Modern Cryptography	Dec 11, 2018

Homework 10

Lecturer: Daniel Slamanig, TA: Karen Klein — *Due: 23.59 CET, Dec 19, 2018*

To get credit for this homework it must be submitted no later than Wednesday, December 19th via email to `michael.walter@ist.ac.at`, please use "MC18 Homework 10" as subject.
Please put your solutions into a single pdf file[1] and name this file Yourlastname_HW10.pdf.

1. DL-related Problems

   - **[8.15 in book, 2nd edition]** Prove that hardness of the CDH problem relative to $\mathcal{G}$ implies hardness of the discrete-logarithm problem relative to $\mathcal{G}$, and that hardness of the DDH problem relative to $\mathcal{G}$ implies hardness of the CDH problem relative to $\mathcal{G}$.
   - **[8.19 in book, 2nd edition]** Can the following problem be solved in polynomial time? Given a prime p, a value $x \in \mathbb{Z}_{p-1}^*$, and $y := [g^x \bmod p]$ (where g is a uniform value in $\mathbb{Z}_p$), find g, i.e., compute $y^{1/x} \bmod p$. If your answer is "yes", give a polynomial-time algorithm. If your answer is "no", show a reduction to one of the assumptions introduced in lecture 10.
   - Let G be a cyclic group of prime order q and g a generator. The square Diffie-Hellman (sq-DH) problem is given (G, q, g, g^a) for $a \in \mathbb{Z}_q^*$ to compute g^{a^2}. Show that sq-DH $\iff$ CDH (Hint: $(x + y)^2$).

2. Key-Exchange

   - Let p be a prime and g be a generator of $\mathbb{Z}_p^*$. Argue why we are not able to prove $\widehat{\mathsf{KE}}_{\mathcal{A},\Pi}^{\mathsf{eav}}$ security of the Diffie Hellman key-exchange protocol in this setting. Construct a polynomial-time distinguisher (Hint: quadratic residues).

[1] If you don't know how to do it, you can use e.g. `https://www.pdfmerge.com/`