

Homework 7 (due on June 1)

This homework set consists of 2 exercises.

By this point in the quarter you may want to focus on your final project. This homework set should not take much time. Please keep your answers short.

Exercise 1:

Suppose that A and B are two principals that want to establish a shared secret K_{AB} . They initially have shared keys K_{AS} and K_{BS} with a server S and they invent nonces N_A and N_B , respectively. The server S invents K_{AB} for them. In order to save state, S has a secret key K_S , gives K_{AB} encrypted under K_S to A , and forgets K_{AB} and all other ingredients of the particular session until B reminds S about them. Their messages are:

$A \rightarrow S : A, B, N_A$

$S \rightarrow A : \{B, N_A, K_{AB}\}_{K_{AS}}, \{B, N_A, K_{AB}\}_{K_S}$

$A \rightarrow B : A, \{B, N_A, K_{AB}\}_{K_S}$

$B \rightarrow S : A, B, N_B, \{B, N_A, K_{AB}\}_{K_S}$

$S \rightarrow B : \{A, N_B, K_{AB}\}_{K_{BS}}$

After this, A may for example send data to B encrypted under a key derived from K_{AB} .

Exercise 1 (cont.):

- a) Briefly explain how an attacker C can impersonate A , that is, break the protocol so that B is convinced that it shares a secret with A when in fact C knows the secret. As usual, C may intercept messages, etc., but does not a priori know how to break the underlying cryptosystem.
- b) Briefly explain a simple, minimal fix.

Exercise 2:

This exercise concerns the applied pi calculus, with the unary symbol h , and no equations.

Let

$$P_0 = (\nu k)\bar{d}\langle h(k)\rangle.\bar{e}\langle k\rangle.nil$$

$$P_1 = (\nu k)\bar{d}\langle h(h(k))\rangle.\bar{e}\langle k\rangle.nil$$

- a) Briefly explain what P_0 does (in other words, paraphrase it in an English sentence).
- b) Argue that P_0 and P_1 are not equivalent. A one-line answer with the definition of a test that distinguishes them is sufficient.