Kryptografie und -analyse, Übung 7

Henry Haustein

AES

(a) 10 Rundenschlüssel + 1 Schlüssel am Anfang
11 Runden $\cdot$ 4 Blöcke = 44 Blöcke
w_4: $\mathrm{Rcon}[j = i/N_k] = \mathrm{Rcon}[1] = [x^{j-1}, 00, 00, 00] = [01, 00, 00, 00]$
w_8: $\mathrm{Rcon}[j = 8/4] = \mathrm{Rcon}[2] = [x^{j-1}, 00, 00, 00] = [02, 00, 00, 00]$
w_{40}: $\mathrm{Rcon}[j = 40/4] = \mathrm{Rcon}[10] = [x^{j-1}, 00, 00, 00] = [36, 00, 00, 00]$. Muss noch modulo $x^8 + x^4 + x^3 + x + 1$ gerechnet werden:

$$x^9 \div (x^8 + x^4 + x^3 + x + 1) = x \quad R : x^5 + x^4 + x^2 + x = 00110110_2 = 36_{16}$$

(b) k_0

w_0	w_1	w_2	w_3
2b	28	ab	09
7e	ae	f7	cf
15	d2	15	4f
16	a6	88	3c

$k_1 = w_4 w_5 w_6 w_7$ mit

- $w_4 = w_0 \oplus (\mathrm{Rcon}[1] \oplus \mathrm{SubWord}(\mathrm{Rot}(w_3)))$
  - $\mathrm{Rot}(w_3) = \mathrm{cf4f3c09}$
  - $\mathrm{SubWord}(\mathrm{cf4f3c09}) = \mathrm{8a84eb01}$
  - $\mathrm{Rcon}[1] \oplus \mathrm{8a84eb01} = 01000000 \oplus \mathrm{8a84eb01} = \mathrm{8b84eb01}$
  - $w_0 \oplus \mathrm{8b84eb01} = \mathrm{2b7e1516} \oplus \mathrm{8b84eb01} = \mathrm{a0fafe17}$
- $w_5 = w_4 \oplus w_1 = \mathrm{a0fafe17} \oplus \mathrm{28aed2a6} = \mathrm{8b542cb1}$
- $w_6 = w_5 \oplus w_2 = \mathrm{8b542cb1} \oplus \mathrm{abf71588} = \mathrm{23a33939}$
- $w_7 = w_6 \oplus w_3 = \mathrm{23a33939} \oplus \mathrm{09cf4f3c} = \mathrm{2a6c7605}$

(c) Runde 0: $m \oplus k_0$

$$\begin{array}{c|c|c|c} 32 & 08 & \mathrm{f1} & \mathrm{e0} \\ 43 & 5\mathrm{a} & 31 & 37 \\ \mathrm{f6} & 30 & 58 & 07 \\ 68 & 8\mathrm{d} & \mathrm{a2} & 34 \end{array} \oplus \begin{array}{c|c|c|c} 2\mathrm{b} & 28 & \mathrm{ab} & 09 \\ 7\mathrm{e} & \mathrm{ae} & \mathrm{f7} & \mathrm{cf} \\ 15 & \mathrm{d2} & 15 & 4\mathrm{f} \\ 16 & \mathrm{a6} & 88 & 3\mathrm{c} \end{array} = \begin{array}{c|c|c|c} 19 & & & \\ & \mathrm{f4} & & \\ & & 4\mathrm{d} & \\ & & & 08 \end{array}$$

Runde 1: Ergebnis SubBytes, Ergebnis ShiftRow, Ergebnis Mixcolumn, $\oplus k_1$

$$\begin{array}{c|c|c|c}
\text{d4} & & & \\
& \text{bf} & & \\
& & \text{e3} & \\
& & & 30
\end{array}
,
\begin{array}{c|c|c|c}
\text{d4} & & & \\
\text{bf} & & & \\
\text{e3} & & & \\
30 & & &
\end{array}
,
\begin{array}{c|c|c|c}
\text{ba} & & & \\
& & & \\
& & & \\
& & &
\end{array}
\oplus
\begin{array}{c|c|c|c}
\text{a0} & \text{8b} & 23 & \text{2a} \\
\text{fa} & 54 & \text{a3} & \text{6c} \\
\text{fe} & \text{2c} & 39 & 76 \\
17 & \text{b1} & 39 & 05
\end{array}
=
\begin{array}{c|c|c|c}
\text{1a} & & & \\
& & & \\
& & & \\
& & &
\end{array}$$

Ergebnis von MixColumn: $d_i = a(x) \otimes c_i \mod x^4 + 1$, mit $a(x) = 03x^3 + 01x^2 + 01x + 02$ das heißt

$$\begin{pmatrix} d_{0i} \\ d_{1i} \\ d_{2i} \\ d_{3i} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} c_{0i} \\ c_{1i} \\ c_{2i} \\ c_{3i} \end{pmatrix}$$

$$\begin{aligned}
d_{0,0} &= 02 \cdot d4 \oplus 03 \cdot bf \oplus e3 \oplus 30 \mod x^8 + x^4 + x^3 + x + 1 \\
&= 00000010_2 \cdot 11010100 \ldots \mod x^8 + x^4 + x^3 + x + 1 \\
&= x \cdot (x^7 + x^6 + x^4 + x^2) \ldots \mod x^8 + x^4 + x^3 + x + 1 \\
&= x^8 + x^7 + x^5 + x^3 \ldots \mod x^8 + x^4 + x^3 + x + 1 \\
&= x^7 + x^5 + x^4 + x + 1 \ldots \mod x^8 + x^4 + x^3 + x + 1 \\
&= 10110011_2 \ldots \mod x^8 + x^4 + x^3 + x + 1 \\
&= b3 \ldots \mod x^8 + x^4 + x^3 + x + 1 \\
&= ba
\end{aligned}$$

(d) letzte Runde: Shift^{-1}, Sub^{-1} vertauschen
vorletzte Runden: $\oplus k_{r-1}$, MC^{-1} vertauschen ($k_{r-1} \to k'_{r-1}$) und Shift^{-1}, Sub^{-1} vertauschen, ...
$\Rightarrow$ neue Reihenfolge: Sub^{-1}, Shift^{-1}, MC^{-1}, $\oplus k'_{r-1}$, Sub^{-1}, Shift^{-1}, ... $\Rightarrow$ selbe Reihenfolge wie bei der Verschlüsselung