

Homework 7 in Cryptography I

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Steven Corroy
08.12.2009

Exercise 19. 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?

Exercise 20. A block cipher is a cryptosystem where plaintext and ciphertext space are the set \mathcal{A}^n of words of length n over an alphabet \mathcal{A} . The number n is called the block length.

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 $n = 6$?

Exercise 21. Consider the following AES-128 key given in hexadecimal notation:

$$K = 2d\ 61\ 72\ 69\ 65\ 00\ 76\ 61\ 6e\ 00\ 43\ 6c\ 65\ 65\ 66\ 66$$

- What is the round key K_0 ?
- What are the first 4 bytes of round key K_1 ?