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 $l, k \in \mathbb{Z}$

$$\begin{aligned} a &\equiv x \mod n \implies a = ln +_n x \\ b &\equiv y \mod n \implies b = kn +_n y \end{aligned}$$

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

□

Problem 4

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

Abgeschlossenheit

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

$$\begin{aligned} x \cdot y = z &\implies xyy^{-1} = x1_R = x = zy^{-1} \\ &\implies xx^{-1} = 1 = zy^{-1}x^{-1} \\ &\implies z \in R^* \end{aligned}$$

$\square$

Inverse

Sei $x \in R$

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

$\square$

Neutrales

Sei $1_R \in R$

$$1_R \cdot 1_R^{-1} = 1_R \implies 1_R \in R^*$$

$\square$

Problem 5

Problem 6