Lehrstuhl für
Theoretische Informationstechnik

RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

Homework 7 in Cryptography II

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten

26.06.2008

Excercise 18. Let G be a finite Abelian group and $g_1, g_2 \in G$. Let e_1 and e_2 be positive integers. Describe a "square-and-multiply"-like algorithm for the efficient computation of $g = g_1^{e_1} g_2^{e_2}$.

This algorithm should not compute g by multiplying $g_1^{e_1}$ and $g_2^{e_2}$. Instead, use a table of precomputed values $g_{b_1,b_2} = g_1^{b_1} g_2^{b_2}$, $b_1, b_2 \in \{0, 1\}$.

Exercise 19. Discuss the following properties of the Lamport protocol:

- Show that the one-way function is not required to be secret.
- Which properties must a hash function fullfil to be useable as a one-way function in the protocol?
- Propose a function that could be used as the one-way function, assuming that the discrete logarithm is hard to solve in $\mathbb{Z}_p^*$ for a useable p. Describe the Lamport protocol for this special case.
- How can an attacker get access to a one-time password using an active attack?