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

Hausübungen zur Vorlesung

Kryptographie I

WS 2012/13

Blatt 1 / 12. Oktober 2012

Abgabe: 22. Oktober 2012, 12 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* Verschlüsselungsverfahrens.

(b) Damit das Verfahren perfekt sicher ist, muss der Schlüssel zufällig und *gleichverteilt* aus $\mathcal{K}$ gewählt werden. In der Originalversion des Verschlüsselungsverfahrens aus der Präsenzübung bestand die Schlüsselmenge aus vier Elementen. Hier konnte man mit zwei (echten) Münzwürfen gleichverteilt einen Schlüssel wählen. Bei $|\mathcal{K}| = 5$ ist es allerdings *mit Hilfe von einzelnen Münzwürfen* nicht möglich *gleichverteilt* aus $\mathcal{K}$ zu wählen. Dies ist ein nicht unwichtiges praktisches Problem, das z.B. in `http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1002_reportDSA.pdf` (Kapitel 5) angesprochen wird. **Beschreiben Sie** (kurz, in 2-3 Sätzen) das Problem gleichverteilt zu wählen, wenn $|\mathcal{K}|$ keine Zweierpotenz ist, anhand der Implementierungsschwäche, die Bleichenbacher in seinem Angriff ausnutzt.

(c) Nehmen Sie hier (und auch für den Rest der Vorlesung) an, es gibt für jede Größe $|\mathcal{K}|$ eine Möglichkeit zufällig und gleichverteilt Schlüssel aus $\mathcal{K}$ zu wählen. Zeigen Sie die perfekte Sicherheit Ihres Verschlüsselungsverfahrens.

Bitte wenden!

AUFGABE 2 (5 Punkte)**:**

Sei $n \in \mathbb{N}$. Wir definieren das symmetrische Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ mit dem Nachrichtenraum $\mathcal{M} = \mathbb{Z}_{2n}$, dem Chiffretextraum $\mathcal{C} = \mathbb{Z}_{2n}$ und dem Schlüsselraum $\mathcal{K} = \{k \in \mathbb{Z}_{2n} \mid k \text{ gerade}\}$ wie folgt:

- $\mathsf{Gen}(1^n)$: Wählt $r \in_R \mathbb{Z}_n$ uniform. Ausgabe $k := 2r \in \mathcal{K}$.
- $\mathsf{Enc}_k(m)$: Gibt $c := k + m \bmod 2n$ aus.

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

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

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

AUFGABE 3 (5 Punkte)**:**

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

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

AUFGABE 4 (5 Punkte)**:**

Wir erlauben in dieser Aufgabe einem Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ bei der Entschlüsselung mit einer gewissen Wahrscheinlichkeit falsch zu liegen, d.h. wir fordern lediglich

$$\mathsf{Ws}[\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m] \geq 2^{-t}$$

anstelle von $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$. Zeigen Sie, dass dann für $t \geq 1$ Verfahren existieren, die perfekt sicher sind und $|\mathcal{K}| < |\mathcal{M}|$ erfüllen.

Hinweis: Versuchen Sie, für Nachrichten $m \in \{0,1\}^{\ell+t}$ den vorderen Teil mit einem One-Time Pad zu verschlüsseln und für den hinteren Teil auszunutzen, dass Entschlüsselungsfehler erlaubt sind.