Cryptography, winter 2014/2015

PD Dr. Adrian Spalka, Dr. Daniel Loebenberger

4. Exercise sheet
Hand in solutions until
Wednesday, 26 November 2014, 23:59:59

Exercise 4.1 (Birthday? Paradox!). (12 points)

We again turn to the birthday problem, which is the content of the following theorem.

Theorem. *Consider an urn containing N numbered, distinct balls. Randomly drawing balls and putting each one back right away, on average it takes $O(\sqrt{N})$ rounds until one ball is drawn for the second time.*

Prove the theorem as follows.

(i) Show: For $x \in \mathbb{R}$ holds $1 - x \leq e^{-x}$. Hint: Taylor expansion. If you do not remember it, look it up. [2]

(ii) Let B_i be the number on the ith ball. Show that for any i we have [2]

$$\text{prob}\left(B_i \notin \{B_1, \ldots, B_{i-1}\} | \#\{B_1, \ldots, B_{i-1}\} = i-1\right) = 1 - \frac{i-1}{N}.$$

(iii) Denote by the random variable S the number of rounds until one of the balls is drawn for the second time. Then [3]

$$\text{prob}(S \geq j) = \prod_{i=1}^{j-1} \text{prob}\left(B_i \notin \{B_1, \ldots, B_{i-1}\} | \#\{B_1, \ldots, B_{i-1}\} = i-1\right).$$

Show: $\text{prob}(S \geq j) \leq e^{-(j-2)^2/2N}$.

(iv) For the expected number of rounds we can compute [5]

$$E(s) = \sum_{j \geq 1} j \cdot \text{prob}(S = j) = \sum_{j \geq 1} \text{prob}(S \geq j).$$

Show that this is less or equal than $2 + \sqrt{\frac{\pi}{2}}\sqrt{N}$. Hint: You may use without a proof that $\int_0^\infty e^{-x^2}\, dx = \sqrt{\pi}/2$.

Exercise 4.2 (MERKLE-DAMGÅRD construction). (4 points)

Modify h^* in the MERKLE-DAMGÅRD construction as follows:

2 (i) Drop the last y_i and show how to construct a collision for h^* without having one for h.

2 (ii) Omit the final bit for all y_j and show how to construct a collision for h^* without having one for h, but with the assumption that $h(0 \dots 0) = 0 \dots 0$.

Exercise 4.3 (Trees as mode of operation). (7 points)

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

3 (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

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

Show: h_1 ist collision-resistant.

1 (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

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

Show: h_i is collision-resistant.

3 (iii) Discuss pros and cons of this construction. Also compare to the MERKLE-DAMGÅRD construction.