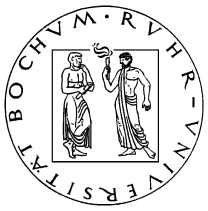
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann




**Präsenzübungen zur Vorlesung**

# Kryptographie 2

**SS 2009**

Blatt 3 / 20. Mai 2009

**AUFGABE 1:**
Betrachten Sie den in der Vorlesung vorgestellten Chosen-Ciphertext Angriff auf das ElGamal-Verfahren. Ein Angreifer beobachtet dabei einen Chiffretext $c = \langle c_1, c_2 \rangle = \langle g^y, h^y \cdot m \rangle$ und sendet anschließend den Chiffretext $c' = \langle c_1, c_2 \cdot m' \rangle$, der eine gültige Verschlüsselung der Nachricht $m \cdot m'$ ist.
Angenommen der Empfänger findet es verdächtig, wenn zwei Verschlüsselungen mit der gleichen ersten Komponente an ihn gesendet werden und verwirft den zweiten Chiffretext. Zeigen Sie, wie ein Angreifer dieses Problem beseitigen kann.

**AUFGABE 2:**
Sei $f(x)$ eine Einwegfunktion. Zeigen Sie, das dann auch $g(x_1, x_2) := (x_1, f(x_2))$ mit $|x_1| = |x_2|$ eine Einwegfunktion ist.

**AUFGABE 3:**
Betrachten Sie folgende Variante der Verschlüsselung mit Hilfe einer Familie von Trapdoor-Permutationen:

> Sei $\widehat{\Pi} = (\widehat{Gen}, f)$ eine Familie von Trapdoor-Permutationen und $hc$ ein Hardcore-Prädikat für $\widehat{\Pi}$. Wir konstruieren das ein Public Key Encryption Schema durch
>
> - **Gen**: Starte $(I, td) \leftarrow \widehat{Gen}(1^n)$, öffentlicher Schlüssel $pk$ ist $I$, geheimer Schlüssel $sk$ ist $td$.
> - **Enc**: Eingabe $pk$ und $m \in \{0,1\}$. Wähle zufällig $x \leftarrow \mathcal{D}_I$ so dass $hc_I(x) = m$ und gebe den Chiffretext $c = f_I(x)$ aus.
> - **Dec**: Eingabe $sk$ und $c \in \mathcal{D}_I$. Berechne $x := f_I^{-1}(c)$ und gebe die Nachricht $hc_I(x)$ zurück.

1. Warum kann die Verschlüsselung in Polynomialzeit durchgeführt werden?
2. Zeigen Sie, dass falls $\widehat{\Pi}$ eine Familie von Trapdoor-Permutationen ist und $hc$ ein Hardcore-Prädikat für $\widehat{\Pi}$, dann ist die Konstruktion CPA-sicher.