FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2023/24
zu bearbeiten bis
15.11.23

Praktikum 1
zur Vorlesung Kryptologie

1. Schreiben Sie eine Funktion zur Bestimmung des größten gemeinsamen Teilers zweier Zahlen:
   - Eingabewerte: Zwei ganze Zahlen $a,\ b \geq 0$.
   - Rückgabewert: $\gcd(a,b)$.

   Testwerte: 1. $a = 282$, $b = 240$, 2. $a = 9^{100} + 1$, $b = 10^{100} + 1$. (Lsg.: 1. 6, 2. 401)

2. Schreiben Sie eine Funktion, die ausgibt, wieviel Schritte bei der Berechnung des größten gemeinsamen Teilers mittels des euklidischen Algorithmus nötig sind:
   - Eingabewerte: Zwei ganze Zahlen $a,\ b \geq 0$.
   - Rückgabewert: Anzahl der Modulo-Berechnungen bei Berechnung von $\gcd(a,b)$ mittels des euklidischen Algorithmus.

   Testwerte: wie bei 1. (Lsg. bei den zweiten Werten: ca. 168)

3. Schreiben Sie eine Funktion, die berechnet, wieviel Schritte im Mittel bei der Berechnung des größten gemeinsamen Teilers zweier Zahlen einer bestimmten Größenordnung nötig sind:
   - Eingabewerte: Zwei natürliche Zahlen anz und n.
   - Ablauf: Es werden anz-oft zwei Zahlen $0 \leq a, b < n$ zufällig gezogen und die Anzahl der Modulo-Berechnungen bei Berechnung von $\gcd(a,b)$ bestimmt.
   - Rückgabewert: Mittlere Anzahl.

4. Experimentieren Sie mit der Funktion aus 3. und stellen Sie eine Vermutung für einen funktionalen Zusammenhang (Näherung) zwischen n und dem Rückgabewert bei großen anz und n auf.

   Wie lautet der Zusammenhang zwischen mittlerer Schrittanzahl und Problemgröße, wenn man als Problemgröße die dezimale Stellenanzahl von n nimmt?

   Fertigen Sie ein oder zwei Folien zur Ergebnispräsentation an!

5. Schreiben Sie eine Funktion zur Lösung der Gleichung $c \cdot x = d \bmod m$:
   - Eingabewerte: Ganze Zahlen $c \geq 0$, $d \geq 0$ und $m > 0$.
   - Rückgabewert:
     Falls die Gleichung $c \cdot x = d \bmod m$ keine Lösung besitzt: -1.
     Sonst: Eine Lösung x mit $0 \leq x < m$.

   Testwerte:

c	25	86	19	6	6	$9^{100}+1$
d	13	13	14	3	3	$8^{100}+1$
m	61	61	61	15	18	$10^{100}+1$