Exercise 9 in Advanced Methods of Cryptography
Prof. Dr. Rudolf Mathar, Henning Maier, Markus Rothe
2015-01-09


Problem 29. (Lamports protocol) Discuss the following properties of Lamport’s protocol:

a) Show that the one-way function is not required to be secret.

b) Which properties must a hash function fulfill to be usable as a one-way function in the protocol?

c) 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 usable $p$. Describe Lamport’s protocol for this special case.

d) How can an attacker get access to a one-time password using an active attack?

Problem 30. (attacks on identification schemes)

a) Describe a replay attack for a fixed password identification. Propose a simple identification scheme to prevent this attack.

b) The following challenge-response mutual authentication protocol is given

1) $A \rightarrow B : r_A$
2) $A \leftarrow B : E_K(r_A, r_B)$
3) $A \rightarrow B : r_B$

Explain how an eavesdropper $E$ can authenticate to $A$ without knowing the symmetric key $K$. This a reflection attack. Propose an improved protocol.

c) The following challenge-response protocol based on digital signatures is given

1) $A \rightarrow B : r_A$
2) $A \leftarrow B : r_B, S_B(r_B, r_A, A)$
3) $A \rightarrow B : r'_A, S_A(r'_A, r_B, B)$

Explain how an eavesdropper $E$ can authenticate to $B$ without signing any message with his own identity. This is an interleaving attack.
Problem 31.  

(Christmas exercise)

WOBBIMRBSCD WKCKXNKRKZZIXOGIOKB