Übungen zur Vorlesung Kryptographie

Blatt 4

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

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), wieviele Primzahlen es zwischen 2^{k-1} und 2^k geben sollte, jeweils für $k = 16$ und $k = 24$.
(b) Zählen Sie (mit dem Rechner), wieviele Primzahlen es zwischen 2^{k-1} und 2^k wirklich gibt, jeweils für $k = 16$ und $k = 24$.

Aufgabe 14: (Fermattest nutzen) Eine der Zahlen $2^{80}+85$ und $2^{80}+71$ 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 geich gut geeignet, um die benötigten Terme zu berechnen!)*

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 $a \in \{2, 3, \ldots, N-1\}$ mit $\mathrm{ggT}(a, N) = 1$, so dass der Miller-Rabin-Test für dieses a ausgibt "N ist keine Primzahl".)

(b) Finden Sie alle Miller-Rabin-Lügner für $N = 145$, und für $N = 1105$. (Das heißt, finden Sie $a \in \{2, 3, \ldots, N-1\}$ mit $\mathrm{ggT}(a, N) = 1$, 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 $1 \le i \le 3$.

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

(b) Zeigen Sie: falls $p_i - 1$ Teiler von $N - 1$ für alle $1 \le i \le 3$ 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 $18m + 1$ alles Primzahlen sind.

(d) Finden Sie mittels (c) eine Carmichaelzahl.

Abgabe bis Dienstag 2.5.2023 bis 23:59 Uhr per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben!

Jakob Niermann janiermann+krypto@techfak.de
Tim Lakämper tlakaemper+krypto@techfak.de