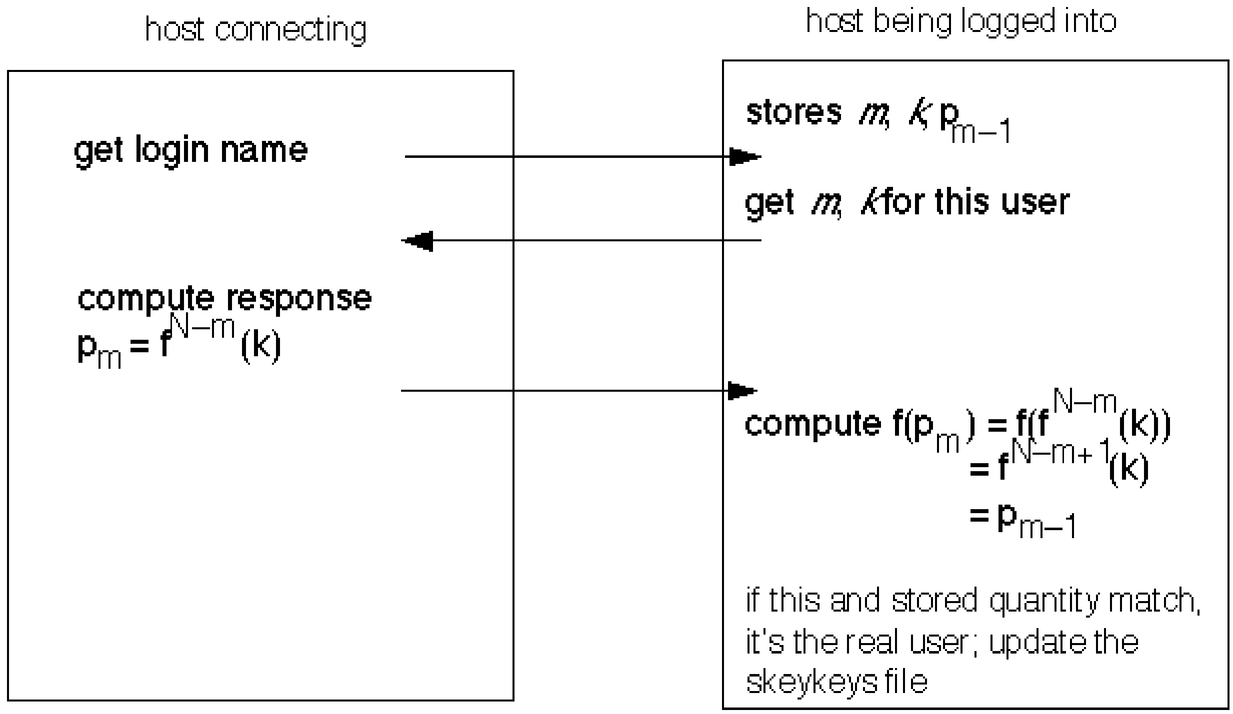
The S/Key Protocol

The S/Key login protocol is summarized in the following picture:



The host being logged into stores the sequence number m, the seed k, and the previously used hash p_{m-1} in the skeykeys file (which is world readable). In what follows, the *remote host* is the host being connected to and the *local host* is the host on which the user is working. The protocol proceeds as follows:

local host. Send login name to remote host.

remote host. Send m and k to local host.

local host. Hash the S/Key password and k $N-m$ times, where N is the number of one-time passwords that have been generated. Send this value, called X, to the remote host.

remote host. Hash X once. If the result is the stored p_{m-1}, the user has authenticated himself or herself correctly. Store X in the skeykeys file. If the result is not the stored $pm-1$, the user has not authenticated properly and access is denied.