



---

# Opdrachten

---

12 februari 2019

*Student:*  
Sander Hansen  
10995080

## 1 Week 1

### 1.1 Exercises 1b

#### 1.1.1 Problem 1: Caesar cipher

(a)  
Hello mister  
7 4 11 11 14 12 8 18 19 4 17  
10 7 14 14 17 15 11 21 22 7 20  
khood plvwlu

#### 1.1.2 Problem 2: Alphabet creation

a  
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
A L P H B E T C R I O N D F G J K M Q S U V W X Y Z

#### 1.1.3 Problem 3: Decimation

Legacy = A B C D E F = 11 22 33 44 55  $\rightarrow$  11 22 7 18 3 = lwbsd  
Modern = A B C D E F = 0 11 22 33 44  $\rightarrow$  0 11 22 7 18 = alwbs

#### 1.1.4 Problem 4: Extended Euclidean Algorithm

Voor het Extended Euclidean Algoritme maak je een tabel van vijf kolommen. De eerste kolom is de index, de tweede de deelsom, de derde de remainder, de vierde  $s_i$  en de laatste  $t_i$ .

Bij index 0 en 1 wordt de quotient leeggelaten, zijn de remainders de getallen waarmee gerekend wordt.  $s_0 = 1, t_0 = 0, s_1 = 0, t_1 = 1$ .

Vervolgens is  $s_i = s_{i-2} - s_{i-1} * \text{quotient}_i$  en  $t_i = t_{i-2} - t_{i-1} * \text{quotient}_i$ .

Als hier de inverse van een modulo van moet worden berekend is de laatste kolom overbodig. Bij bijvoorbeeld  $15 \bmod(26)$  schrijf je alleen  $s_i$  uit.

| Index | Quotient | Remainder | s <sub>i</sub> | t <sub>i</sub> |
|-------|----------|-----------|----------------|----------------|
| 0     |          | 144       | 1              | 0              |
| 1     |          | 55        | 0              | 1              |
| 2     | 144:55=2 | 34        | 1-2*0=1        | 0-1*2=-2       |
| 3     | 55:34=1  | 21        | 0-1*1=-1       | 1-2*1=3        |
| 4     | 34:21=1  | 13        | 1-1*1=2        | -2-3*1=-5      |
| 5     | 21:13=1  | 8         | -1-2*1=-3      | 3-5*1=8        |
| 6     | 13:8=1   | 5         | 2-3*1=5        | -5-8*1=-13     |
| 7     | 8:5=1    | 3         | -3-5*1=-8      | 8-13*1=21      |
| 8     | 5:3=1    | 2         | 5-8*1=13       | -13-21*1=34    |
| 9     | 3:2=1    | 1         | -8-13*1=-21    | 21-34*1=55     |
| 10    | 2:1=2    | 0         |                |                |

### 1.1.5 Problem 5: Playfair cipher

Bij de playfair cipher maak je een 5x5 matrix met een codewoord. Je maakt bigrammen van letters. Diagonalen worden vervangen door tegenovergestelde diagonalen. Op een rij kies je voor de letter direct rechts. In een kolom voor de letter eronder.

Sander wordt dus QC OC BP

### 1.1.6 Problem 6: Hill cipher

Inverse van  
matrix ken-  
nen?

(a)

## 2 Week 2

### 2.1 Exercises 2a

#### 2.1.1 Problem 1: A simple substitution

## 3 Week 3

## 4 Week 4

## 5 Week 5

## 6 Week 6