RUHR UNIVERSITÄT BOCHUM

RUB

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

**Hausübungen zur Vorlesung**

# Kryptanalyse

**WS 2012/2013**

Blatt 7 / 27. November 2012 / Abgabe bis spätestens 04. Dezember 2012, 8:30 Uhr in dem Kasten auf NA 02

**AUFGABE 1** (5 Punkte)**:**
Sei ein Algorithmus A gegeben, der bei Eingabe $N$ einen nicht-trivialen Faktor von $N$ in Zeit polynomiell in $\log N$ berechnet. Zeigen Sie, dass dann die komplette Primfaktorzerlegung von $N$ in Zeit polynomiell in $\log N$ berechnet werden kann.

**AUFGABE 2** (5 Punkte)**:**

(a) Seien $\mathbf{v}_1, \ldots, \mathbf{v}_j \in \mathbb{Z}_2^n$ linear unabhängig. Zeigen Sie, dass dann die Wahrscheinlichkeit, dass ein zufällig aus $\mathbb{Z}_2^n$ gezogener Vektor zu $\mathbf{v}_1, \ldots, \mathbf{v}_j$ linear unabhängig ist, durch $1 - 2^{j-n}$ gegeben ist.

(b) Seien $\mathbf{v}_1, \ldots, \mathbf{v}_k \in \mathbb{Z}_2^n, k \leq n$ zufällig gewählte Vektoren. Zeigen Sie, dass diese Vektoren mit Wahrscheinlichkeit

$$\prod_{i=0}^{k-1}(1 - 2^{i-n})$$

linear unabhängig sind.

*Hinweis:* Führen Sie einen Beweis per Induktion über $k$.

**AUFGABE 3** (5 Punkte)**:**
Implementieren Sie den Faktorisierungs-Algorithmus mittels Faktorbasen (Skript Seite 87). Bestimmen Sie die *vollständige* Faktorisierung von `N=4343386802335140949`. Verwenden Sie eine Faktorbasis $F_B$ für die Glattheitsschranke $B = 1000$. Geben Sie den Quellcode mit ab.

*Hinweis:* Zur Erzeugung der Faktorbasis ist der Befehl `prime_range(n)` hilfreich, welche alle Primzahlen zwischen $2, \ldots, n$ liefert. Eine naive Implementierung in sage kann zur Lösung einige Minuten in Anspruch nehmen.
Sie dürfen gerne eigentständige Verbesserungen benutzen (z.B. *Siebtechniken* zur effizienteren Bestimmungen $B$-glatter Elemente).