

Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Markus Rothe

Exercise 7

Friday, June 8, 2018

Problem 1. (*AES mix columns*) The step `MixColumns` of the AES scheme is given by $\mathbf{r} = \mathbf{T}\mathbf{c}$ with input $\mathbf{c} = (c_0, c_1, c_2, c_3)' \in \mathbb{F}_{2^8}^4$, output $\mathbf{r} = (r_0, r_1, r_2, r_3)' \in \mathbb{F}_{2^8}^4$, and the circulant matrix

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

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 $(c_3u^3 + c_2u^2 + c_1u + c_0)((x+1)u^3 + u^2 + u + x) \bmod (u^4 + 1) = r_3u^3 + r_2u^2 + r_1u + r_0$.

Problem 2. (*block ciphers are permutations*) A block cipher is a cryptosystem where both plaintext and ciphertext space are the set \mathcal{A}^n of words of length n over an alphabet \mathcal{A} .

- Show that the encryption functions of block ciphers are permutations.
- How many different block ciphers exist if $\mathcal{A} = \{0, 1\}$ and the block length is $n = 6$?

Problem 3. (*determine φ*) Let $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ be the Euler φ -function, i.e., $\varphi(n) = |\mathbb{Z}_n^*|$.

- Determine $\varphi(p)$ for a prime p .
- Determine $\varphi(p^k)$ for a prime p and $k \in \mathbb{N}$.
- Determine $\varphi(p \cdot q)$ for two different primes $p \neq q$.
- Determine $\varphi(4913)$ and $\varphi(899)$.