Exercise 29. 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 30. 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 fulfill to be useable as a one-way function in the protocol?
- Propose a function that could be used as a one-way function, assuming that the discrete logarithm problem 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?