

## Aufgabe 2.1

**Vorgehensweise** Um die Aufgaben zu bearbeiten, betrachten wir zunächst die Definition aus der Vorlesung, um zu prüfen, ob die Anforderungen an eine Hashfunktion erfüllt sind:

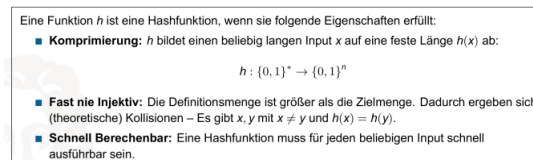


Abbildung 1: Definition Hashfunktion

Im Anschluss betrachten wir die erweiterte Definition aus der Vorlesung für kryptografische Hashfunktionen, die aus folgenden Eigenschaften besteht:

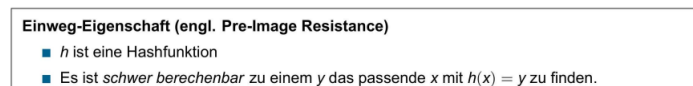


Abbildung 2: Einweg-Eigenschaft

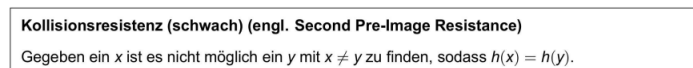


Abbildung 3: Kollisionsresistent Schwach

a)  $h(x) = x \bmod 7$

**Komprimierung:**

Ist erfüllt, da wir durch das Modulo 7, egal wie hoch die Eingabe ist, eine Zahl zwischen 0 und 6 erhalten werden.

**Fast nie injektiv:**

Ist erfüllt, die mögliche Definitionsmenge ( $=\infty$ ) ist für diese Funktion als größer anzusehen, verglichen mit der Zielmenge (0,1,2,3,4,5,6).

**Schnell berechenbar:**

Ist erfüllt, da es sich beim Modulo um eine einfache Rechenoperation handelt, ist diese auch schnell berechenbar.

Da wir gezeigt haben, dass es sich um eine Hashfunktion handelt, müssen wir nur noch die Kriterien für eine kryptografische Hashfunktion prüfen.

**Einweg-Eigenschaft:**

Ist nicht erfüllt, es ist möglich die Funktion umzukehren, um dann durch Ausprobieren zum  $x$  zu gelangen. Die Funktion dazu lautet **Kollisionsresistent Schwach:**

**Kollisionsresistent Stark:**

b)

$$g(x) = x \bmod 12$$

**Kollisionsresistenz (stark) (engl. Collision Resistance)**  
Es ist nicht möglich ein  $x, y$  mit  $x \neq y$  zu finden, sodass  $h(x) = h(y)$ .

#### Abbildung 4: Kollisionsresistent Stark

Zunächst überprüfen wir, ob es sich bei der Funktion um eine Hashfunktion handelt. Dazu betrachten wir die oben beschriebenen Kriterien.

**Komprimierung:**

Ist erfüllt, da wir durch das Modulo 7, egal wie hoch die Eingabe ist eine Zahl zwischen 0 und 6 erhalten werden.

**Fast nie injektiv:**

Ist erfüllt, die mögliche Definitionsmenge ( $=\infty$ ) ist für diese Funktion als größer anzusehen, verglichen mit der Zielmenge (Zahlen zwischen 0 und 11).

**Schnell berechenbar:**

Ist erfüllt, da es sich beim Modulo um eine einfache Rechenoperation handelt, ist diese auch schnell berechenbar. Da wir gezeigt haben, dass es sich um eine Hashfunktion handelt, müssen wir nur noch die Kriterien für eine kryptografische Hashfunktion prüfen.

**Einweg-Eigenschaft:**

**Kollisionsresistent Schwach:**

**Kollisionsresistent Stark:**

### Aufgabe 2.2

### Aufgabe 2.3

### Aufgabe 2.4

### a) b) c) d) Aufgabe 2.5