Exercise 9

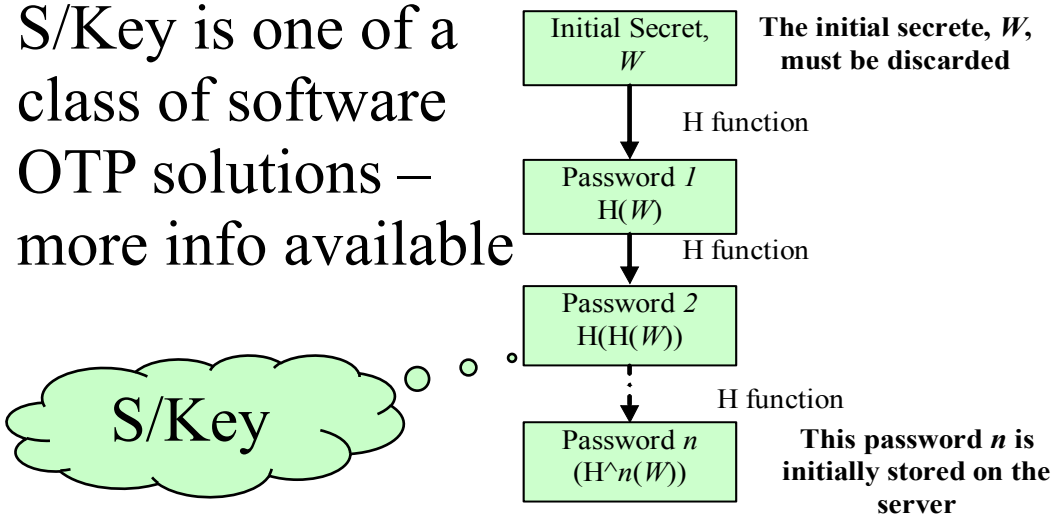
(a) You are given a hash function, and are asked to design a password based OTP (One Time Password) solution. You are not supposed to use random numbers, counter or timing information in this design.

(b) Comment on any strength or limitation of the solution in (a).

Answer to Exercise 9

Password-based authentication

- S/Key is one of a class of software OTP solutions – more info available



Password-based authentication

- Initial secret, *W*, is hashed *n* times, each hash value is used as an OTP; thus *n* hashing operation generates *n* OTPs in total.
- *n* OTPs are sent to the user to be used in the reversed order, i.e. H^*n*(*W*), H^*n-1*(*W*), …, H(H(*W*)), H(*W*); note