Homework 8 in Cryptography I
- Proposal for Solution -

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier
09.06.2011

Solution to Exercise 25.

The AES-128 Key K is given in hexadecimal notation as

$$K = 2D\ 61\ 72\ 69\ 65\ 00\ 76\ 61\ 6E\ 00\ 43\ 6C\ 65\ 65\ 66\ 66.$$

(a) The round key is $K_0 = K = (W_0, W_1, W_2, W_3)$ with $W_0 = (2D\ 61\ 72\ 69)$, $W_1 = (65\ 00\ 76\ 61)$, $W_2 = (6E\ 00\ 43\ 6C)$, and $W_3 = (65\ 65\ 66\ 66)$.

(b) In order to calculate the first 4 bytes of round key K_1 recall that $K_1 = (W_4, W_5, W_6, W_7)$, where W_4 contains the first 4 bytes. Follow Algorithm 1 to calculate W_4. Intialize for-loop with $i \leftarrow 4$.

Algorithm 1 AES key expansion

Split K into 4 32-bit words W_0, W_1, W_2, W_3
for $(i \leftarrow 4;\ i < 4 \cdot (r+1);\ i++)$ **do**
  tmp $\leftarrow W_{i-1}$
  if $(i \mod 4 = 0)$ **then**
    tmp $\leftarrow$ `SubByte`(`RotByte`(tmp)) $\oplus$ `Rcon`$(i/4)$
  end if
  $W_i \leftarrow W_{i-4} \oplus$ tmp
end for

tmp $\leftarrow W_3 = (65\ 65\ 66\ 66)$
$(i \mod 4 = 0)$ equals zero, so evaluate `SubByte`(`RotByte`(tmp)) $\oplus$ `Rcon`$(i/4)$

- $i/4 = 1$: `Rcon`$(i/4) = (RC(1)\ 00\ 00\ 00) = (01\ 00\ 00\ 00)$, $RC(i) = x^{i-1}$
- `RotByte`(tmp) $= (65\ 66\ 66\ 65)$, cyclic left shift
- `SubByte`(`RotByte`(tmp)) $=$ `SubByte`$(65\ 66\ 66\ 65) = (4D\ 33\ 33\ 4D)$ look it up in Table 5.8 at row 6 in columns 5 and 6 (77, 51). Note that the enumeration of rows and columns starts with zero.
- $tmp \leftarrow (4D\ 33\ 33\ 4D) \oplus (01\ 00\ 00\ 00) = (4C\ 33\ 33\ 4D)$

With the last command of Algorithm 1 it follows:
$W_4 \leftarrow W_0 \oplus$ tmp $= (61\ 52\ 41\ 24)$ which are the first 4 bytes of round key K_1:

	W_0	2	D	6	1	7	2	6	9
$\oplus$	tmp	4	C	3	3	3	3	4	D
	W_0	0010	1101	0110	0001	0111	0010	0110	1001
$\oplus$	tmp	0100	1100	0011	0011	0011	0011	0100	1101
	W_4	0110	0001	0101	0010	0100	0001	0010	0100
	W_4	6	1	5	2	4	1	2	4