Wolfgang K. Seiler
*Tel.* 2515

B6, B4.18

*14. Oktober 2019*

# 6. Übungsblatt Kryptologie

**Aufgabe 1:** *(9 Punkte)*

Der private Schlüssel $d$ zum öffentlichen RSA-Schlüssel $(N, e)$ wird über den erweiterten Euklidischen Algorithmus so bestimmt, daß $de - k\varphi(N) = 1$ ist, wobei $N = pq$ ist und $\varphi(N) = (p-1)(q-1)$.

*a)* Angenommen, Sie kennen $e$ und $d$. Wie können Sie dann $\varphi(N)$ bestimmen?

*b)* Wie lassen sich die beiden Primzahlen $p$ und $q$ aus $N$ und $\varphi(N)$ bestimmen?

*c)* Für den RSA-Schlüssel $(N, e) = (13\,342\,081,\ 7)$ führt obige Vorgehensweise auf den privaten Exponenten $d = 3\,809\,847$. Was ist $\varphi(N)$ ?

*d)* Bestimmen Sie, ohne $N$ zu faktorisieren, die privaten Exponenten für die RSA-Schlüssel $(N, 3)$ und $(N, 5)$ !

*e)* Berechnen Sie $p$ und $q$ sowie das kleinste gemeinsame Vielfache $\lambda$ von $p-1$ und $q-1$ !

*f)* Auf welchen privaten Exponenten für $(N, 7)$ kommt man, wenn man den erweiterten Euklidischen Algorithmus auf $e$ und $\lambda$ anwendet? Würden *c)* bis *e)* einfacher oder schwieriger, wenn man von $(N, 7)$ und dem so berechneten $d$ ausgeht?

**Aufgabe 2:** *(8 Punkte)*

*a)* Schreiben Sie

$$x = 1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{5}}}}$$

als gewöhnlichen Bruch!

*b)* Berechnen Sie die Kettenbruchentwicklung von $\sqrt{15}$ !

*c)* Welche Zahl wird durch den periodischen Kettenbruch

$$y = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}}$$

dargestellt? *(Hinweis: Betrachten Sie* $z = 1 + 1/y$*.)*

**Aufgabe 3:** *(3 Punkte)*

Finden Sie einen Bruch mit höchstens zweistelligem Nenner, der den Bruch $\dfrac{13579}{24680}$ mit einem Fehler von höchstens einem Tausendstel approximiert!

**Abgabe** bis zum Freitag, dem 18. Oktober 2019, um 11.55 Uhr