Cryptography, winter term 16/17: Assignment 8

Prof. Markus Bläser, Cornelius Brand, Marc Roth
http://www-cc.cs.uni-saarland.de/course/55/

Due January 11th, 2017

Exercise 8.1 (Be nice to your tutors and TAs, 1 Bonus Point) Write the name and matriculation number of every author as well as number, time slot and the name of the tutor of your tutorial group on the first page of your solution. Furthermore write in english and staple *all* sheets of your solution.

Exercise 8.2 (Hash functions, 2+2+2 Points) Let (Gen_1, H_1) and (Gen_2, H_2) be hash functions from which *at least one* is collision-resistant. Decide for the following constructions whether the resulting hash function is *necessarily* collision-resistant [1] and prove your answer.

(a) $H_a^{(s_1,s_2)}(x) := H_1^{s_1}(x)||H_2^{s_2}(x)$

(b) $H_b^{(s_1,s_2)}(x) := H_1^{s_1}(H_2^{s_2}(x))||H_2^{s_2}(H_1^{s_1}(x))$

(c) $H_c^{(s_1,s_2)}(x) := H_1^{s_1}(H_2^{s_2}(x)||x)||H_2^{s_2}(H_1^{s_1}(x)||x)$

Exercise 8.3 (Random-Oracle model, 2+2+2 Points) Let (Gen, H) be a collision-resistant hash function with inputs of arbitrary size. We define a MAC for arbitrary-length messages by

$$\mathrm{Mac}_{s,k}(m) = H^s(k||m)\,.$$

(a) Show that this is not a secure MAC if H is constructed by the Merkle-Damgard transform. (We assume that s is known to the attacker.)

(b) Show that this MAC is secure if H is modeled as a random oracle.
Hint: You do *not* need to prove this by hand. Instead, use a property of random oracles that was introduced in the lecture and the canonical construction of a MAC (Theorem 4.6).

(c) Explain *briefly* the consequences of (a) and (b) for the soundness of the Random-Oracle model.

Exercise 8.4 (One-way functions and hard-core predicates, 2+2 Points) Let f be a length-preserving one-way function. Define the function $g(x_1, x_2) = (x_1, f(x_2))$, where $|x_1| = |x_2|$.

(a) Show that g is one-way as well.

(b) Show that if f has a hard-core predicate, then so has g.

[1] In each case we assume that Gen runs Gen_1 and Gen_2 to obtain a key (s_1, s_2).