Prof. Dr. Johannes Blömer
Nils Löken

June 23rd, 2017
submission due: July 4th, 2017: 11 a.m.

Cryptographic Protocols

SS 2017

Handout 1

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

Exercise 2:
Consider Lamport's one-time signature scheme. Show that the scheme does not provide existential unforgeability under chosen message attacks.

Exercise 3 (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. Define

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

a) Prove that if at least on of the hash functions is collision resistant, then (Gen, H) is also collision resistant.

b) Determine whether an analogous claim holds for second pre-image resistance. Prove your answer.

c) Determine whether an analogous claim holds for pre-image resistance. Prove your answer.

Exercise 4:
Prove that collision resistant hash functions are not necessarily one-way functions.

Exercise 5 (4 points)**:**
(*) Prove that one-way functions are not necessarily collision resistant.