Homework 9 in Cryptography II

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Steven Corroy

06.07.2010

Exercise 25.

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 $g_2^{e_2}$.

Hint: 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 26.

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?

Exercise 27.

Construct a Challenge-Response-Protocol allowing Alice and Bob to authenticate each other. The protocol should be based on public key cryptography. Is it possible to construct such a protocol without a hash function and only 3 rounds of communication?