Homework 5 in Advanced Methods of Cryptography

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

13.11.2012

Exercise 12. 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 $\mathcal{A}$.

(a) Show that the encryption functions of block ciphers are permutations.

(b) How many different block ciphers exist if $\mathcal{A} = \{0, 1\}$ and the block length is $n = 6$?

Exercise 13. Consider the following AES-128 key given in hexadecimal notation:

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

(a) What is the round key K_0?

(b) What are the first 4 bytes of round key K_1?

Exercise 14. Within the step `MixColumns` of the AES algorithm $\mathbf{r} = (r_0, r_1, r_2, r_3)' \in \mathbb{F}_{2^8}^4$, $\mathbb{F}_{2^8} = \mathbb{F}_2[X]/(x^8 + x^4 + x^3 + x + 1)\mathbb{F}_2[X]$, is given by $\mathbf{r} = \mathbf{Tc}$ with $\mathbf{c} = (c_0, c_1, c_2, c_3)' \in \mathbb{F}_{2^8}^4$,

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

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