6. 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: 17.06.2014 (15:15)

Task 1 (2+2 Credits) Differential Cryptanalysis of Variants of CubeHash
In the course CubeHash was introduced as one of the SHA-3 candidates. Now, consider two variants CubeHash* and CubeHash**, which have a slightly different round function (see Slide 144 in Section 7.3 for the original round function).

CubeHash*: The rotations (Steps 2 and 7) are omitted.

CubeHash:** The swap operations (Steps 3, 5, 8, and 10) are omitted.

Explain how these changes influence the security of the particular round functions regarding to differential cryptanalysis and the existence of symmetric states.

Task 2 (3+5 Credits) Differential Cryptanalysis of BLAKE
Consider the round function G of BLAKE-256 as given on Slide 162 in Section 7.5. The rotation amounts are given on the slide and applied from left to right (see also `https://131002.net/blake/blake.pdf` for a more formal specification of G). Now, consider a slightly changed variant G' which consists of two consecutive applications of G, where four message words M_0, M_1, M_2, and M_3 are injected in their natural order.

Find and describe a differential characteristic with a high probability for G' for the following two cases:

a) You are allowed to choose the input chaining values a, b, c, and d.

b) The values a, b, c, and d are fixed constant values.

For simplicity, it is sufficient to assume at most one active bit per message word M_i for $0 \leq i \leq 3$.

Task 3 (4 Credits) Differential Cryptanalysis of Skein*
Consider the hash function Skein*-256 which is a modified variant of the SHA-3 finalist Skein-256, where the rotation constants within Threefish are set to zero. The Mix-Function of Skein*-256 is thus given by:

$$Mix(L, R) = (X, Y) \text{ with } X = L \boxplus R \text{ and } Y = R \oplus X.$$

The values L, R, X, Y are all 64-bit integers (unsigned). Find a non-zero 72-round differential characteristic with reasonable probability for Skein*-256.

Task 4 (5 Credits) Programming Task (Python)
Implement a variant of the internal function of Skein-256 (Threefish with 72 rounds, where each round consists of one application of the Mix function) and check for the best possible differential characteristic depending on the input differences and the rotation constant. The variation to the original Threefish function is given by assuming the rotation constant to be the same for each call to Mix. Thus, your program should fulfill the following tasks:

- For all possible one-bit input differences (256 possible):
  - check for the best differential characteristic (highest probability) depending on the rotation constant (64 possible)
  - output the maximum number of rounds which can be reached using this input difference and the particular rotation constant
  - output the probability for this path

Hint: The upper bound on the probability for a differential characteristic for Skein-256 is given by 2^{-255}. Thus, if the probability for a differential characteristic after r rounds would become $< 2^{-255}$, one can stop the computation and output this characteristic with the maximum number of $r - 1$ rounds.