

# Homework 1 in Cryptography I

Prof. Dr. Rudolf Mathar, Michael Naehrig

22.10.2007

**Exercise 1.** Decrypt the following ciphertexts and explain your approach. The plaintext messages are in English.

1. Caesar cipher:

sdscsxceppsmsoxddyzbydomdyebcovfocgsdrvkg  
cgoxoondyzbydomdyebcovfocgsdrwkdrowkdsmc

2. Affine cipher:

onhldqrattydxtlgtojkhqtjxctdc

**Exercise 2.** Determine the number of possible keys for the following cryptosystems:

- Substitution cipher,
- Affine cipher with the alphabet  $\Sigma = \mathbb{Z}_{26} = \{0 \dots 25\}$ ,
- Permutation cipher with a fixed blocklength  $k$ .

**Exercise 3.** Let  $e_K$  be one of the ciphers from Exercise 2. Show that encrypting a message  $m$  with key  $K_1$  and the result afterwards with the key  $K_2$  is the same as doing one encryption with a different key  $K_3$ , i.e.

$$e_{K_2}(e_{K_1}(m)) = e_{K_3}(m).$$

Compute the corresponding keys for the concatenation in all three cases.