André Bajorat
Rasmus Diederichsen
Lisa Goerke

Sebastian Höffner
Kristin Schmidt

Lösungen zu Übungsblatt 2
Kryptographische Verfahren

Besprechung 30. Oktober 2015

Aufgabe 2.1. Multiplikation von Resten

a)

$$\begin{aligned}
[km]_n - [km']_n &= 0 \\
k \odot_n m - k \odot_n m' &= 0 \\
[km - km']_n &= 0 \\
[k \cdot (m - m')]_n &= 0 \\
k \odot_n (m - m') &= 0
\end{aligned}$$

Das bedutet, dass n $k \odot_n (m - m')$ teilt. Nach Vorraussetzung sind n und k teilerfremd, sodass n stattdessen $(m - m')$ teilen muss. Da $m, m' \in \mathbb{Z}_n$, kann $[m - m']_n = 0$ nur gelten, falls $m = m'$. □

b)

Für die Injektivität ist Folgendes zu zeigen.

$$E_k(m_1) = E_k(m_2) \Rightarrow m_1 = m_2$$

$$\begin{aligned}
[m_1 k + l]_n &= [m_2 k + l]_n \\
[m_1 k]_n \oplus_n [l]_n &= [m_2 k]_n \oplus_n [l]_n \\
[m_1 k]_n \oplus_n l \oplus_n (n - l) &= [m_2 k]_n \oplus_n l \oplus_n (n - l) \\
[m_1 k]_n &= [m_2 k]_n
\end{aligned}$$

Nach Teilaufgabe a) folgt hieraus $m_1 = m_2$. □

Aufgabe 2.2. Die Wahrscheinlichkeit von Kryptotexten in perfekt sicheren Kryptosystemen

Sei Y die Zufallsvariable über den möglichen Kryptotexten $y \in \mathcal{C}$. Sei mit $\mathcal{C}(k) = \{c \in \mathcal{C} \mid \exists x \in \mathcal{M} : E_k(x) = c\}$ die Menge der durch einen Schlüssel k in Abhängigkeit des Klartextes erzeugbaren

Kryptotexte bezeichnet. Für die Wahrscheinlichkeit, einen bestimmten Kryptotext zu erhalten, gilt

$$\begin{aligned}
P(Y = y) &= \sum_{\{k \mid y \in \mathcal{C}(k)\}} P(K = k, E_k(x) = y) \\
P(Y = y) &= \sum_{\{k \mid y \in \mathcal{C}(k)\}} P(K = k, X = E_k^{-1}(y)) \\
&= \sum_{\{k \mid y \in \mathcal{C}(k)\}} P(K = k)\ P(X = E_k^{-1}(y)) && \text{Schlüssel und Klartext unabhängig} \\
&= \frac{1}{|\mathcal{K}|} \sum_{\{k \mid y \in \mathcal{C}(k)\}} P(X = E_k^{-1}(y)) && \text{Schlüssel gleichverteilt}
\end{aligned}$$

Da das System perfekt sicher ist, E_k injektiv sowie $|\mathcal{C}| = |\mathcal{M}|$, gibt es für jedes $(x, y) \in \mathcal{M} \times \mathcal{C}$ genau ein k mit $E_k(x) = y$.

$$= \frac{1}{|\mathcal{K}|} \sum_{\{k \mid y \in \mathcal{C}(k)\}} \frac{1}{|\mathcal{K}|}$$

Da E_k injektiv ist, muss jedes k auf $|\mathcal{M}| = |\mathcal{C}|$ verschiedene Kryptotexte abbilden. Dies bedeutet aber auch, dass jeder Kryptotext $c \in \mathcal{C}$ durch jedes $k \in \mathcal{K}$ generiert werden kann. Die obige Summe iteriert folglich über komplett $\mathcal{K}$, somit

$$P(Y = y) = \frac{1}{|\mathcal{K}|} \cdot 1$$

□

Aufgabe 2.3. Eine Weitere Formel für die a-posteriori-Wahrscheinlichkeit

Die Wahrscheinlichkeit des Ereignisses, einen bestimmten Kryptotext zu erhalten, ergibt sich aus der Wahrscheinlichkeit, irgendeinen Klartext und gleichzeitig einen ihn in den gegebenen Kryptotext überführenden Schlüssel zu erhalten. Es kann mehrere solcher Kombinationen geben.

