



Hausübungen zur Vorlesung

Kryptanalyse

WS 2009/2010

Blatt 7 / 20. Januar 2010 / Abgabe bis spätestens 03. Februar 2010, 10 Uhr
(vor der Übung)

AUFGABE 1 (6 Punkte):

- (a) Seien $v_1, \dots, v_j \in \mathbb{F}_2^n$ linear unabhängig. Dann ist die Wahrscheinlichkeit, dass ein zufällig aus \mathbb{F}_2^n gezogener Vektor zu v_1, \dots, v_j linear unabhängig ist, durch $1 - 2^{j-n}$ gegeben.
- (b) Seien $v_1, \dots, v_k \in \mathbb{F}_2^n, k \leq n$ zufällig gewählte Vektoren. Zeigen Sie, dass diese Vektoren mit Wahrscheinlichkeit

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

linear unabhängig sind.

AUFGABE 2 (4 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 3 (10 Punkte):

- Implementieren Sie den Algorithmus zur Faktorisierung wie er im Skript beschrieben ist. (*Sie können auch gerne Verbesserungen wie z.B. Sieben verwenden.*)
- Benutzen Sie den Algorithmus um einen nicht-trivialen Faktor der Zahl $N = 4343386802335140949$ zu bestimmen. Verwenden Sie dabei als Glattheitsschranke $B = 1000$. (*Rechenzeit für naive Implementierung in SAGE etwa 5 Minuten, C vermutlich um einen Faktor 5-10 schneller.*)

- Analysieren Sie die Gesamtlaufzeit Ihres Algorithmus in Abhängigkeit der Faktorbasisgröße. D.h. Berechnen Sie für $B_i = 648 + 25i$ für $i = 0, \dots, 120$ einen nicht-trivialen Faktor und messen Sie die benötigte Zeit. Stellen Sie das Ergebnis in einem Graph dar. Finden Sie dabei immer mind. $|FB_{B_i}| + 1$ viele B_i -glatte Werte. (*Rechenzeit im Bereich mehrerer Stunden.*)