Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Eike Kiltz
Gottfried Herold

Hausübungen zur Vorlesung

Kryptographie I

WS 2011/2012

Blatt 1 / 14. Oktober 2011 / Abgabe **bis spätestens Montag, 24.10.2011 16:00 Uhr**

AUFGABE 1:

Betrachten sie folgende Modifikation des One-Time-Pads (die der Verschlüsselung von 2 Nachrichten mit dem selben OTP-Schlüssel entspricht):

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

(a) Geben Sie eine korrekte Entschlüsselungsfunktion an und zeigen Sie, dass es sich um ein symmetrisches Verschlüsselungsverfahren handelt. [2 Punkte]

(b) Zeigen Sie, dass dieses symmetrische Verschüsselungsverfahren nicht perfekt sicher ist. [2 Punkte]

AUFGABE 2:

Beweisen oder widerlegen Sie: [3 Punkte]
Für ein perfekt sicheres symmetrisches Verschlüsselungsverfahren gilt, dass für jede Verteilung auf dem Nachrichtenraum $\mathcal{M}$, jedes $m, m' \in \mathcal{M}$ und jedes $c \in \mathcal{C}$ gilt:

$$\mathbf{Ws}[M = m \mid C = c] = \mathbf{Ws}[M = m' \mid C = c].$$

- bitte wenden -

AUFGABE 3:

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

(a) $\mathbf{Ws}[K = k \mid M = m] = \mathbf{Ws}[K = k]$ für alle $k \in \mathcal{K}, m \in \mathcal{M}$ [1 Punkt]

(b) $\mathbf{Ws}[K = k \mid C = c] = \mathbf{Ws}[K = k]$ für alle $k \in \mathcal{K}, c \in \mathcal{C}$,
falls $|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$ und die Verteilungen auf $\mathcal{M}$ die Gleichverteilung ist [3 Punkte]

(c) Zeigen Sie, dass die Behauptung aus (b) falsch wird, wenn man lediglich annimmt, dass $|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$, aber die Verteilung auf $\mathcal{M}$ keine Gleichverteilung ist. [2 Punkte]

(d) Zeigen Sie, dass die Behauptung aus (b) falsch wird, wenn man die Bedingung $|\mathcal{K}| = |\mathcal{M}| = |\mathcal{C}|$ weglässt, aber Gleichverteilung auf $\mathcal{M}$ und $\mathcal{K}$ annimmt. [3 Punkte]

Hinweise: (a) hat mit perfekt sicherer Verschlüsselung nichts zu tun.
Benutzen Sie für (b) den Satz von Shannon aus der Vorlesung.
Für (c) bzw. (d) sollten Sie ein Gegenbeispiel angeben. Vergessen Sie nicht, Korrektheit und perfekte Sicherheit für Ihre Beispiele zu zeigen.
Sie sollten zeigen, dass in (b) und (c) die Verteilung auf $\mathcal{K}$ die Gleichverteilung sein muss.

AUFGABE 4:

Betrachten Sie folgende Definition perfekter Sicherheit für 2 Nachrichten:
Es soll gelten, dass für alle Wahrscheinlichkeitsverteilungen auf dem Nachrichtenraum $\mathcal{M}$, für alle $m \neq m' \in \mathcal{M}$ und $c \neq c' \in \mathcal{C}$ gilt, dass

$$\mathbf{Ws}[M = m \wedge M' = m' | C = c \wedge C' = c'] = \mathbf{Ws}[M = m \wedge M' = m' | M \neq M']$$

Dabei bezeichnen $M, M' \in_R \mathcal{M}$ zwei unabhängige Nachrichten aus die gemäß der Wahrscheinlichkeitsverteilung auf $\mathcal{M}$ gewählt werden und C, C' deren Verschlüsselungen (unter demselben Schlüssel $k \leftarrow \mathbf{Gen}$).

(a) Zeigen Sie, dass die Bedingung äquivalent ist zu
$\mathbf{Ws}[C = c \wedge C' = c' | M = m \wedge M' = m] \cdot \mathbf{Ws}[M \neq M'] = \mathbf{Ws}[C = c \wedge C' = c']$
für alle Wahrscheinlichkeitsverteilungen auf $\mathcal{M}$, $m \neq m'$, $c \neq c'$. [2 Punkte]

(b) Geben Sie ein Verschlüsselungsverfahren an, das dieser Bedigung genügt. $\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec}$ müssen dabei *nicht* notwendigerweise ppt. Algorithmen sein. [3 Punkte]

(c) (Bonus) Geben Sie ein Verschlüsselungsverfahren an (mit $|\mathcal{M}|$ exponentiell im Sicherheitsparameter), dass dieser Bedingung genügt, wobei $\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec}$ ppt. Algorithmen sind. [4 Bonuspunkte]

Hinweis: Wählen Sie in (b) $\mathcal{C} = \mathcal{M}$ sowie den Schlüsselraum $\mathcal{K}$ als die Menge aller Bijektionen auf $\mathcal{M}$.