Rasmus Diederichsen
Lisa Goerke
Sebastian Höffner

Sven Kleine-Albers
Kristin Schmidt

Lösungen zu Übungsblatt 3
Kryptographische Verfahren

Besprechung 13. November 2015

Aufgabe 3.1. Polynomiell Sichere Kaskadenverschlüsselung

a)

Um ein Textpaar (m, c) zu entschlüsseln, können alle Ergebnisse der Verschlüsselungen $E_{k_i}(m)$ und die der Entschlüssselungen $D_{k_j}(c)$ miteinander verglichen werden. Im Fall $E_{k_i}(m) = D_{k_j}(c)$ gilt, dass ein valider Schlüssel zum Textpaar (m, c) genau (k_i, k_j) ist. Es sind also nun nur genau $2|\mathcal{K}|$ Ver- bzw. Entschlüsselungsoperationen nötig.

b)

Genau wie bei a) können hier Zwischenergebnisse verglichen werden. Dabei müssen wir in einer Richtung $|\mathcal{K}|^2$ Verschlüsselungen anwenden (eben genau $E_{k_i}(E_{k_j}(m))$), in der anderen genau $|K|$ viele Entschlüsselungen, $D_{k_l}(c)$.

Es sind also $|K|^2 + |K|$ Ver- und Entschlüsselungsoperationen nötig.

c)

Wählt man $k_2 = k_1$, so ergibt sich direkt:

$$\begin{aligned}
3\mathrm{DES}_{k_1,k_2}(m) &= \mathrm{DES}_{k_1}\left(\mathrm{DES}^{-1}_{k_2}\left(\mathrm{DES}_{k_1}(m)\right)\right)\\
3\mathrm{DES}_{k_1,k_1}(m) &= \mathrm{DES}_{k_1}\left(\mathrm{DES}^{-1}_{k_1}\left(\mathrm{DES}_{k_1}(m)\right)\right)\\
3\mathrm{DES}_{k_1,k_1}(m) &= \mathrm{DES}_{k_1}(m)
\end{aligned}$$

Das heißt, um DES zu simulieren, muss in 3DES nur zweimal der selbe Schlüssel gewählt werden.

Aufgabe 3.2. Betriebsmodi

m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	m_9	m_{10}	m_{11}	m_{12}	m_{13}	k	c_0
K	R	Y	P	T	O	G	R	A	P	H	I	E	D	X
10	17	24	15	19	14	6	17	0	15	7	8	4	3	23

a) CBC-Modus

$$
\begin{aligned}
\oplus &: [23+10]_{26} && = [33]_{26} = 7\\
c_1 &: [7+3]_{26} && = 10\\
\oplus &: [10+17]_{26} && = [27]_{26} = 1\\
c_2 &: [1+3]_{26} && = 4\\
\oplus &: [4+24]_{26} && = [28]_{26} = 2\\
c_3 &: [2+3]_{26} && = 5\\
\oplus &: [5+15]_{26} && = 20\\
c_4 &: [20+3]_{26} && = 23\\
\oplus &: [23+19]_{26} && = [42]_{26} = 16\\
c_5 &: [16+3]_{26} && = 19\\
\oplus &: [19+14]_{26} && = [33]_{26} = 7\\
c_6 &: [7+3]_{26} && = 10\\
\oplus &: [10+6]_{26} && = 16\\
c_7 &: [16+3]_{26} && = 19\\
\oplus &: [19+17]_{26} && = [36]_{26} = 10\\
c_8 &: [10+3]_{26} && = 13\\
\oplus &: [13+0]_{26} && = 13\\
c_9 &: [13+3]_{26} && = 16\\
\oplus &: [16+15]_{26} && = [31]_{26} = 5\\
c_{10} &: [5+3]_{26} && = 8\\
\oplus &: [8+7]_{26} && = 15\\
c_{11} &: [15+3]_{26} && = 18\\
\oplus &: [18+8]_{26} && = 0\\
c_{12} &: [0+3]_{26} && = 3\\
\oplus &: [3+4]_{26} && = 7\\
c_{13} &: [7+4]_{26} && = 11
\end{aligned}
$$

