Homework 4 in Cryptography I

Prof. Dr. Rudolf Mathar, Paul de Kerret, Georg Boecherer

10.06.2010

Exercise 10. Which of the functions IP, E, $\oplus K_i$, S, P in the encryption procedure of the Data Encryption Standard (DES) are linear?
(A function is said to be linear if $f(X_1 \oplus X_2) = f(X_1) \oplus f(X_2)$ with addition modulo 2.)

Exercise 11. Let M be a block of bits of length 64 and 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. Show that

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

where $\bar{\cdot}$ denotes the bitwise complement.

Exercise 12. There are four so called *weak* DES keys. One of those is the key

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

What happens if you use this key? Can you find the other three weak keys?