Prof. Martin Hofmann
Dr. Ulrich Schöpp

Ludwig-Maximilians-Universität München
Institut für Informatik
Summer 2017

# Cryptography

Exercise Sheet 10

**Exercise 10-1** Prove that hardness of the Decisional Diffie-Hellman problem (DDH) implies hardness of the Discrete Logarithm Problem.

**Exercise 10-2** The RSA hardness assumption states that $P(\mathsf{RSA\text{-}inv}_{\mathcal{A}}(n) = 1) \leq \mathit{negl}(n)$ for any probilistic polynomial time adversary $\mathcal{A}$.

Show that the RSA hardness assumption implies that factoring is hard in the following sense: No probabilistic polynomial time adversary $\mathcal{B}$ can succeed in the following factoring experiment with non-neglible probability.

1. Randomly generate two primes $p$ and $q$ and let $N := p \cdot q$.
2. Adversary $\mathcal{B}$ is given $N$ and returns two numbers $p'$ and $q'$.
3. The adversary succeeds in the experiment if $p' \cdot q' = N$.

**Exercise 10-3** For any given pseudorandom function $F$, one can attempt to define a hash function $(\mathsf{Gen}, H)$ by letting $\mathsf{Gen}(n)$ be a random string $s$ of length $n$ and defining $H_s(x) := F_s(x)$. Would this definition always produce a collision-resistant hash function?