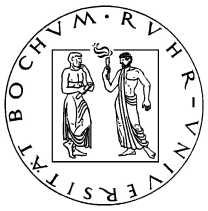
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Thomas Dullien



Präsenzübungen zur Vorlesung

Kryptographie I

WS 2009

Blatt 2 / 30.Oktober 2009

AUFGABE 1:
Der momentan beste Faktorisierungsalgorithmus berechnet einen Primfaktor von einer n-Bit Zahl in $2^{cn^{\frac{1}{3}}(\log n)^{\frac{2}{3}}}$ Rechenschritten. Nehmen Sie an, dass $c = 2$ und eine Instruktion auf einem Prozessor genau einem Rechenschritt entspricht und dieser Algorithmus perfekt verteilbar ist. Desweiteren nehmen Sie an, dass ein Prozessor 2^{32} Instruktionen pro Sekunde ausführen kann, und dass dieser Prozessor 250 EU kostet.
Unter der Annahme, dass man in 5 Jahren fertig sein möchte:

- Wie viel würde es ungefähr kosten, eine 512-Bit Zahl zu faktorisieren ?
- Wie viel würde es ungefähr kosten, eine 1024-Bit Zahl zu faktorisieren ?
- Wie viel würde es ungefähr kosten, eine 2048-Bit Zahl zu faktorisieren ?

Hinweis: 5 Jahre haben ca. 2^{27} Sekunden.

AUFGABE 2:
Beweisen Sie die Äquivalenz der folgenden Definitionen:

Definition 1. *Eine Funktion $f : \mathbb{R} \to \mathbb{N}$ heisst vernachlässigbar, wenn für jedes Polynom p ein $N \in \mathbb{N}$ existiert, sodass für alle $n \geq N$ gilt $f(n) < \frac{1}{p(n)}$*

Definition 2. *Eine Funktion $f : \mathbb{R} \to \mathbb{N}$ heisst vernachlässigbar, wenn für jede Konstante $c \in \mathbb{R}$ ein $N \in \mathbb{N}$ existiert, sodass $f(n) < n^{-c}$ für $n \geq N$ gilt.*

AUFGABE 3:
Betrachten Sie den folgenden Algorithmus, der aus einem zufälligen 8-Bit-String $x = x_0 \dots x_8$ einen pseudozufälligen 24-String $x = x_0 \dots x_8 x_8 \dots x_0 x_0 \dots x_8$ generiert.
Konstruieren Sie einen Unterscheidungsalgorithmus, der mit einer Fehlerwahrscheinlichkeit von weniger als 2^{-64} den Pseudozufallsgenerator von "echtem" Zufall unterscheidet.

AUFGABE 4:
Sei G ein Pseudozufallsgenerator mit $|G(s)| > 2|s|$. Definiere $G'(s) = G(s0^{|s|})$. Ist G' notwendigerweise auch ein Pseudozufallsgenerator ?