Das RSA-Verfahren

Das RSA-Verfahren wurde 1977 von Rivest, Shamir und Adleman zur Verschlüsselung von Nachrichten erfunden und beruht zu großen Teilen auf dem Satz von Fermat. Seine Sicherheit resultiert aus dem Umstand, dass eine sehr große Zahl aus zwei Primfaktoren relativ leicht gebildet, aber sehr schlecht wieder faktorisiert werden kann.

Wir nehmen der Einfachheit halber an, die zu verschlüsselnde Nachricht sei eine natürliche Zahl zwischen 0 und $M \in \mathbb{N}$.

Empfänger:

- Wählt $p, q \in \mathbb{P}$, $p \neq q$, möglichst groß (in der Regel mit mehreren hundert Stellen), so dass $pq =: n > M$.
- Wählt $e, d \in \mathbb{N}$, so dass $\text{ggT}(e, \varphi(n)) = 1$, $e \neq d$ und

$$ed \equiv 1 \pmod{\varphi(n)} \quad \Leftrightarrow \quad \exists k \in \mathbb{Z} : ed = k\varphi(n) + 1.$$

- Besitzt nun zwei Schlüssel:

$$\begin{array}{ll} \boxed{(e, n)} & \text{(öffentlicher Schlüssel)} \\ \boxed{(d, n)} & \text{(privater Schlüssel)} \end{array}$$

- Teilt dem Sender (öffentlich) den öffentlichen Schlüssel (e, n) mit.

Sender:

- Bestimmt Zahl $\tilde{m} \in \{0, \dots, n-1\}$, so dass

$$\boxed{\tilde{m} \equiv m^e \pmod{n}}$$

(wobei $m \in \{0, \dots, M\}$ die zu verschlüsselnde Nachricht ist).

- Teilt dem Empfänger (öffentlich) die verschlüsselte Nachricht $\tilde{m}$ mit.

Empfänger:

- Bestimmt $m \in \{0, \dots, M\}$ mit

$$\boxed{m \equiv \tilde{m}^d \pmod{n}}$$

Dies gilt, da

$$\tilde{m}^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{k\varphi(n)+1} \equiv (m^{\varphi(n)})^k m \stackrel{\text{Fermat}}{\equiv} 1^k m \equiv m \pmod{n}.$$

Da $e, n, \tilde{m}$ öffentlich sind, würde einem Dritten die Kenntnis von d genügen, um die Nachricht zu entschlüsseln.

Aber d kann nur ermittelt werden, wenn man $\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$ kennt. Dies wiederum würde allerdings bedeuten, dass man die Primfaktorzerlegung von $n = pq$ kennen müsste, was, wie oben erwähnt, recht schwierig ist.