Homework 10 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Georg Bocherer

21.12.2010

Exercise 32. Read *Leslie Lamport, Password authentication with insecure communication, Communications of ACM 24 (11), pp. 770–771.* You can find this document under the name `Lamport1981.pdf` on L^{2}P.

Exercise 33. 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 34. 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?