

Übungen zur Vorlesung Kryptographie

Blatt 4

Für Aufgaben 13-15 sollte `sagemath` oder `python` benutzt werden.

Aufgabe 13: (Fermattest nutzen) Eine der Zahlen $2^{100} + 447$ und $2^{100} + 471$ ist eine Primzahl, die andere nicht. Finden Sie mit dem Fermattest heraus, welche was ist.
(Nutzen Sie bitte den Fermattest, nicht etwa `is_prime` oder `next_prime` oder Ähnliches. Obacht, nicht alle Befehle sind gleich gut geeignet, um die benötigten Terme zu berechnen!)

Aufgabe 14: (Zwei ist ein Lügner/alle sind Lügner) Obwohl der Fermattest nicht perfekt ist (siehe Vorlesung bzw. Skript), ist es ganz oft so, dass bereits die 2 ein Zeuge ist für “ N ist Nichtprimzahl“. Diese Aufgabe illustriert das.

(a) Finden Sie drei Zahlen $N \in \mathbb{N} \setminus \{1\}$ mit $N \leq 1000$, die keine Primzahlen sind, und für die dennoch gilt: $2^{N-1} \equiv 1 \pmod{N}$.

(b) Finden Sie zwei Carmichaelzahlen größer als 1000. Also: finden Sie zwei Zahlen $N \in \mathbb{N}$ mit $N \geq 1000$, die keine Primzahlen sind, so dass dennoch für alle $a \in \mathbb{N}$ mit $2 \leq a \leq N-1$ gilt: Falls $\text{ggT}(a, N) = 1$, so ist $a^{N-1} \equiv 1 \pmod{N}$.

(Ergoogelte Lösungen zählen hier nicht, zeigen Sie Ihren Programmcode.)

Aufgabe 15: (Miller-Rabin-Lügner)

(a) Finden Sie den kleinste Miller-Rabin-Zeugen dafür, dass $N = 3215031751$ keine Primzahl sein kann. (Das heißt, finden Sie $a \in \{2, 3, \dots, N-1\}$ mit $\text{ggT}(a, N) = 1$, so dass der Miller-Rabin-Test für dieses a ausgibt “ N ist keine Primzahl“.)

(b) Finden Sie alle Miller-Rabin-Lügner für $N = 155$, und für $N = 561$. (Das heißt, finden Sie $a \in \{2, 3, \dots, N-1\}$ mit $\text{ggT}(a, N) = 1$, so dass der Miller-Rabin-Test für dieses a ausgibt “ N ist wahrscheinlich Primzahl“.)

(c) Vergleichen sie diese Anzahlen mit denen in Satz 3.3.

Aufgabe 16: (Carmichaelzahlen selber basteln)

Es sei $N = p_1 \cdot p_2 \cdot p_3$, wobei die p_i ungerade Primzahlen sind. Das **Kriterium von Korselt** sagt in diesem Fall, dass N eine Carmichaelzahl ist genau dann, wenn $p_i - 1$ Teiler von $N - 1$ für alle $1 \leq i \leq 3$.

(a) Zeigen Sie: falls N eine Carmichaelzahl ist, dann ist $p_i - 1$ Teiler von $N - 1$ für alle $1 \leq i \leq 3$.

(b) Zeigen Sie: falls $p_i - 1$ Teiler von $N - 1$ für alle $1 \leq i \leq 3$ ist, dann ist N eine Carmichaelzahl.

(c) Zeigen Sie damit, dass jede Zahl der Form $(6m+1)(12m+1)(18m+1)$ eine Carmichaelzahl ist, sofern $6m+1$, $12m+1$ und $18m+1$ alle Primzahlen sind.

Abgabe bis Mittwoch 12.5.2021 bis 14 Uhr per Email an den Tutor.

Bitte auf jeder Abgabe das Tutorium angeben!

Jan Jan-Philipp Brünger
Leonard Simon Ellinghaus
Kallias Stoupas

jbruenger@techfak.de
lellinghaus+krypto@techfak.de
kstoupas+krypto@techfak.de