RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold

Präsenzübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 11 / 24.–26. Juni 2013

AUFGABE 1:
Sei $n \geq 3$ eine zusammengesetzte ungerade Zahl, $n-1 = 2^r d$, d ungerade. Wir betrachten den Miller-Rabin Primzahltest, angewendet auf n. Dieser kann an vier verschiedenen Stellen im Algorithmus die Antwort „Zusammengesetzt“ ausgeben. Modifizieren Sie den Miller-Rabin Algorithmus dahingehend, dass er zusätzlich eine (partielle) Faktorisierung von n ausgibt, wenn der Algorithmus „Zusammengesetzt“ ausgibt, und dies *nicht* in Zeile 3.5. (in der Notation im Skript), d.h. beim Test, ob $(a^d)^{2^r} \equiv 1 \mod n$ gilt, geschieht.

AUFGABE 2:
Faktorisieren Sie die zusammengesetzen Zahlen $n = 4331$ und $m = 7171$ mit Hilfe der Fermat-Faktorisierungsmethode.

AUFGABE 3:
Sei $n \equiv 2 \mod 3$ ungerade zusammengesetzte Zahl. Nehmen wir an, wir kennen $x \not\equiv y \mod n$ mit $x^3 \equiv y^3 \mod n$. Zeigen Sie, dass Sie dann effizient einen nicht-trivialen Faktor von n finden können.

Hinweis: Es gibt einen Primteiler p mit $p \equiv 2 \mod 3$.

AUFGABE 4:
Faktorisieren Sie Zahl $n = 6887$ mit Hilfe von Faktorbasen. Wählen Sie als Faktorbasis $B \subset \{-1, 2, 3, 5, 7, 11, 13\}$. Wählen Sie Ihre x_i's aus dem Intervall $[81, 85]$, d.h. nahe $\sqrt{n}$.

Bemerkung: Um die -1 in der Faktorbasis nutzen zu können sollte man mit dem Repräsentantensystem $\{-\frac{p-1}{2}, \ldots, +\frac{p-1}{2}\}$ von $\mathbb{Z}/(n)$ arbeiten. Sie benötigen in diesem Beispiel nicht unbedingt $|B|$ B-glatte Zahlen.