mir nun eine Nachricht schicken will, soll sie zunächst in eine lange Zahlenreihe übersetzen, indem etwa der ASCII-Code verwendet wird. Daraus werden Blöcke gebildet, die – zum Beispiel – jeweils die Länge 50 haben.

Und nun kann das Verschlüsseln beginnen. Ist ein Block durch eine Zahl m dargestellt, so muss $m^k \bmod n$ ausgerechnet werden (das Ergebnis wollen wir r nennen). Das geht, da ja n und k bekannt sind. Man macht das für alle Blöcke und schickt mir die Ergebnisse (also die Zahlen r). Dabei kann jeder, der Lust hat, mitlesen.

Das Entschlüsseln geht dann so. Der Panzerschrank wird geöffnet, und mit den darin enthaltenen Informationen (also mit p, q und l) kann $r^l \bmod n$ berechnet werden. Nun ist $r^l = (m^k)^l = m^{kl}$, und $k \cdot l$ ist 1 modulo $\phi(n)$. Es gibt also eine ganze Zahl s, so dass $k \cdot l = s \cdot \phi(n) + 1$ gilt. Es folgt

$$\begin{aligned} r^l \bmod n &= m^{kl} \bmod n \\ &= m^{s\phi(n)+1} \bmod n \\ &= m \cdot (m^{\phi(n)})^s \bmod n. \end{aligned}$$

Aufgrund des Satzes von Euler ist aber $m^{\phi(n)}$ (und damit auch die s-te Potenz dieser Zahl) gleich 1 modulo n. Zusammen heißt das, dass

$$r^l \bmod n = m \bmod n = m;$$

dabei gilt das letzte Gleichheitzeichen, weil $m < n$ ist. Man kann also wirklich das m aus dem öffentlich übertragenen r rekonstruieren.

Aber dazu ist wirklich nur der in der Lage, der $\phi(n)$ kennt, also $(p-1)(q-1)$. Wer p und q aus n ermitteln könnte, hätte das Problem gelöst. Und das ist der Grund, warum der Frage der Faktorisierung so viel Aufmerksamkeit geschenkt wird[26].

Hier noch ein *konkretes Beispiel mit kleinen Zahlen* (die bei ernsthaften Anwendungen auftretenden sind viel größer). Wir haben uns zu $p = 47$ und $q = 59$ entschlossen, veröffentlicht wird dann $n = 47 \cdot 59 = 2773$. Dann sind noch k und l zu finden, unsere Wahl fällt auf $k = 17$ und $l = 157$. Da $\phi(n)$ gleich $46 \cdot 58 = 2668$ und da $17 \cdot 157 = 2669$ und damit gleich 1 modulo $\phi(n)$ ist, sind diese Zahlen wirklich geeignet. Die Zahlen 2773 und 17 werden allen mitgeteilt, aber 47, 59 und 157 sind streng geheim.

Nun soll verschlüsselt werden. Mal angenommen, jemand möchte mir die Zahl 1115 übermitteln. Er lässt seinen Computer die Zahl $1115^{17} \bmod 2773$ berechnen, das Ergebnis ist 1379. Das schreibt er auf eine Postkarte, am nächsten Tag finde ich sie im Briefkasten. Nun rechnet *mein* Computer $1379^{157} \bmod 2773$ aus. Sein Ergebnis liegt nach wenigen Millisekunden vor: 1115. Spione, die die Postkarte heimlich kopiert haben, hätten das aber nicht herausbekommen.

---

[26] Siehe zum Beispiel Beitrag 43.