Prof. Dr. Johannes Blömer
Nils Löken, Fabian Eidens

June 21st, 2016
submission due: June 10th, 2016: 11 a.m.

Cryptographic Protocols

SS 2016

Handout 2

Exercises marked (*) or (**) will be checked by tutors.
We encourage submissions of solutions by small groups of up to four students.

Exercise 1:
Consider Lamport's one-time signature scheme. Show that the scheme does not provide existential unforgeability under chosen message attacks.

Exercise 2 (4 points)**:**
(**) Let (Gen_1, H_1) and (Gen_2, H_2) be two hash functions. Define (Gen, H) so that Gen runs Gen_1 and Gen_2 in order to obtain keys s_1 and s_2 respectively. Then define

$$H^{s_1,s_2}(x) = \langle H_1^{s_1}(x), H_2^{s_2}(x) \rangle$$

- Prove that if at least one of the functions is collision resistant, then (Gen, H) is also collision resistant.
- Determine whether an analogous claim holds for second pre-image resistance and pre-image resistance respectively. Prove your answer in each case.

Exercise 3 (4 points)**:**
(*) Prove the following statements:

- Collision resistant hash functions are not necessarily one-way.
- One-way functions are not necessarily collision resistant.

Remark: Full points can only be awarded if solutions for both statements are submitted.