

## Problem Set 10

We will work on the following exercises together during the work sessions on Friday, 13 October 2017.

You are strongly encouraged to work together on the exercises, including the homework. You do not have to hand in solutions to these problem sets.

### Problem 1: Man-In-The-Middle Attacks

Describe in detail a man-in-the-middle attack on the Diffie-Hellman key-exchange protocol whereby the adversary ends up sharing a key  $k_A$  with Alice and a (different) key  $k_B$  with Bob, and Alice and Bob cannot detect that anything has gone wrong. What happens if Alice and Bob try to detect the presence of a man-in-the-middle adversary by sending each other (encrypted) questions that only the other party would know how to answer?

### Problem 2: Key Exchange with Bit Strings

Consider the following key-exchange protocol:

1. Alice chooses  $k, r \leftarrow \{0, 1\}^n$  at random, and sends  $s := k \oplus r$  to Bob.
2. Bob chooses  $t \leftarrow \{0, 1\}^n$  at random and sends  $u := s \oplus t$  to Alice.
3. Alice computes  $w := u \oplus r$  and sends  $w$  to Bob.
4. Alice outputs  $k$  and Bob computes  $w \oplus t$ .

Show that Alice and Bob output the same key. Analyze the security of the scheme (i.e., either prove its security or show a concrete attack).