Security and Privacy, Blatt 1

Franziska Hutter (3295896)
Felix Truger (3331705)
Felix Bühler (2973410)

29. Mai 2018

Problem 1: Matching Algorithm

Problem 2: Basics - Probability Theory

Problem 3: Basics - Algorithms

a)

b)

c)

d)

Problem 4: Basics - Group Theory

a)

- $(\mathbb{Z}_8^*, \cdot_8)$Nein, da es isomorph zu $\mathbb{Z}_2^* * \mathbb{Z}_2^*$ ist.
  ($\rightarrow$Es besitzt keine Primitivwurzel.)
- $(\mathbb{Z}_{10}^*, \cdot_{10})$ Ja. Generator ist 3 oder 7

Generator = x	3	7
xˆ0	1	1
xˆ1	3	7
xˆ2	9	9
xˆ3	7	3
xˆ4	1	1

b)

Aus der Vorlesung:
$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n | gcd(a, n) = 1\} \rightarrow \mathbb{Z}_n^* = \{a, b \in \mathbb{Z}_n | gcd(a * b, n) = 1\}$
Multiplikation ist ein Gesetz der Komposition auf $\mathbb{Z}_n^*$.

$a, b, c \in \mathbb{Z}_n^*$

- Die Multiplikation ist assoziativ auf $\mathbb{Z}_n^*$: $(a * b) * c = abc = a * (b * c)$
  $(gcd((a * b) * c, n) = 1 = gcd(a * b * c, n) = gcd(a * (b * c), n))$

- Ebenso ist die Multiplikation kommutativ: $a * b = b * a$
  $(gcd(a * b, n) = 1 = gcd(b * a, n))$

- Neutrales Element:

  Wir nehmen als Identität 1. Natürlich ist, $\forall x \in \mathbb{Z} : gcd(1, x) = 1$, also $1 \in \mathbb{Z}_n^*$. Dann $a * 1 = a = 1 * a$. Somit erfüllt 1 die Eigenschaft des neutralen Elements.

- Inverses Element:

  $\forall x \in \mathbb{Z}$: $ax \equiv 1 \pmod{n}$. Es existiert genau dann, wenn a Teilerfremd zu n ist, weil in diesem Fall $gcd(a, n) = 1$. Und nach Bezous existiert somit ein Inverses Element.