Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Stefan Hoffmann, Ilya Ozerov

Hausübungen zur Vorlesung

Kryptographie

WS 2013/14

Blatt 2 / 21. Oktober 2013

Abgabe: 29. Oktober 2013, 14.00 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (5 Punkte)**:**

Bei weiteren Ausgrabungen (vgl. Präsenzübung, Aufgabe 1) wird eine Schriftrolle gefunden, in der eine Erweiterung der Kriegs-Verschlüsselung beschrieben wird. Neben den bekannten Truppenbewegungen $<, >, \wedge$ und $\vee$ wird ein weiteres Symbol $\diamondsuit$ für „Position halten" benötigt, so dass für Nachrichten- und Chiffretextraum $\mathcal{M} = \mathcal{C} = \{<, >, \wedge, \vee, \diamondsuit\}$ gilt.

(a) Überlegen Sie sich eine geeignete Schlüsselmenge $\mathcal{K}$ mit $|\mathcal{K}| = 5$ und erstellen Sie die Tabelle eines *perfekt sicheren*, korrekten, symmetrischen Verschlüsselungsverfahrens.

(b) Zeigen Sie die Korrektheit und die perfekte Sicherheit Ihres Verschlüsselungsverfahrens. Sie dürfen (hier und für den Rest der Vorlesung) davon ausgehen, dass $k \in_R \mathcal{K}$ effizient gewählt werden kann.

AUFGABE 2 (5 Punkte)**:**

Beweisen oder widerlegen Sie: Für jedes perfekt sichere Verschlüsselungsverfahren gilt, dass es eine Verteilung auf dem Nachrichtenraum $\mathcal{M}$ gibt, so dass für jedes $m, m' \in \mathcal{M}$ und jedes $c \in \mathcal{C}$ gilt

$$\mathsf{Ws}[M = m | C = c] = \mathsf{Ws}[M = m' | C = c].$$

Bitte wenden!

AUFGABE 3 (5 Punkte)**:**

Betrachten Sie folgende Modifikation des One-Time Pads, das „Two-Time Pad“. Sei der Schlüsselraum $\mathcal{K} = \{0,1\}^n$ und der Nachrichten- und Chiffretextraum $\mathcal{M} = \mathcal{C} = \{0,1\}^{2n}$.

- $\mathsf{Gen}(1^n)$: Wähle $k \in_R \{0,1\}^n$.
- $\mathsf{Enc}_k(m)$: Für $m = (m_1, m_2) \in \{0,1\}^{2n}$ gib $c := (m_1 \oplus k, m_2 \oplus k)$ aus.

(a) Geben Sie eine korrekte Entschlüsselungsfunktion $\mathsf{Dec}_k(c)$ an.

(b) Zeigen Sie, dass das „Two-Time Pad” *nicht* perfekt sicher ist.

AUFGABE 4 (5 Punkte)**:**

Wir definieren das symmetrische Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ mit identischem Nachrichten-, Chiffretext- und Schlüsselraum $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{2^n}$ wie folgt:

- $\mathsf{Gen}(1^n)$: Wähle $k \in_R \mathbb{Z}_{2^n}$.
- $\mathsf{Enc}_k(m)$: Gib $c := k + m \bmod 2^n$ aus.

(a) Geben Sie eine korrekte Entschlüsselungsfunktion $\mathsf{Dec}_k(c)$ an.

(b) Zeigen Sie, dass Π perfekt sicher ist.

Anmerkung: Für $a \in \mathbb{N}$ ist $\mathbb{Z}_a := \{0, \ldots, a-1\}$.