# Grundlagen Informations Sicherheit
# Übungsblatt 02

Max Kurz (3265240) Mohamed Barbouchi (3233706)
Daniel Kurtz (123456)

## Problem 1

**Algorithm 1** $D(Y)$

send($x_1$)
$y_1$ = receive($y_1$)
send($x_2$)
$y_2$ = receive($y_2$)
$a = (y_1 -_n y_2)/(x_1 -_n x_2)$
$b = y_2 -_n ax_2$
$x_{d1} = D(y_1, (a, b))$
$x_{d2} = D(y_2, (a, b))$
if($x_{d1}$ == $x_1$) $b = 1$ else $b = 0$
return $b$

Die Wahrscheinlichkeit für den Angreifer das richtige $b$ zurrückzugeben und liegt bei 1, da mit dem oben beschrieben Algorithmus das Tupel $(a, b)$ rekonstruiert werden kann.

## Problem 2

## Problem 3

Sei $x, y \in \mathbb{Z}_n$ und $l, k \in \mathbb{Z}$

$$a \equiv x \mod n \implies a = ln +_n x$$
$$b \equiv y \mod n \implies b = kn +_n y$$

$$\begin{aligned} a \cdot b &= (ln + x)(kn + y) \\ &= lkn^2 + lny + kxn + xy \\ &= lkn^2 + n(ly + kx) + xy \equiv x \cdot y \mod n \end{aligned}$$

$\square$

## Problem 4

Assoziativität ist gegeben[1] da $(R, \cdot)$ bereits assozitiv ist. Wir zeigen Abgeschlossenheit, die Existenz von Inversen, und neutralem Element.

### Abgeschlossenheit

$\forall x, y \in R^* \implies \exists x^{-1}, y^{-1} \in R^* : xx^{-1} = 1_R = x^{-1}x,\ yy^{-1} = 1_R = y^{-1}y$

$$\begin{aligned} x \cdot y = z &\implies xyy^{-1} = x1_R = x = zy^{-1} \\ &\implies xx^{-1} = 1 = zy^{-1}x^{-1} \\ &\implies \exists z^{-1} \in R^* : y^{-1}x^{-1} = z^{-1} : zz^{-1} = 1_R \qquad \text{Assoziativität} \\ &\implies z \in R^* \end{aligned}$$

### Inverse

Sei $x \in R$

$$\begin{aligned} &\forall x \in R\ \exists x^{-1} \in R^* : x \cdot x^{-1} = 1_R \\ \implies &\forall x^{-1} \in R^*\ \exists x \in R : x^{-1} \cdot x = 1_R \end{aligned}$$

### Neutrales

Sei $1_R \in R$

$$1_R \cdot 1_R = 1_R \implies 1_R \in R^*$$

$\square$

## Problem 5

Zu zeigen: $a \mid b \implies (x \mod b) \mod a = x \mod a$. Sei $z = (x \mod b)$

$$\begin{aligned} a \mid b \implies b &\mod a = 0 \\ (x \mod b) \mod a = x &\mod a \\ (x \mod b) \equiv x &\mod a \\ z \equiv x &\mod a \end{aligned}$$

Da $(x \mod b) = z$ gilt, und wir $b \mod a = 0$ vorrausetzen können, wissen wir dass für $z = lb + x$ mit $l \in \mathbb{Z}$ gilt.

$$\begin{aligned} lb + x \equiv x &\mod a \\ x = x & \end{aligned}$$

$\square$

[1] $\forall a, b, c \in R^* : a, b, c \in R$

## Problem 6

Sei $a = lb + k$ mit $l, k \in \mathbb{Z}$, und $d = \texttt{ggt}(a, b)$, $e = \texttt{ggt}(b, k)$.
Wir zeigen $d = e$ und somit $\texttt{ggt}(a, b) = \texttt{ggt}(b, a \mod b)$.

**Fall** $d \mid e$

$$
\begin{aligned}
&d = \texttt{ggt}(a, b) \\
&\quad \Longrightarrow \; d \mid a \text{ und } d \mid b \\
&\quad \Longrightarrow \; d \mid (lb + k) \\
&\quad \Longrightarrow \; d \mid (a - lb) \\
&\quad \Longrightarrow \; d \mid k \text{ und } d \mid l \\
&\quad \Longrightarrow \; d \mid e
\end{aligned}
$$

**Fall** $e \mid d$

$$
\begin{aligned}
&e = \texttt{ggt}(b, k) \\
&\quad \Longrightarrow \; e \mid b \text{ und } e \mid k \\
&\quad \Longrightarrow \; e \mid (lb + k) \\
&\quad \Longrightarrow \; e \mid a \\
&\quad \Longrightarrow \; e \mid \texttt{ggt}(a, b) \\
&\quad \Longrightarrow \; e \mid d
\end{aligned}
$$

$\square$