Ludwig-Maximilans-
Universität München
Dr. Pascal Reisert

Wintersemester 2018/2019
Übungsblatt 6
21. November 2018

Übungen zur Kryptographie
Lösung

Aufgabe 24

Dieser Fall verläuft analog zu Aufgabe 17. Es gilt $p = \prod_i p_i$ und $q = \prod_j q_j$ für paarweise verschiedene Primzahlen p_i, q_j, also

$$\mathbb{Z}/N \simeq \prod_i \mathbb{Z}/p_i \times \prod_j \mathbb{Z}/q_j.$$

Wie zuvor erhalten wir $ed = 1 \bmod p-1,\ ed = 1 \bmod q-1$. Für Carmichael-Zahlen gilt weiter $p_i - 1 | p-1$ und $q_j - 1 | q-1$ also auch $ed = 1 \bmod p_i - 1,\ ed = 1 \bmod q_j - 1$ und somit $x^{ed} = x$ in $\prod_i \mathbb{Z}/p_i \times \prod_j \mathbb{Z}/q_j$. Carmichael-Zahlen haben allerdings den Nachteil, dass sie aus mindestens drei Primfaktoren zusammengesetzt sind, so dass die Faktorisierung von N einfacher wird und die Verschlüsselung damit weniger sicher ist.

Bemerkung. Die Teilerfremdheit ist notwendig, denn z.B. für $p = 561$ und $q = 1105$ und $\gcd(p, q) = 17 = 2 \cdot 561 - 1105$ ist $\varphi(N) = 2 \cdot 4 \cdot 10 \cdot 12 \cdot 16 \cdot 17 = 261120$. Sei $e = 11$ und damit $d = 168611$ mit $ed = 1 \bmod (p-1)(q-1)$ sowie $x = (2, 2) = 34$. Dann ist $ed = 6818955$ und $x^{ed} \bmod N = 39304 \neq 34$.