# Homework 1 in Cryptography I

Prof. Dr. Rudolf Mathar
Wolfgang Meyer zu Bergsten, Michael Reyer
28.10.2008

**Exercise 1.** Consider the following cipher for encrypting a message $\mathbf{m} = (m_1, m_2, \ldots, m_n)$ with the numeric key $k$, where $1 \leq k \leq n$:

$i \leftarrow 1$

`for` $j \leftarrow 1$ `to` $k$

$l \leftarrow 0$

`while` $lk + j \leq n$

$c_i \leftarrow m_{lk+j}$

$l \leftarrow l + 1$

$i \leftarrow i + 1$

`return` $\mathbf{c} = (c_1, \ldots, c_n)$

a) Which classical cipher is described by this algorithm?

b) Encrypt the message "ThisEncryptionSchemeIsNotSafeBecauseAttacksExplainedInTheFollowingLecturesWillBreakIt" with the key $k = 7$.

**Exercise 2.** Decrypt the following ciphertext and explain your approach. The plaintext message is in English.

```
sdscsxceppsmsoxddyzbydomdyebcovfocgsdrvkg
cgoxoondyzbydomdyebcovfocgsdrwkdrowkdsmc
```

**Exercise 3.**

a) Create the tables for addition and multiplication of two numbers $a + b = c \mod 7$ and $a \cdot b = c \mod 7$.

b) Determine the greatest common divisor for the following pairs using the Euclidian algorithm: (72, 40), (31,21) and (720, 123).