

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 $\text{ggT}(a, N) = 1$, so ist $a^{N-1} \equiv 1 \pmod{N}$.

(b) Eine der Zahlen $10^{100} + 253$ und $10^{100} + 267$ 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 gleich gut geeignet, um die benötigten Terme zu berechnen!)

Aufgabe 15: (Wieviele Fermat-Lügner?)

(a) Finden Sie alle Fermat-Lügner mod 143 und alle Fermat-Lügner mod 341. (Nebenbei: warum sind 143 bzw. 341 keine Primzahlen?)

(b) Zeigen Sie: sind p und $2p - 1$ beides Primzahlen, sowie $N = p(2p - 1)$, so sind alle $a \in Z_N^*$, die quadratische Reste mod $2p - 1$ sind, Fermat-Lügner mod N .

Aufgabe 16: (Wieviele Miller-Rabin-Lügner?)

Finden Sie alle Miller-Rabin-Lügner für $N = 185$. Das heißt, finden Sie $a \in \{2, 3, \dots, 184\}$, 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 Dienstag 14.5.2024 bis 23:59 Uhr per Email an den Tutor.

Jakob Niermann	Mi 16 Uhr in T2-233	janiermann+krypto@techfak.de
Enrico di Gaspero	Do 16 Uhr in U2-216	edigaspero+krypto@techfak.de
Lisa Henetmayr	Fr 10 Uhr in X-E0-205	lhenetmayr+krypto@techfak.de
Richard Freidhof	Fr 12 Uhr in T2-141	rfreidhof+krypto@techfak.de