Prof. Dr. Rudolf Mathar, Dr. Michael Reyer

Tutorial 5

Friday, May 17, 2019

Problem 1. (*Weak DES keys*) There are four so called *weak* DES keys. One of those keys is

$$K = 00011111\ 00011111\ 00011111\ 00011111\ 00001110\ 00001110\ 00001110\ 00001110.$$

a) What happens if you use this key?

b) Can you find the other three weak keys?

Problem 2. (*AES mix columns*) The step `MixColumns` of the AES scheme is given by $\boldsymbol{r} = \boldsymbol{T}\boldsymbol{c}$ with input $\boldsymbol{c} = (c_0, c_1, c_2, c_3)' \in \mathbb{F}_{2^8}^4$, output $\boldsymbol{r} = (r_0, r_1, r_2, r_3)' \in \mathbb{F}_{2^8}^4$, and the circulant matrix

$$\boldsymbol{T} = \begin{pmatrix} x & (x+1) & 1 & 1 \\ 1 & x & (x+1) & 1 \\ 1 & 1 & x & (x+1) \\ (x+1) & 1 & 1 & x \end{pmatrix} \in \mathbb{F}_{2^8}^{4\times 4},$$

for the polynomial field $\mathbb{F}_{2^8} = \mathbb{F}_2[X]/(x^8 + x^4 + x^3 + x + 1)\mathbb{F}_2[X]$.
Show $(c_3u^3 + c_2u^2 + c_1u + c_0)((x+1)u^3 + u^2 + u + x) \mod (u^4 + 1) = r_3u^3 + r_2u^2 + r_1u + r_0$.