RWTH AACHEN UNIVERSITY

Lehrstuhl für Theoretische Informationstechnik

Homework 5 in Cryptography

Prof. Dr. Rudolf Mathar, Markus Rothe, Milan Zivkovic

05.06.2014

Exercise 17. Which of the functions IP, E, $\oplus K_i$, S, P in the encryption procedure of the Data Encryption Standard (DES) are linear?
Note: Linearity: $f(a \oplus b) = f(a) \oplus f(b)$.

Exercise 18. Let M be a block of bits of length 64 and let K be a block of bits of length 56. Let $\text{DES}(M, K)$ denote the encryption of M with key K using the DES cryptosystem. $\overline{x}$ denotes the bitwise complement of a block x.

(a) Show that the *complementation property* holds:

$$\text{DES}(M, K) = \overline{\text{DES}(\overline{M}, \overline{K})}$$

(b) How does the complementation property help to attack DES?

Exercise 19. 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 20. 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 21. The step `MixColumns` of the AES scheme is given by $\mathbf{r} = \mathbf{Tc}$ 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 $(c_3u^3 + c_2u^2 + c_1u + c_0)((x+1)u^3 + u^2 + u + x) \mod (u^4 + 1) = r_3u^3 + r_2u^2 + r_1u + r_0$.