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

Präsenzübungen zur Vorlesung

Kryptographie

WS 2013/14

Blatt 2 / 21. Oktober 2013

AUFGABE 1:

(a) Überlegen Sie sich einen ppt-Algorithmus, der zufällig, gleichverteilt aus der Schlüsselmenge $\mathcal{K}$ zieht, wenn $|\mathcal{K}| = 2^n$ für ein $n \in \mathbb{N}$ gilt.

(b) Weshalb existiert kein ppt-Algorithmus, wenn $|\mathcal{K}|$ keine Zweierpotenz ist? Wie lässt sich das Problem beheben?

AUFGABE 2:

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

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

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.

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.