RSA-Verfahren: Eine mathematische Erklärung

Joris R. Parthier

12.4.2024

1 Grundlagen und Modulare Inverse

Die modulare Arithmetik ist ein Schlüsselkomponente im Verständnis des RSA-Verfahrens. Betrachten wir ein einfaches Beispiel: $2 \times 3 = 1 \pmod 5$ und $2 \times 3 = 1$ in $\mathbb{Z}_5$. In $\mathbb{R}$ wäre $2^{-1} = \frac{1}{2}$, aber in $\mathbb{Z}_5$ ist $2^{-1} = 3$, da $2 \times 3 = 6 \equiv 1 \pmod 5$.

Dies zeigt, dass es eine Inverse gibt, weil 2 und 5 teilerfremd sind, was durch den euklidischen Algorithmus bestimmbar ist.

2 Erzeugung eines RSA-Schlüsselpaares

1. Wähle zwei große Primzahlen p und q.
2. Berechne $n = p \times q$ und $\phi(n) = (p-1)(q-1)$, wobei ϕ die Eulersche Phi-Funktion ist, die die Anzahl der Zahlen von 1 bis n zählt, die teilerfremd zu n sind.
3. Wähle $e \in \mathbb{N}$ mit $\gcd(e, \phi(n)) = 1$.
4. Bestimme d so, dass $e \times d \equiv 1 \pmod{\phi(n)}$.

Das private Schlüsselpaar ist (d, n), das öffentliche Schlüsselpaar ist (e, n).

3 Verschlüsselung und Entschlüsselung

Zum Verschlüsseln einer Nachricht m, berechne $c \equiv m^e \pmod{n}$. Zum Entschlüsseln von c, berechne $m \equiv c^d \pmod{n}$. Die Begründung hierfür ist, dass $c^d = (m^e)^d = m^{e \times d} = m^{k \times \phi(n)+1} \equiv m \pmod{n}$.