Cryptology Exercise Week 5

Zijun Yu 202203581

Octobor 2023

Exercise 6.6

According to the definition of AES, the first column of R is

$$
\begin{aligned}
&R[:,0] \\
=&MC([S(a_{0,0}), S(a_{1,1}), S(a_{2,2}), S(a_{3,3})]) \\
=&MC([S(a_{0,0}), 0, 0, 0] \\
&\qquad \oplus [0, S(a_{1,1}), 0, 0] \\
&\qquad \oplus [0, 0, S(a_{2,2}), 0] \\
&\qquad \oplus [0, 0, 0, S(a_{3,3})]) \\
=&MC([S(a_{0,0}), 0, 0, 0]) \\
&\quad \oplus MC([0, S(a_{1,1}, 0, 0)]) \\
&\quad \oplus MC([0, 0, S(a_{2,2}), 0]) \\
&\quad \oplus MC([0, 0, 0, S(a_{3,3})]) \\
=&T_0(a_{0,0}) \oplus T_1(a_{1,1}) \oplus T_2(a_{2,2}) \oplus T_3(a_{3,3})
\end{aligned}
$$

Similarly, the rest of each column are

$$
\begin{aligned}
R[:,1] &= T_0(a_{0,1}) \oplus T_1(a_{1,2}) \oplus T_2(a_{2,3}) \oplus T_3(a_{3,0}) \\
R[:,2] &= T_0(a_{0,2}) \oplus T_1(a_{1,3}) \oplus T_2(a_{2,0}) \oplus T_3(a_{3,1}) \\
R[:,3] &= T_0(a_{0,3}) \oplus T_1(a_{1,0}) \oplus T_2(a_{2,1}) \oplus T_3(a_{3,2})
\end{aligned}
$$

Implementation

For S-box, we use a table that has 256 entries, each containing the S-box output for the respective input byte.

Besides the S-box operation, we also have a MixColumns operation in the T function, so for each of T_0, T_1, T_2, T_3, we have a table that has 256 entries, mapping from the input byte, i.e. the result of $S(a)$, to the output 4-byte column. Then each T function is a composition of the two table lookups.

Finally we apply the XOR operations shown in the above equations and in the *AddRoundkey* operation.

The memory usage of the tables is $256 + 4 * 4 * 256 = 4352$ bytes.