1. Problem Session
Cryptographic Hash Functions
(Summer Term 2014)

Bauhaus-Universität Weimar, Chair of Media Security
Prof. Dr. Stefan Lucks, Jakob Wenzel
URL: `http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching/`

Date: 08.04.2014 (15:15)

Task 1 (6 Credits)
Let $h(X)$ be a hash function which uses the division method (see Slide 8 of Section 1.1). Solve the following tasks, where $m = 1$ and $p = 2857$.

a) Find X with $h(X) = 1$.

b) Given $X = (00110011001100)_2$, find $h(X)$.

c) Find any $X' \neq X$ with $h(X) = h(X')$.

d) Find X with $h(X) = 0$.

e) Find X with $h(X) = 5$.

f) Find a 2nd-Preimage of $h(1001011)$ with $p = 17$.

Task 2 (6 Credits)
Let $h : \{0,1\}^* \to \{0,1\}^n$ be a cryptographically secure hash function (see Slide 11 of Section 1.2). Say for each of the following hash function constructions h' if it is **collision resistant, preimage resistant, or 2nd-preimage resistant**. If a construction does not satisfy one or more of these requirements, provide a **simple attack**, each.

a) $h'(X) = h(X) \mid\mid X$

b) $h'(X) = h(X) \mid\mid const$

c) $h'(X) = h(X) \oplus \overline{h(X)}$

d) $h'(X) = h(X \oplus 1^n)$

e) $h'(X) = h(const)$

f) $h'(X, Y) = h(X) \oplus h(Y)$

Note that $X \mid\mid Y$ denotes the concatenation of the values X and Y, *const* denotes a fixed constant value, and $\overline{X}$ the inverse of X.

Task 3 (4 Credits)
Show that the following hash function is **not collision resistant**, *i.e.,* find two pairs (a, x) and (a', x'), so that $h(a, x) = h(a', x')$.

$$h(a, x) = x^a \bmod n,$$

where x describes the input message with $x \in \mathbb{Z}_n^*$, n is an arbitrarily large number with $n > 2$, and the value a is chosen so that $x > a$ and $2 < a < n$ hold.