Dr. Dirk Frettlöh 2.5.2022

Übungen zur Vorlesung Kryptographie

Blatt 4

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 `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 $10^{100} + 253$ 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 geich 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 $a \in \{2, 3, \ldots, 184\}$, so dass der Miller-Rabin-Test für dieses a ausgibt "185 ist wahrscheinlich Primzahl".

Abgabe bis Montag 9.5.2022 bis 14 Uhr per Email an Ihren Tutor.
Bitte auf jeder Abgabe das Tutorium angeben. Bitte die Abgaben so nennen:
techfakaccount-bl$n$.pdf, also z.B. `dfrettloeh-bl4.pdf`, oder `dfrettloeh+mnebel-bl4.pdf`.

Jan-Philipp Brünger jbruenger@techfak.de
Simon Hahm shahm+krypto@techfak.de
Tim Lakämper tlakaemper+krypto@techfak.de