Mathematische Begründung des RSA-Verfahrens *www.r-krell.de* (März 2017)

Nach dem Lemma von Bézout gibt es für je zwei natürliche Zahlen a und b immer auch zwei ganze Zahlen s und t, sodass $s{\cdot}a + t{\cdot}b = ggT(a,b)$ ist. Diese Darstellung ist nicht eindeutig, wie das Beispiel $ggT(6, 10) = 2 = 2{\cdot}6 + (-1){\cdot}10 = (-3){\cdot}6 + 2{\cdot}10$ zeigt.

Folgerung: Weil ggT(e, phi) = 1 ist (e wurde extra so gewählt, dass diese Eigenschaft gilt), gibt es also $s, t \in \mathbb{Z}$ mit $s{\cdot}e + t{\cdot}phi = 1$ bzw. mit $s{\cdot}e = 1 - t{\cdot}phi$. Auch hier sind unendlich viele Lösungen möglich. Insbesondere könnte das zuerst gefundene s negativ sein. In diesem Fall addiert man auf beiden Seiten der Gleichung $s{\cdot}e = 1 - t{\cdot}phi$ den Term $| + u{\cdot}e{\cdot}phi$ mit ausreichend großem $u \in \mathbb{N}$ und erhält $s{\cdot}e + u{\cdot}e{\cdot}phi = 1 - t{\cdot}phi + u{\cdot}e{\cdot}phi$ bzw. $(s + u{\cdot}phi){\cdot}e = 1 + (u{\cdot}e - t){\cdot}phi$.
Benennt man jetzt die Klammern noch mit $d := s + u{\cdot}phi$ und $v := u{\cdot}e - t$, so ist klar, dass man ein positives d mit $d{\cdot}e = 1 + v{\cdot}phi$ erhalten kann. Dabei könnten d und v sogar beide positiv, also natürliche Zahlen sein. Wichtig ist vor allem, dass d natürlich ist. Dieses d bzw. ein solches (möglichst kleines, aber positives) d wird (zusammen mit n) als privater Schlüssel beim RSA-Verfahrens verwendet!

Der Satz von Euler/Fermat besagt: Sei z eine natürliche Zahl und $\varphi(z)$ der Wert der Eulerfunktion an der Stelle z, nämlich die Anzahl aller natürlicher Zahlen zwischen 1 und z–1, die (außer 1) keine gemeinsamen Teiler mit z haben. Dann gilt für jede natürliche Zahl a, die teilerfremd zu z ist (also mit ggT(a,z)=1) die Gleichung

$$a^{\varphi(z)} \bmod z = a^{\varphi(z)} \,\%\, z = 1$$

d.h. die Potenz $a^{\varphi(z)}$ liefert für jede zu z teilerfremde Basis a nach der Division durch z immer den Rest 1

Für Primzahlen p, q liefert die Eulerfunktion $\varphi(p) = p-1$ und $\varphi(q) = q-1$, weil keine der kleineren Zahlen p und q gemeinsame Teiler mit einer Primzahl haben kann. Für Primzahlprodukte gilt außerdem immer $\varphi(p{\cdot}q) = (p-1){\cdot}(q-1)$.

Beispiel: $\varphi(z) = |\{i \in \mathbb{N} \mid 1 \le i \le z\text{-}1 \ \wedge$ i teilerfremd zu z, d.h. $ggT(i,z)=1\}|$, also $\varphi(3) = |\{1, 2\}| = 2$, $\varphi(6) = |\{1, ~~2, 3, 4,~~ 5\}| = |\{1, 5\}| = 2$ und $\varphi(3{\cdot}6) = \varphi(18) = |\{1, ~~2, 3, 4,~~ 5, ~~6,~~ 7, ~~8, 9, 10,~~ 11, ~~12,~~ 13, ~~14, 15, 16,~~ 17\}| = 6$, weil 6 Zahlen übrig bleiben, nachdem die Zahlen mit gemeinsamen Teilern gestrichen wurden. Bei der Primzahl 5 gilt hingegen $\varphi(5) = |\{1, 2, 3, 4\}| = 4$ und $\varphi(3{\cdot}5) = \varphi(15) = 8 = 2{\cdot}4 = |\{1, 2, ~~3,~~ 4, ~~5, 6,~~ 7, 8, ~~9, 10,~~ 11, ~~12,~~ 13, 14\}|$.

Folgerung: Da unser $phi = (p-1){\cdot}(q-1) = \varphi(p{\cdot}q) = \varphi(n)$ ist, gilt auch für jede Basis k (mit $k \neq p$, $k \neq q$) die Euler-Gleichung $k^{phi} \,\%\, n = k^{\varphi(n)} \,\%\, n = 1$, da k dann teilerfremd zu $p{\cdot}q$ ist. Für die RSA-Entschlüsselung bzw. die vom Empfänger berechnete Klarzahl k_E gilt außerdem $k_E = g^d \,\%\, n = (k^e \,\%\, n)^d \,\%\, n = (k^e)^d \,\%\, n = k^{e{\cdot}d} \,\%\, n$. In der Herleitung wurde neben den Rechenvorschriften für k_E und g noch $(a \,\%\, n){\cdot}(b \,\%\, n) \,\%\, n = a{\cdot}b \,\%\, n$ bzw. die entsprechende Gleichheit bei Potenzen benutzt.

Setzt man für $e{\cdot}d = 1 + v{\cdot}phi$ ein (wie oben dargestellt), so kann weiter umgeformt werden: $k_E = k^{e{\cdot}d} \,\%\, n = k^{1 + v{\cdot}phi} \,\%\, n = k \cdot k^{v{\cdot}phi} \,\%\, n = k \cdot (k^{phi})^v \,\%\, n = k \cdot (k^{phi} \,\%\, n)^v \,\%\, n = k{\cdot}1^v \,\%\, n = k{\cdot}1 \,\%\, n = k \,\%\, n = k$, wobei der letzte Schritt nur wegen $k < n$ gilt. Unter den gegebenen Voraussetzungen ist also $k_E = k$ und damit bewiesen, dass beim RSA-Verfahren der Empfänger mit seinem privaten Schlüssel (n, d) aus g genau die Klarzahl k heraus bekommt, die der Sender mit dem öffentlichen Schlüssel (n, e) zur übermittelten Geheimzahl g verschlüsselt hatte. ▣