Dr. Dirk Frettlöh 6.5.2026

Übungen zur Vorlesung Kryptographie

Blatt 4

Wenn es nicht ausdrücklich verboten ist, dürfen oder gar sollten Sie `sagemath` *oder* `python` *zum Lösen benutzen.*

Aufgabe 13: (Genug Primzahlen?)
Die Aufgabe ist, zu bestimmen, wieviele 16-bit-Primzahlen es gibt, und wieviele 24-bit-Primzahlen. Genauer:

(a) Bestimmen Sie mit dem Primzahlsatz (Satz 3.1 im Skript) möglichst genaue obere und untere Schranken dafür, wieviele Primzahlen es zwischen 2^{k-1} und 2^k geben sollte, jeweils für $k = 16$ und $k = 24$.

(b) Zählen Sie (mit `sagemath` oder `python`), wieviele Primzahlen es zwischen 2^{k-1} und 2^k wirklich gibt, jeweils für $k = 16$ und $k = 24$.

Aufgabe 14: (Alles Lügner / Primzahl entlarven)
(a) Finden Sie drei Zahlen $N \in \mathbb{N} \setminus \{1\}$, die keine Primzahlen sind, so dass dennoch für alle $a \in \mathbb{N}$ mit $2 \leq a \leq N-1$ gilt: Falls $\mathrm{ggT}(a, N) = 1$, so ist $a^{N-1} \equiv 1 \bmod N$.

(b) Eine der Zahlen $2^{99} + 255$ und $2^{99} + 257$ ist eine Primzahl, die andere nicht. Finden Sie mit dem Fermattest heraus, welche was ist.

(Nutzen Sie den Fermattest, nicht etwa `is_prime` *oder* `next_prime` *oder Ähnliches. Obacht, nicht alle Befehle sind geich gut geeignet, um die benötigten Terme zu berechnen!)*

Aufgabe 15:(Chinesische Primzahlen)
Sei p eine ungerade Primzahl.

(a) Zeigen Sie: p ist Teiler von $2^p - 2$.

(b) Eine Zahl n mit der Eigenschaft "n ist Teiler von $2^n - 2$" heißt *chinesische Primzahl*. Denn chinesische Gelehrte hatten einst vermutet, dass aus "n ist Teiler von $2^n - 2$" folgt, dass n eine Primzahl ist. Widerlegen Sie diese, d.h.: Finden Sie drei Gegenbeispiele.

(c) Finden Sie eine gerade chinesische Primzahl.

Aufgabe 16: (Wieviele Miller-Rabin-Lügner?)
Finden Sie alle Miller-Rabin-Lügner für $N = 185$. Das heißt, finden Sie $a \in \{2, 3, \ldots, 184\}$, so dass der Miller-Rabin-Test für dieses a ausgibt "185 ist wahrscheinlich Primzahl".

Challenge nur für die Ehre: Finden Sie ein N, dass mehr Miller-Rabin-Lügner hat als 185.

Abgabe bis Mittwoch 13.5.2026 bis 12:00 Uhr per Email an die Tutorin.

Lisa Henetmayr Mi 12 Uhr in S0-115 lhenetmayr+krypto@techfak.de
Lisa Henetmayr Mi 16 Uhr in U2-147 lhenetmayr+krypto@techfak.de