2. 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: 22.04.2014 (15:15)

Task 1 (4 Credits) Weak Hash Function Designs I
Consider a hash function $h : \{0,1\}^{1024} \to \{0,1\}^{256}$ that satisfies the following property:

$$\mathrm{Par}(x) = \mathrm{Par}(h(x)), \quad \text{for all } x \in \{0,1\}^{1024}, \tag{1}$$

where the parity Par of an n-bit string $x = x_1, \ldots, x_n$ is defined by

$$\mathrm{Par}(x) = x_1 \oplus x_2 \oplus \cdots \oplus x_n.$$

Example: Par(10010011011) = 0 and Par(10011101) = 1.

a) Explain how one can take advantage of Property (1) in order to mount a preimage attack. Approximate the complexity of the attack.

b) Note that, based on the birthday paradox, the success probability of an adversary in finding a collision, when asking at most q queries to an oracle, can be approximated by

$$\frac{q^2}{2^{n+1}}.$$

Show how one can use Property (1) to find a collision on h. Compute the number of distinct elements of $\{0,1\}^{1024}$ that are needed by this method to reach a success probability for a collision of 0.90.

Task 2 (4 Credits) Weak Hash Function Designs II
Consider a hash function $h : \{0,1\}^{2048} \to \{0,1\}^{256}$ satisfying the following property:

$$x \equiv x' \bmod 2^{64} \quad \Longrightarrow \quad h(x) = h(x'). \tag{2}$$

a) Let $Y \overset{\$}{\leftarrow} \{0,1\}^{256}$ be a randomly and uniformly chosen value. Compute an upper bound on the probability that Y has a preimage for h.

b) How does Property (2) influence the *2nd-preimage-security* of h?

c) How does Property (2) influence the *collision-security* of h?

Task 3 (4 Credits) k-Collisions
Let $h : \{0,1\}^* \to \{0,1\}^n$ be a cryptographically secure hash function. We denote by $h(x_1) = h(x_2)$ with $x_1 \neq x_2$ a 2-collision for h, and by $h(x_1) = h(x_2) = h(x_3)$ a 3-collision, where $x_1, \ldots, x_3$ are pairwise distinct. Approximate the success probability of an adversary that wants to find k-collisions for arbitrary values of k.

Task 4 (5 Credits) Programming Task

Write a program in Python that searches for a collision for the hash function SHA-512 ($n = 512$ bits output size). Since the success probability for a collision is given by $2^{512/2} = 2^{256}$ (due to the birthday attack), a collision for the full output is highly unlikely. Thus, try to find a collision for the first k bytes of the hash values, with k much smaller than n. Furthermore, measure the time your program is running.

Note 1: You can use the `hashlib` library for this task (see `https://docs.python.org/2/library/hashlib.html`).

Note 2: Send me the source code and the input messages that lead to the largest value of k via E-Mail to `jakob.wenzel(at)uni-weimar.de` **until 21.04.2014**. The group with the largest value of k gets a bag of gummi bears :-)