Mathe Hausaufgaben zum 13. Januar 2017

Elaha Khaleqi(6947801), Matz Radloff(6946325)

12. Januar 2017

4.

Nachricht: 5 Öffentlicher Schlüssel: $(11, 247)$ Privater Schlüssel: $(59, 247)$

$$\begin{aligned} M &= 5 \\ 5^{11} &= 48828125 = 197684 \cdot 247 + 177 \\ \Rightarrow C &= 177 \equiv 5^{11} (\text{mod } 247) \end{aligned}$$

Die verschlüsselte Nachricht lautet $C = 177$. Entschlüsselung zur Probe:

$$\begin{aligned} 177^{59} &= 4.269949270145140822682063612888 9... \cdot 10^{132} \\ &= 1.728724400868478065863183648942 9... \cdot 10^{130} \cdot 247 + 5 \\ \Rightarrow M' &= M = 5 \end{aligned}$$

5.

(a)

$$\begin{aligned} p = 7, q = 11, N &= 77 \\ \varphi(N) = (p-1)(q-1) &= 60 \\ e &= 13 \\ d &= \frac{r \cdot \varphi(N) + 1}{e} \end{aligned}$$

Für ein großes $r = 4615384297$ ergibt sich $d = 999999931$.

Der private Schlüssel lautet also $(999999931, 60)$ und der öffentliche öffentliche $(13, 60)$. Die Zahlen wurden so gewählt, damit Nachrichten schnell verschlüsselt werden können, aber beim Entschlüsseln von einem möglichen Angreifer, d nicht durch einfaches Ausprobieren erraten werden kann (In praktischen Anwendungsfällen sollten die Zahlen natürlich trotzdem deutlich größer gewählt werden).

(b)