Ergebnis: **KEFXTKTNQISDL**

b) CTR-Modus

$$
\begin{aligned}
\oplus : [23+1]_{26} &= 1 \\
c_1 : [1+10]_{26} &= 11 \\
\oplus : [23+2]_{26} &= 2 \\
c_2 : [2+17]_{26} &= 19 \\
\oplus : [23+3]_{26} &= 3 \\
c_3 : [3+24]_{26} &= 1 \\
c_4 : [4+15]_{26} &= 19 \\
c_5 : [5+19]_{26} &= 24 \\
c_6 : [6+14]_{26} &= 20 \\
c_7 : [7+6]_{26} &= 16 \\
c_8 : [8+17]_{26} &= 25 \\
c_9 : [9+0]_{26} &= 9 \\
c_{10} : [10+15]_{26} &= 25 \\
c_{11} : [11+7]_{26} &= 18 \\
c_{12} : [12+8]_{26} &= 20 \\
c_{13} : [13+4]_{26} &= 17
\end{aligned}
$$

Ergebnis: **LTBTYUNZJZSUR**

c) Counter-Modus

d) OFB-Modus

$$
\begin{aligned}
s_1 : [23+3]_{26} &= 0\\
c_1 : [10+0]_{26} &= 10\\
s_2 : [0+3]_{26} &= 3\\
c_2 : [17+3]_{26} &= 20\\
s_3 : [3+3]_{26} &= 6\\
c_3 : [24+6]_{26} &= 4\\
s_4 : [6+3]_{26} &= 9\\
c_4 : [15+9]_{26} &= 24\\
s_5 : [9+3]_{26} &= 12\\
c_5 : [19+12]_{26} &= 5\\
s_6 : [12+3]_{26} &= 15\\
c_6 : [14+15]_{26} &= 3\\
s_7 : [15+3]_{26} &= 18\\
c_7 : [6+18]_{26} &= 24\\
s_8 : [18+3]_{26} &= 21\\
c_8 : [17+21]_{26} &= 12\\
s_9 : [21+3]_{26} &= 24\\
c_9 : [0+24]_{26} &= 24\\
s_{10} : [24+3]_{26} &= 1\\
c_{10} : [15+1]_{26} &= 16\\
s_{11} : [1+3]_{26} &= 4\\
c_{11} : [7+4]_{26} &= 11\\
s_{12} : [4+3]_{26} &= 7\\
c_{12} : [8+7]_{26} &= 15\\
s_{13} : [7+3]_{26} &= 10\\
c_{13} : [4+10]_{26} &= 14
\end{aligned}
$$

Ergebnis: **KUEYFDYMYQLPO**

Aufgabe 3.3. Kaskade

Unter der Annahme, dass ein Angreifer $\mathcal{A}$ existiert mit

$$P\left(\mathrm{Att}^{\mathrm{CP}}_{\mathcal{A},\Pi}(n) = 1\right) = \frac{1}{2} + \frac{1}{p(n)}$$

lässt sich das Schema aus Abbildung 1 konstruieren. Der konstruierte Angreifer $\mathcal{A}'$ spielt gegenüber $\mathcal{A}$ die Rolle von $\Pi = \Pi^1 \circ \Pi^2$. Er erhält von $\mathcal{A}$ zwei Klartexte, leitet diese an Π^2 weiter, das einen zufällig auswählt und mit E_2 verschlüsselt. Den Kryptotext $\widetilde{c}$ verschlüsselt $\mathcal{A}'$ mit E_1 und schickt das Ergebnis $E^1_{k_1}(E^2_{k_2}(m_b))$ an $\mathcal{A}$ zurück. $\mathcal{A}$ entscheidet sich nun für einen der beiden Klartexte.

$\mathcal{A}'$ leitet die Entscheidung an Π^2 weiter. Offensichtlich ist $\mathcal{A}'$ genau dann erfolgreich, wenn $\mathcal{A}$ erfolgreich ist. Damit wäre das sicher Kryptosystem Π^2 mit nicht vernachlässigbarer Wahrscheinlichkeit geknackt.

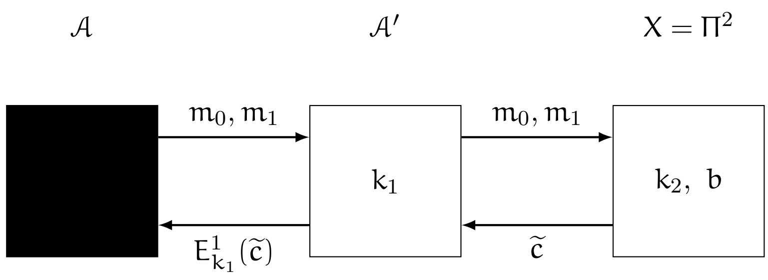

Abbildung 1: Ablauf des hypothetischen Angriffs