Prof. Dr. M. Kreuzer
P. Ackermann

Abgabe: 15.05.2005, 14h

Kryptografie
Übungsblatt 5

Aufgabe 16:

a) Schreiben Sie ein Programm `SPH(...)`, welches als Eingabe eine Primzahl p, die Primfaktorzerlegung $p-1 = \prod p_i^{\alpha_i}$ von $p-1$, einen Erzeuger g von $(\mathbb{Z}/p\mathbb{Z})^\times$ sowie ein Element $y \in (\mathbb{Z}/p\mathbb{Z})^\times$ erwartet und den Algorithmus von Silver, Pohlig und Hellman benutzt, um ein $x \in \{0, \ldots, p-2\}$ mit $g^x = y$ zu bestimmen.

b) Bestimmen Sie den diskreten Logarithmus von 153 zur Basis 2 in $(\mathbb{Z}/181\mathbb{Z})^\times$. Dass 2 die Gruppe $(\mathbb{Z}/181\mathbb{Z})^\times$ erzeugt, kann vorausgesetzt werden.

Aufgabe 17:
Sei $n = pq$ das Produkt zweier verschiedener Primzahlen p und q, und sei $d = \mathrm{ggT}(p-1, q-1)$.

a) Beweisen Sie, dass n genau dann eine Pseudoprimzahl zu einer Basis b ist, wenn $b^d \equiv 1 \pmod{n}$ gilt

b) Bezüglich wie vieler Basen in $\{b \in \{1, \ldots, n-1\} \mid \mathrm{ggT}(b, n) = 1\}$ ist n eine Pseudoprimzahl?

c) Geben Sie diese Basen im Fall $q = 2p + 1$ an.

Aufgabe 18:
Sei n quadratfrei, d.h. n sei Produkt von paarweise verschiedenen Primzahlen. Zeigen Sie, dass n genau dann eine Carmichael-Zahl ist, wenn $p - 1 | n - 1$ für jede Primzahl p, die n teilt.