FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2025/26
05.11.2025

Musterlösung zum 6. Übungsblatt zur Vorlesung Kryptologie

Übung 1

48 ist Zeuge:

$$48^{324} = 66 \bmod 325.$$

49 ist kein Zeuge:

$$49^{324} = 1 \bmod 325,$$
$$49^{162} = 1 \bmod 325,$$
$$49^{81} = 324 = -1 \bmod 325.$$

51 ist Zeuge:

$$51^{324} = 1 \bmod 325,$$
$$51^{162} = 1 \bmod 325,$$
$$51^{81} = 51 \bmod 325.$$

57 ist kein Zeuge:

$$57^{324} = 1 \bmod 325,$$
$$57^{162} = 324 = -1 \bmod 325.$$

68 ist Zeuge:

$$68^{324} = 1 \bmod 325,$$
$$68^{162} = 274 \bmod 325.$$

126 ist kein Zeuge:

$$126^{324} = 1 \bmod 325,$$
$$126^{162} = 1 \bmod 325,$$
$$126^{81} = 1 \bmod 325.$$

Bei der alternativen Prüfung zerlegt man

$$325 - 1 \;=\; 324 \;=\; 2^2 \cdot 81.$$

Man muss also a^{81} und $a^{2\cdot 81}$ betrachten.

Man beginnt bei a^{81} und testet zunächst auf $\pm 1 \bmod 325$. Dies ist bei $a = 126$ und $a = 49$ der Fall, so dass diese keine Zeugen sind.

Falls $a^{81} \neq \pm 1 \bmod 325$ quadriert man, d.h., man berechnet $(a^{81})^2 = a^{162}$. Erhält man eine -1, so hat man keinen Zeugen. Dies ist bei $a = 57$ der Fall.

In allen anderen Fällen hat man Zeugen.

Übung 2

Es ist (alles jeweils $\bmod n$)

$$(n-1)^k \;=\; (-1)^k \;=\; 1, \quad \text{solange } k \text{ gerade ist.}$$

Im Algorithmus wird k so lange halbiert bis k ungerade ist. Dann ist $(n-1)^k = (-1)^k = -1$, und der Algorithmus stoppt, ohne dass ein Widerspruch zur (möglichen) Primalität von n aufgetreten ist, d.h. $n-1$ ist kein Zeuge.

Bei der alternativen Prüfung beginnt man direkt mit $(n-1)^r$ mit ungeradem r und erhält -1, ohne Widerspruch zur (möglichen) Primalität von n, d.h. $n-1$ ist kein Zeuge.

Übung 3

Entscheidet man nach dem Miller-Rabin Test mit n Ziehungen fälschlich für eine Primzahl, so hat man n mal einen nicht-Zeugen gezogen. Die Wahrscheinlichkeit für einen nicht-Zeugen ist $\frac{1}{4}$, die Wahrscheinlichkeit, dies n-mal hintereinander zu tun, ist $\left(\frac{1}{4}\right)^n$. Also gilt:

$$\begin{aligned} &\text{Wahrscheinlichkeit}(\text{Fehlentscheidung}) = \left(\frac{1}{4}\right)^n < 10^{-100} \\ \Leftrightarrow \quad & n \;>\; \log_{\frac{1}{4}} 10^{-100} \;=\; -100 \cdot \log_{\frac{1}{4}} 10 \;\approx\; 166. \end{aligned}$$

Übung 4

Die Primzahlen sind nicht gleichverteilt. Da die Wahrscheinlichkeit, Zahlen aus einer großen Lücke zu ziehen, größer ist, als aus einer kleinen Lücke, ist der Abstand zur nächsten Primzahl im Durchnitt größer als $\frac{\ln n}{2}$.