

Problem Set 1  
**Cryptographic Hash Functions**  
(Summer Term 2019)

Bauhaus-Universität Weimar, Chair of Media Security

Prof. Dr. Stefan Lucks, Nathalie Dittrich

URL: <http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching/>

**Due Date:** 18 April 2019, 11:00 AM, via email to [eik.list@uni-weimar.de](mailto:eik.list@uni-weimar.de).

*Note: For all tasks, explain your solutions in brief in your own words. You can work in groups of at most **three students**. Only one write-up per group is required. The use of  $\text{\LaTeX}$  is recommended; a  $\text{\LaTeX}$  template file can be found on the website of the problem session.*

**Goal of this Problem Set:** Basics of hash functions.

**Task 1 – Division Method (4 Credits)**

For  $p = 2857$  and for inputs  $x_i \in \mathbb{Z}_p$ , let

$$H(x_1, \dots, x_m) \stackrel{\text{def}}{=} \left( \sum_{i=1}^m 2^{m-i} \cdot x_i \right) \bmod p$$

be the division-method hash function as given on Slide 8 of Chapter 1. Solve the following tasks for  $m = 2$  and  $m = 3$ .

- a) Find  $x$  with  $H(x) = 1$ .
- b) Find some  $(x, x')$  with  $x \neq x'$  that collide:  $H(x) = H(x')$ .
- c) Find  $x$  with  $H(x) = 0$ .
- d) Find  $x$  with  $H(x) = 42$ .

**Task 2 – Collision and Preimage Resistance (6 Credits)**

Let  $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$  be a secure cryptographic hash function. Let  $\text{const} \in \{0, 1\}^n$  denote a public constant,  $\bar{x}$  the bitwise inverse of  $x$ , and  $x \parallel y$  the concatenation of  $x$  and  $y$ .

Recall the security definitions on Slide 12 of Chapter 1. For each of the following functions  $H'$ , say if, and explain briefly why,  $H'$  is collision-resistant or not, preimage-resistant or not, and second-preimage-resistant or not.

- a)  $H'(x) \stackrel{\text{def}}{=} H(x) \parallel x$
- b)  $H'(x) \stackrel{\text{def}}{=} H(\text{const}) \oplus x$
- c)  $H'(x) \stackrel{\text{def}}{=} H(x) \parallel \overline{H(x)}$
- d)  $H'(x) \stackrel{\text{def}}{=} H(\bar{x})$

e)  $H'(x) \stackrel{\text{def}}{=} H(x \oplus \text{const})$

f)  $H'(x, y) \stackrel{\text{def}}{=} H(x) \oplus H(y)$

**Task 3 – Product Hash (3 Credits)**

Let  $p = 61$  and let  $H$  be a keyed hash function with  $k_1, k_2 \in \mathbb{Z}_p$  for inputs  $x_1, x_2 \in \mathbb{Z}_p$ :

$$H_{k_1, k_2}(x_1, x_2) \stackrel{\text{def}}{=} (k_1 + x_1) \cdot (k_2 + x_2) \bmod p.$$

Say, Eve has eavesdropped the following three inputs  $(x_1, x_2)$  and their corresponding hashes. Recover the secret key  $(k_1, k_2)$ .

$$H_{k_1, k_2}(20, 10) = 34$$

$$H_{k_1, k_2}(6, 8) = 11$$

$$H_{k_1, k_2}(5, 3) = 49$$