

Grundlagen Informations Sicherheit

Übungsblatt 02

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

Problem 1

Algorithm 1 $D(Y)$

```
1: send( $x_1$ )
2:  $y_1 = \text{receive}(y_1)$ 
3: send( $x_2$ )
4:  $y_2 = \text{receive}(y_2)$ 
5:  $a = (y_1 -_n y_2) / (x_1 -_n x_2)$ 
6:  $b = y_2 -_n ax_2$ 
7:  $x_{d1} = D(y_1, (a, b))$ 
8:  $x_{d2} = D(y_2, (a, b))$ 
9: if ( $x_{d1} == x_1$ )  $b = 1$  else  $b = 0$ 
10: return  $b$ 
```

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

Problem 2

Problem 3

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

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

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

□

Problem 4

Assoziativität ist gegeben¹ da (R, \cdot) bereits assoziativ ist. Wir zeigen Abgeschlossenheit, die Existenz von Inversen, und neutralem Element.

Abgeschlossenheit

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

$$x \cdot y = z \implies xyy^{-1} = x1_R = x = zy^{-1}$$

$$\implies xx^{-1} = 1 = zy^{-1}x^{-1}$$

$$\implies \exists z^{-1} \in R^* : y^{-1}x^{-1} = z^{-1} : zz^{-1} = 1_R \quad \text{Assoziativität}$$

$$\implies z \in R^*$$

△

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 $1_R \in R$

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

□

Problem 5

Zu zeigen: $a|b \implies (x \bmod b) \bmod a = x \bmod a$. Sei $z = (x \bmod b)$

$$a|b \implies b \bmod a = 0$$

$$(x \bmod b) \bmod a = x \bmod a$$

$$(x \bmod b) \equiv x \bmod a$$

$$z \equiv x \bmod a$$

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

$$lb + x \equiv x \bmod a$$

$$x = x$$

□

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

Problem 6