$$\begin{aligned}
P(C = c) &= \sum_{m \in \mathcal{M}} \sum_{k \in \mathcal{K}_{m,c}} P(M = m \cap K = k) \\
&= \sum_{m \in \mathcal{M}} \sum_{k \in \mathcal{K}_{m,c}} P(M = m) \cdot (K = k) && \text{Schlüssel \& Klartext unabhängig} \\
&= \sum_{m \in \mathcal{M}} P(M = m) \sum_{k \in \mathcal{K}_{m,c}} (K = k) \\
&= \sum_{m \in \mathcal{M}} P(M = m) \cdot P(\mathcal{K}_{m,c})
\end{aligned}$$

Damit gilt

$$\begin{aligned}
P(M = m \mid C = c) &= \frac{P(M = m \cap C = c)}{P(C = c)} \\
&= \frac{P(M = m) \cdot P(\mathcal{K}_{m,c})}{\sum_{m' \in \mathcal{M}} P(M = m') \cdot P(\mathcal{K}_{m',c})} && \text{Siehe VL, Folie 5.33}
\end{aligned}$$

□

Aufgabe 2.4. Die Affine Verschlüsselung

a)

$$\begin{aligned} E_{(k,l)}(m) &= [km + l]_{26} \\ c &= [km + l]_{26} \\ c &= [[km]_{26} + l]_{26} \\ [c - l]_{26} &= [km]_{26} \end{aligned}$$

Da $l \in \mathbb{Z}_{26}$ können wir l als eine arbiträre Verschiebung ansehen und somit auslassen, d.h. wenn wir eine Lösung für $[c]_{26} = [km]_{26}$ finden, gibt es auch genau eine passende Lösung für $[c - l]_{26} = [km]_{26}$.

Das bedeutet auch, dass c und km kongruent modulo n sind. Das widerum bedeutet, dass $[c]_{26} = [km]_{26}$ genau dann lösbar ist, wenn $ggT(k, n)$ c teilt. Weil $ggT(k, n) = 1$ gegeben ist, und $\frac{c}{1} = c$ ist, ist somit die Gleichung lösbar – genauer noch: Sie hat genau $ggT(k, n)$ viele Lösungen.

Sie ist damit eindeutig lösbar in m, was im Umkehrschluss aber auch bedeutet, dass es für jedes Paar (m, c) genau eine Lösung von $[c]_{26} = [km]_{26}$ gibt, womit gezeigt ist, dass die Anzahl Schlüssel für jedes Paar konstant 1 ist.

b)

Wenn die Schlüssel gleichverteilt gewählt werden, ist die Wahrscheinlichkeit pro Schlüsselpaar (k, l)

$$P(\mathcal{K}_{m,c}) = \frac{1}{12 \cdot 26} = \frac{1}{312}$$

Wir können in die Formel der vorhergehenden Aufgabe einsetzen

$$\begin{aligned} P(M = m \mid C = c) &= \frac{P(M = m) \cdot P(\mathcal{K}_{m,c})}{\sum_{m' \in \mathcal{M}} P(M = m') \cdot P(\mathcal{K}_{m',c})} \\ &= \frac{P(M = m) \cdot \frac{1}{312}}{\sum_{m' \in \mathcal{M}} P(M = m') \cdot \frac{1}{312}} \\ &= \frac{P(M = m) \cdot \frac{1}{312}}{\frac{1}{312} \cdot \sum_{m' \in \mathcal{M}} P(M = m')} \\ &= \frac{P(M = m)}{\sum_{m' \in \mathcal{M}} P(M = m')} \\ &= \frac{P(M = m)}{1} \\ &= P(M = m) \end{aligned}$$

□

Das heißt bei einer Gleichverteilung der Schlüssel ist AFFIN tatsächlich perfekt sicher.