Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Florian Giesen

RUHR UNIVERSITÄT BOCHUM RUB

Präsenzübungen zur Vorlesung

Kryptographie 1

WS 2010/11

Blatt 1 / 18./20. Oktober 2010

AUFGABE 1. Angriffe.
Konstruieren Sie für folgende drei Chiffren einen trivialen KPA-Angreifer und erläutern Sie, wie viele Klartextsymbole jeweils nötig sind, um den geheimen Schlüssel zu berechnen.

a) Verschiebechiffre

b) Vigenèrechiffre (wobei Sie annehmen dürfen, dass t bekannt ist)

c) allgemeine Substitutionschiffre, d.h. für eine Permutation $\pi : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ verschlüsseln wir $m \in \mathbb{Z}_{26}^n$ mit $c := \langle \pi(m_0), \ldots, \pi(m_{n-1}) \rangle$.

Kommt man mit noch weniger Klartextsymbolen aus, wenn man anstelle eines KPA-Angreifers einen stärkeren CPA-Angreifer betrachtet?

AUFGABE 2. Two-Time Pad.
Betrachten Sie folgende Modifikation des One-Time Pads:

Sei $\mathcal{K} = \{0,1\}^\ell$ und $\mathcal{M} = \mathcal{C} = \{0,1\}^{2\ell}$.
Gen: Ausgabe $k \in_R \{0,1\}^\ell$.
Enc: Für $m = (m_1, m_2) \in \{0,1\}^{2\ell}$ gib aus $c = (m_1 \oplus k, m_2 \oplus k)$.

Geben Sie eine korrekte Entschlüsselung Dec an. Zeigen Sie, dass das Two-Time Pad *nicht* perfekt sicher ist.

AUFGABE 3. Perfekte Sicherheit.

a) Beweisen oder widerlegen Sie: Für ein perfekt sicheres Verschlüsselungsverfahren gilt, dass für jede Verteilung auf dem Nachrichtenraum $\mathcal{M}$, jedes $m, m' \in \mathcal{M}$ und jedes $c \in \mathcal{C}$ gilt

$$\mathbf{Pr}\left[M = m | C = c\right] = \mathbf{Pr}\left[M = m' | C = c\right].$$

b) Kann es ein perfekt sicheres Verschlüsselungsverfahren geben, bei dem es möglich ist, effizient 90% der Bits des geheimen Schlüssels zu berechnen? Falls ja, geben Sie eine Konstruktion an und beweisen Sie die perfekte Sicherheit!