Geheime Botschaften

Sommersemester 2017

Dr. T. Moede
t.moede@tu-bs.de
Universitätsplatz 2, Raum 426
0531 391-7527

Technische Universität Braunschweig

Übungsblatt 6

Aufgabe 1. (AES - Schlüsselexpansion)
Gegeben sei der folgende 128-Bit-Schlüssel, geschrieben als Matrix von 4×4 Bytes:

$$\begin{pmatrix} 0101\ 0101 & 1100\ 0011 & 0111\ 0101 & 1010\ 1111 \\ 1111\ 0010 & 1111\ 0111 & 0110\ 0010 & 0000\ 1000 \\ 0110\ 0011 & 1111\ 1101 & 0110\ 0000 & 1110\ 1000 \\ 1111\ 1101 & 0101\ 0110 & 1011\ 0101 & 1011\ 1010 \end{pmatrix}.$$

Dieser dient als Rundenschlüssel für die Vorrunde im AES-Algorithmus.

Berechnen Sie den Rundenschlüssel für die ersten richtige Runde. Nehmen Sie dafür an, dass für die Funktion S, die SubBytes() beschreibt, gilt:

$$\begin{aligned} S(0000\ 1000) &= 0011\ 0000, \\ S(1110\ 1000) &= 1001\ 1011, \\ S(1011\ 1010) &= 1111\ 0100, \\ S(1010\ 1111) &= 0111\ 1001. \end{aligned}$$

Weiterhin sei die zu addierende Rundenkonstante gegeben als 0000 0001 0000 ... 0000.

Vorgehen:

- Bilde aus den Spalten der Schlüsselmatrix (von oben nach unten gelesen) vier 4-Byte-Wörter $w_0, \ldots, w_3$ gebildet.
- Berechne $w_4 = w_0 \oplus \phi(w_3)$. Hierbei ist ϕ die Hintereinanderausführung von:
  - Linksrotation des Wortes um 1 Byte,
  - Byteweises SubBytes(),
  - Addieren der Rundenkonstante.
- Berechne $w_5 = w_1 \oplus w_4$, $w_6 = w_2 \oplus w_5$, $w_7 = w_3 \oplus w_6$.
- Bilde aus den Wörtern $w_4, \ldots, w_7$ wieder eine (4×4)-Matrix. Diese ist der Rundenschlüssel für die erste Runde.

Aufgabe 2. (AES - MixColumns)
Im Schritt MixColumns() werden die Daten innerhalb der einzelnen Spalten vermischt. Dies geschieht in dem jede Spalte mit der Matrix

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}$$

multipliziert wird. Hierbei sind die Einträge als Bytes zu lesen, d.h.

$$\begin{aligned} 1 &= 0000\ 0001, \\ 2 &= 0000\ 0010, \\ 3 &= 0000\ 0011. \end{aligned}$$

Es gilt für eine Spalte also:

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} (2 \cdot b_0) \oplus (3 \cdot b_1) \oplus (1 \cdot b_2) \oplus (1 \cdot b_3) \\ (1 \cdot b_0) \oplus (2 \cdot b_1) \oplus (3 \cdot b_2) \oplus (1 \cdot b_3) \\ (1 \cdot b_0) \oplus (1 \cdot b_1) \oplus (2 \cdot b_2) \oplus (3 \cdot b_3) \\ (3 \cdot b_0) \oplus (1 \cdot b_1) \oplus (1 \cdot b_2) \oplus (2 \cdot b_3) \end{pmatrix}.$$

Die Addition ist das bekannte XOR. Die Multiplikation der Bytes ist wie folgt definiert:

Wir ordnen zwei Bytes, d.h. Bitfolgen $s_1, \ldots, s_8$ und $t_1, \ldots, t_8$ die Polynome

$$s_1 x^7 + s_2 x^6 + \ldots + s_7 x + s_8 \in \mathbb{F}_2[x]$$

bzw.

$$t_1 x^7 + t_2 x^6 + \ldots + t_7 x + t_8 \in \mathbb{F}_2[x]$$

zu. Das Ergebnis der Multiplikation sind nun die Koeffizienten des Polynoms, welches durch Multiplikation der beiden obenstehenden Polynome (in $\mathbb{F}_2[x]$) modulo $x^8 + x^4 + x^3 + x + 1$ entsteht.

Berechnen Sie die folgenden Produkte:

- $2 \cdot 0101\ 0101$
- $3 \cdot 1111\ 0010$
- $1 \cdot 0110\ 0011$
- $1 \cdot 1111\ 1101$