Exercise 6 in Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Jose Angel Leon Calvo

2015-06-11

Problem 16. (*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 $\mathcal{A}$.

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 $n = 6$?

Problem 17. (*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 18. (*DES Complementation property*) Let M be a block of bits of length 64 and let K be a block of bits of length 56. Let $\mathrm{DES}(M, K)$ 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:

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

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

Problem 19. (*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 $(c_3u^3 + c_2u^2 + c_1u + c_0)((x+1)u^3 + u^2 + u + x) \mod (u^4 + 1) = r_3u^3 + r_2u^2 + r_1u + r_0$.