

---

Prof. Dr. Rudolf Mathar, Dr. Michael Reyer

## Tutorial 6

Friday, May 24, 2019

**Problem 1.** (*AES round key*) 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  $K_1$ ?

**Problem 2.** (*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 3.** (*AES encryption errors*) A sequence of message blocks is encrypted with AES in the modes ECB, CBC, OFB, CFB, and CTR. The ciphertext is sent from Alice to Bob over a channel with random transmission errors.

- a) Bob wants to decrypt the ciphertext. Assume that exactly one bit in one block of the ciphertext changes during transmission. How many bits are wrongly decrypted in the worst case?
- b) What happens, if one bit of the ciphertext is lost or an additional bit is inserted?