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

KRYPTOGRAPHIE
ÜBUNGSBLATT NR. 3

Aufgabe 1 Wir betrachten das Ununterscheidbarkeits-Spiel, das genau so beschrieben wird:

1. Der Herausforderer wählt $k \in \mathcal{K}$ "nach Vorschrift".
2. Der Angreifer wählt zwei verschiedene Nachrichten $m_1, m_2 \in \mathcal{M}$. (Das kann stochastisch sein.) Er schickt diese an den Herausforderer.
3. Der Herausforderer wählt $i \in \{1, 2\}$ gleichverteilt und schickt $c := \mathcal{E}nc_k(m_i)$ an den Angreifer.
4. Der Angreifer wählt $j \in \{1, 2\}$ und gibt dies bekannt.

Der Angreifer gewinnt, wenn $i = j$ ist.

a) Kann man Schritte im Ablauf des Spiels vertauschen, ohne dass man "irgendwas Relevantes ändert"? Das heißt konkret: ohne, dass es Angreifer mit besserer oder schlechterer Gewinnwahrscheinlichkeit gibt. Wenn ja, dann welche Schritte?

b) Ist es relevant, dass der Angreifer m_1 und m_2 stochastisch wählen kann, oder könnte man auch "ohne relevante Änderung" verlangen, dass diese Wahl deterministisch zu erfolgen hat?

c) Der Angreifer wähle $i \in \{1, 2\}$ nicht mehr gleichverteilt, sondern mit einer festen Wahrscheinlichkeit wie – sagen wir – $2/3$ zu $1/3$. Dann gibt es einen trivialen Angreifer mit Gewinnwahrscheinlichkeit $2/3$, stimmt's? Also sollten wir dann für den Vorteil eines Angreifers $\mathcal{A}$ definieren als $\mathbb{P}[\mathcal{A} \text{ gewinnt}] - \frac{2}{3}$.

   Sagen wir, wir machen dies so. Können wir dann die Aussagen über perfekte Sicherheit etc. übertragen oder erhalten wir substantiell andere Aussagen?

Aufgabe 2 (nicht so leicht, bitte – wenn Sie es machen wollen – schriftlich abgeben) Wir nennen ein Verfahren *ϵ-fast-perfekt-sicher* (bei einmaliger Anwendung pro Schlüssel), wenn für jeden Angreifer $\mathcal{A}$ (bzgl. des Unterscheidbarkeits-Experiments) gilt:

$$\mathbb{P}[\mathcal{A} \text{ gewinnt}] \leq \frac{1}{2} + \epsilon$$

a) Für jedes $\epsilon > 0$ gibt es ein ϵ-fast-sicheres Verfahren mit $|\mathcal{K}| < |\mathcal{M}|$.

b) Geben Sie für $|\mathcal{K}| < |\mathcal{M}|$ ein $\epsilon_0 = \epsilon_0(|\mathcal{K}|, |\mathcal{M}|)$ an derart, dass jedes Verschlüsselungsverfahren für $\mathcal{M}$ und $\mathcal{K}$ höchstens ϵ_0-fast-perfekt-sicher ist.