FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2024/25
06.11.2024

# 6. Übungsblatt zur Vorlesung Kryptologie

## Übung 1

Sind 48, 49, 51, 57, 68 bzw. 126 nach dem Miller-Rabin-Test Zeugen für die Zusammengesetztheit von 325?

## Übung 2

Zeigen Sie: Beim Miller-Rabin Test zur Überprüfung der Zusammengesetztheit von $n$ ist $a = n - 1$ nie ein Zeuge.

## Übung 3

Man kann zeigen, dass bei $n$ nicht prim mindestens $3/4$ aller $a \in \mathbb{Z}_n$ Zeugen dafür nach dem Miller-Rabin Test sind.

Wieviel Ziehungen müssen Sie ungefähr beim Miller-Rabin Test durchführen, damit die Wahrscheinlichkeit, eine Fehlentscheidung zu treffen, kleiner ist als $10^{-100}$?

(Falls Sie auf diese Weise jedem der $10^{78}$ Atome im Universum eine (große) Primzahl zuordnen würden, wäre die Wahrscheinlichkeit, dass dabei ein Fehler passiert, kleiner als $10^{-22}$.)

## Übung 4

Man kann zeigen, dass es ungefähr $\frac{n}{\ln n}$ viele Primzahlen kleiner als $n$ gibt, d.h. durchschnittlich ist jede $\ln n$-te Zahl eine Primzahl.

Daraus könnte man schließen: Wählt man zufällig eine Zahl zwischen 1 und $n$, so ist der Abstand zur nächstgrößeren Primzahl im Durchschnitt ungefähr $\frac{\ln n}{2}$.

Vergleichen Sie diese Aussage mit den Ergebnissen der Aufgabe 4 vom Praktikum 2. Dort werden Sie feststellen, dass der Abstand tatsächlich größer ist. Wo liegt der Fehlschluss?