eine Primzahl ist welche n ganzzahlig teilt. (Primfaktoren)

1.2 Kontravalenz

$\oplus$	0	1
0	0	1
1	1	0

1.3 Diskreter Logarithmus

Der diskrete Logarithmus ist die kleinste Lösung für x der Gleichung $a^x \equiv m \bmod p$ mit $m,\ a \in \mathbb{N},\ p \in \mathbb{Z}_p$.

Da sich die diskrete Exponentiation leicht berechnen lässt, gilt das nicht für die Umkehrfunktion. *(Diffie-Hellman-Annahme)* Aufgrund dessen wird diese Ëinwegfunktionü. a. im Diffie-Hellman-Key-Exchange, der ElGamal-Encryption und vielem mehr eingesetzt. Jedoch ist diese Funktion ungeeignet für Verschlüsselungsmethoden, da es keine "Falltürßum entschlüssel gibt.

Ordnung einer Zahl ist der kleinste Exponent, so dass gilt:

$$x^n \bmod m \equiv 1$$

Dabei entspricht die Ordnung von x der Anzahl der Elementen welche einen Zyklus bilden. Wenn x eine Primzahl ist dann gilt: $\text{ord}(x) = x - 1$

$$\text{ord}(x^l) = \frac{\text{ord}(x)}{\gcd(\text{ord}(x), l)}$$

1.4 Modulares Potenzieren

Seien $x, k, m \in \mathbb{N}$, gesucht ist $z = x^k \mod m$

1. Binärdarstellung von k
2. Ersetzen jeder 0 durch **Q** und jeder 1 durch **QM**
3. Dabei wird **Q** als Anweisung zum *Quadrieren* und **M** als Anweisung zum *Multiplizieren* mit der Basis x aufgefasst.
4. Begonnen wird mit 1 bzw. kann die erste **QM** Anweisung durch x substituiert werden.

1.5 Chinesischer Restsatz

Seien $m_1, \ldots, m_n \in \mathbb{N}$ paarweise teilerfremd, dann hat das System von Kongruenzen eine eindeutige Lösung $x \in \mathbb{Z}_m$, wobei $m = m_1 \cdot \ldots \cdot m_n$ das Produkt der einzelnen Module ist.

$$x \equiv a_1 \bmod m_1,\ \ldots, x \equiv a_n \bmod m_n$$

Eine Lösung x kann wie folgt ermittelt werden:

$$x = \left(\sum_{i=1}^{n} a_i \cdot M_i \cdot N_i\right) \bmod m$$

mit folgenden Vorraussetztungen:

$$\begin{aligned} m &= m = m_1 \cdot \ldots \cdot m_n \\ M_i &= \tfrac{m}{m_i} \\ N_i &= M_i^{-1} \bmod m_i \end{aligned}$$

1.6 Euklidischer Algorithmus

Setze $r_0 := a, r_1 := b$

$$\begin{aligned} r_0 &= q_2 \cdot r_1 + r_2 \\ r_1 &= q_3 \cdot r_2 + r_3 \\ &\vdots \\ r_{n-2} &= q_n \cdot r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} \cdot r_n + 0 \end{aligned}$$

$x_0 := 1,\ x_1 := 0,\ y_0 := 0,\ y_1 := 1$

$$\begin{aligned} x_2 &= x_0 - q_2 \cdot x_1 & y_2 &= y_0 - q_2 \cdot y_1 \\ x_3 &= x_1 - q_3 \cdot x_2 & y_3 &= y_1 - q_3 \cdot y_2 \\ x_n &= x_{n-2} - q_n \cdot x_{n-1} & y_n &= y_{n-2} - q_n \cdot y_{n-1} \end{aligned}$$

$$\begin{aligned} x_2 &= x_0 - q_2 \cdot x_1 \\ x_3 &= x_1 - q_3 \cdot x_2 \\ x_n &= x_{n-2} - q_n \cdot x_{n-1} \end{aligned}$$

$$\begin{aligned} x_2 &= x_0 - q_2 \cdot x_1 \\ x_3 &= x_1 - q_3 \cdot x_2 \\ x_n &= x_{n-2} - q_n \cdot x_{n-1} \end{aligned}$$

dann gilt $x_n a + y_n b = \gcd(a, b)$.

1.7 Primitivwurzeln

Hat die Ordnung einer Zahl x modulo m den gro ßtmo glichen Wert, also ord

Primitivwurzeltest Um festzustellen, ob eine Zahl g eine Primitivwurzel in der Restklassengruppe $\mathbb{Z}_p^*$ mit p ist Primzahl ist, führe man folgende Schritte aus:

1. Primfaktorzerlegung von $p - 1$: $p - 1 = p_1 \cdot \ldots \cdot p_i$
2. Prüfe für alle $q \in \{p_1,\ \ldots, p_i\}$ ob gilt $g^{(p-1)/q} \not\equiv 1 \bmod p$
   Sollten demnach alle Primfaktoren ungleich 1 mod p sein, dann ist g eine Primitivwurzel.

Falls g eine Primitivwurzel von $\mathbb{Z}_n^*$ ist, dann ist auch $a = x^t$ eine Primitivwurzel von $\mathbb{Z}_n^*$ genau dann wenn gilt: $\gcd(t, \varphi(n)) = 1$.

1.8 Miller-Rabin

2 Verschlüsselungsalgorithmen

2.1 Asymetrische Verfahren

2.2 Symmetrische Verfahren

2.3 Blockverschlüsselung