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

Präsenzübungen zur Vorlesung

Kryptographie I

WS 2012/13

Blatt 1 / 15./17. Oktober 2012

AUFGABE 1:

Bei Ausgrabungen wird eine Schriftrolle mit folgender antiken Verschlüsselungstabelle gefunden, die leider nicht vollständig erhalten ist:

	$>$	$\vee$	$<$	$\wedge$
$\bullet$	$>$	$\vee$	$<$	$\wedge$
$\leftrightarrows$	$<$	$\wedge$	$>$	
$\circlearrowleft$	$\wedge$	$>$		
$\circlearrowright$				

Auf einer weiteren Schriftrolle findet man die Erklärung, dass diese Verschlüsselung im Krieg genutzt wurde. Die Truppenbewegungen "links", "rechts", "Angriff", "Rückzug" wurden durch die Symbole $\mathcal{M} = \{<, >, \wedge, \vee\}$ kodiert. Die Symbole $\mathcal{K} = \{\bullet, \leftrightarrows, \circlearrowleft, \circlearrowright\}$ bildeten den Schlüsselraum. Die Klartextsymbole wurden auf Chiffretextsymbole $\mathcal{C} = \mathcal{M}$ abgebildet.

Der Schlüssel wurde durch zwei Münzwürfe bestimmt und damit zufällig, gleichverteilt gewählt. Für jede neue Übermittlung einer Truppenbewegung wurde ein neuer Schlüssel verwendet.

(a) Ergänzen Sie die Tabelle zu einem *perfekt sicheren* Verschlüsselungsverfahren und zeigen Sie die perfekte Sicherheit. Benutzen Sie dazu den Satz von Shannon.

(b) Zur Erhöhung der Sicherheit wurde vorgeschlagen, die erste Zeile zu entfernen, also das Verschlüsseln mit $\bullet$ nicht zu erlauben, da in diesem Fall die Verschlüsselung keine Auswirkung hat (und somit praktisch keine Verschlüsselung stattfindet). Zeigen Sie, dass das Verfahren mit $\mathcal{K}' = \{\leftrightarrows, \circlearrowleft, \circlearrowright\}$ nicht mehr perfekt sicher ist.

(c) Überlegen Sie, mit welcher Methode man das Problem aus (b) lösen könnte.

AUFGABE 2:

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

- $\mathsf{Gen}(1^n)$: Ausgabe $k \in_R \{0,1\}^n$.
- $\mathsf{Enc}_k(m)$: 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 Entschlüsselung $\mathsf{Dec}_k(c)$ an.

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

AUFGABE 3:

Gegeben sei ein *perfekt sicheres* symmetrisches Verschlüsselungsverfahren. Zeigen Sie:

(a) $\mathsf{Ws}[K = k \mid M = m] = \mathsf{Ws}[K = k]$ für alle $k \in \mathcal{K}, m \in \mathcal{M}$.

(b) $\mathsf{Ws}[K = k \mid C = c] = \mathsf{Ws}[K = k]$ für alle $k \in \mathcal{K}, c \in \mathcal{C}$, falls $|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$ und die Verteilung auf $\mathcal{M}$ die Gleichverteilung ist.

(c) Zeigen Sie, dass die Behauptung aus (b) falsch wird, wenn die Verteilung auf $\mathcal{M}$ keine Gleichverteilung ist.

Hinweise: (a) hat mit perfekt sicherer Verschlüsselung nichts zu tun. Benutzen Sie für (b) den Satz von Shannon. Für (c) sollten Sie ein Gegenbeispiel angeben.