Privatdozent Dr. C. Diem
diem@math.uni-leipzig.de
http://www.math.uni-leipzig.de/∼diem/krypto

KRYPTOGRAPHIE
ÜBUNGSBLATT NR. 4

Aufgabe 1 Zeigen Sie:

a) Wenn f und $g : \mathbb{N} \longrightarrow \mathbb{R}$ vernachlässigbar sind, dann ist es auch $f + g$.

b) Wenn $f : \mathbb{N} \longrightarrow \mathbb{R}$ vernachlässigbar, dann ist auch für jede nicht-negative Polynomfunktion p die Funktion $p \cdot f$ vernachlässigbar.

Aufgabe 2 Welche der folgenden Funktionen / Folgen sind vernächlässigbar (in n)?

$$2^{-n}\,,\ 2^{-\sqrt{n}}\,,\ 2^{-2\cdot\log_2(n)}\,,\ 2^{-\log_2(n)^2}\,,\ n^{-\log_2(n)}\,,\ \log_2(n)^{-\log_2(n)}$$

Aufgabe 3

i) Definieren Sie formal Verschlüsselungssysteme mit privaten Schlüsseln und Zustand.

ii) Formulieren Sie entsprechende Angriffsszenarien.

iii) Bezüglich welcher dieser Szenarien ist das one-time-Pad (als Verfahren mit Zustand) sicher?

Aufgabe 4 In den Angriffsszenarien für den komplexitätstheoretischen Zugang haben wir festgelegt, dass ein Angreifer immer zwei Nachrichten m_1, m_2 gleicher Länge wählen muss.
Wir geben uns nun ein Verschlüsselungsverfahren vor, das zu einem gegebenen Sicherheitsniveau Nachrichten einer beliebigen Länge akzeptiert.
Wir modifizieren das Spiel für die IND-EAV-Definition derart, dass wir Nachrichten m_1, m_2 verschiedener Länge zulassen. Zeigen Sie, dass das Verfahren die modifizierte Definition nicht erfüllt.

Hinweis. Die Idee ist: Wenn man eine "ganz kurze" Nachricht verschlüsselt, ist der Chiffriertext auch "kurz". Wenn man hingegen eine "recht lange" Nachricht verschlüsselt, ist der Chffriertext "in der Regel" auch "recht lang". Dies "in der Regel" sollte eine Wahrscheinlichkeit werden.

Am besten schriftlich, aber mündlich ist besser als gar nicht ...