Advanced Cryptography: Algorithmic Cryptanalysis

DANIEL LOEBENBERGER, KONSTANTIN ZIEGLER

6. Exercise sheet
Hand in solutions until Saturday, 21 May 2011, 23:59h.

To estimate the average effort you put into solving the following exercises, please add after each exercise the amount of time you spent for it.

Exercise 6.1 (Merkle-Damgård). (5 points)

Prove the Merkle-Damgård Theorem. 5

In other words, show that a collision for the hash-function yields a collision for the compression function. Distinguish the two cases: colliding messages of equal and of different length.

Exercise 6.2 (Trees as mode of operation). (9 points)

Let $h_0 \colon \{0,1\}^{2m} \to \{0,1\}^m$ be a collision-resistant hash function with $m \in \mathbb{N}_{>0}$.

(i) We construct a hash function $h_1 \colon \{0,1\}^{4m} \to \{0,1\}^m$ as follows: Interpret the bit string $x \in \{0,1\}^{4m}$ as $x = (x_1|x_2)$, where both $x_1, x_2 \in \{0,1\}^{2m}$ are words with $2m$ bits. Then compute the hash value $h_1(x)$ as 3

$$h_1(x) = h_0(h_0(x_1)|h_0(x_2)).$$

Show: h_1 ist collision-resistant.

(ii) Let $i \in \mathbb{N}$, $i \geq 1$. We define a hash function $h_i \colon \{0,1\}^{2^{i+1}m} \to \{0,1\}^m$ recursively using h_{i-1} in the following way: Interpret the bit string $x \in \{0,1\}^{2^{i+1}m}$ as $x = (x_1|x_2)$, where both $x_1, x_2 \in \{0,1\}^{2^i m}$ are words with $2^i m$ bits. Then the hash value $h_i(x)$ is defined as 1

$$h_i(x) = h_0(h_{i-1}(x_1)|h_{i-1}(x_2)).$$

Show: h_i is collision-resistant.

(iii) The number $p = 2027$ is prime. Now define $h_0 : \{0,1\}^{22} \to \{0,1\}^{11}$ as follows: Let $x = (b_{21}, \ldots, b_0)$ be the binary representation of x. Then $x_1 = \sum_{0 \leq i \leq 10} b_{11+i} 2^i \bmod p$ and $x_2 = \sum_{0 \leq i \leq 10} b_i 2^i \bmod p$. Show that the numbers 5 and 7 have order $p-1$ modulo p. Now compute $y = 5^{x_1} \cdot 7^{x_2} \bmod p$ and let $h_0(x) = (B_{10}, \ldots, B_0)$ be the binary representation of y, i.e. $y = \sum_{0 \leq i < 11} B_i 2^i$. Use the birthday attack to find a collision of h_0 and of h_1 defined as described in (i). 5

Note: "|" denotes the concatenation of bit strings.

Exercise 6.3 (Bias of the SHA-functions). (4 points)

4

Consider the two non-linear functions MAJ and IF restricted to three bits input (and one bit output). Compute the respective bias.

Exercise 6.4 (SHA-3 finalists). (0+5 points)

+5

Pick three of the five SHA-3 finalists. Find a proper reference for them, and list possible in- and output sizes for the round function. Draw (do not copy (!)) a really nice picture of the state update for one of them with proper labels on the involved variables.