FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik
Prof. Georg Hoever

WS 2023/24
zu bearbeiten bis
29.11.23

Praktikum 2
zur Vorlesung Kryptologie

Bauen Sie Ihre Praktikumslösung modular auf! Überlegen Sie sich zunächst, wie ein sinnvoller Aufbau aussieht!

1. Implementieren Sie den Miller-Rabin-Test:
   - Eingabewerte: Eine Zahl n und eine Versuchsanzahl it.
   - Rückgabewert: 0, falls n wahrscheinlich prim ist, d.h., dass bei it zufälligen Ziehungen kein Zeuge für die Zusammengesetztheit gefunden wurde, 1 sonst.
2. Schreiben Sie eine Funktion, die zu einer Zahl die nächst größere Primzahl berechnet:
   - Eingabewerte: Eine Zahl n und eine Versuchsanzahl it.
   - Rückgabewert: Die kleinste Primzahl $\geq n$ nach dem Miller-Rabin-Test mit Versuchsanzahl it.

   Testwerte: 1. $n = 17$, $it = 5$, 2. $n = 32$, $it = 5$, 3. $n = 10^{100}$, $it = 10$.
   Bei $n = 10^{100}$ ist das Ergebnis $10^{100} + 267$.
3. Schreiben Sie eine Funktion, die zu einer Zahl die Anzahl der Zeugen für die Zusammengesetztheit berechnet:
   - Eingabewerte: Eine Zahl n.
   - Rückgabewert: Die Anzahl der Zahlen $a \in \{1, \ldots, n-1\}$, die Zeuge für die Zusammengesetztheit von n sind.

   Testwerte: 1. $n = 9$, 2. $n = 325$.
   Bei $n = 9$ ist das Ergebnis 6, bei 325 ist es 306.
4. Schreiben Sie eine Funktion, die berechnet, wie weit im Mittel die nächste Primzahl von einer zufällig gewählten Zahl einer bestimmten Größenordnung entfernt ist:
   - Eingabewerte: Zwei natürliche Zahlen anz und n und eine Versuchsanzahl it.
   - Ablauf: Es wird anz-oft eine Zahl m zwischen 0 und n zufällig gezogen und die nächstgrößere Primzahl p_m (wie in 2.) bestimmt.
   - Rückgabewert: Mittelwert der Differenzen $p_m - m$.
5. Experimentieren Sie mit der Funktion aus 4. und stellen Sie eine Vermutung für einen funktionalen Zusammenhang (Näherung) zwischen n (bzw. der dezimalen Stellenanzahl von n) und dem durchschnittlichen Abstand zur nächsten Primzahl auf.

   Fertigen Sie ein oder zwei Folien zur Ergebnispräsentation an!