Lecture 37: More Review

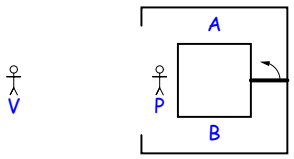
This lecture consists of some review questions about streams and iterators. See `http://inst.cs.berkeley.edu/~cs61a/sp14/slides/lect37.py`.

Announcements

- The CSUA is holding an 18 hour hackathon starting 5/2 at 7pm in the Woz. Prizes include 27" monitors, mechanical keyboards, external HDs, and more. Food will be provided throughout.
- HKN surveys on Friday, 5/2. Points offered for filling out the survey.
- If you think you have been given a deadline extension on a project or homework, *please check* using `glookup -t`. Also use this to check for surprises (assignments you didn't think were late, but are).

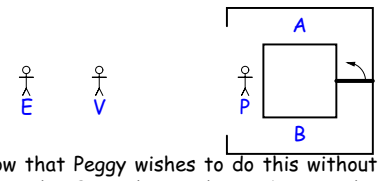
Another Example of Zero-Knowledge Proof

- A classic example: Peggy (P) wishes to prove to Victor (V) that he knows the combination that unlocks the door in this maze:



- That's easy: Peggy just lets Victor see her start down corridor A and return via corridor B.

Example continued



- Suppose now that Peggy wishes to do this without letting Eve (E) know for sure that Peggy knows the combination (just Victor).
- To do so, Peggy repeatedly chooses (at random) to proceed down corridor A or B without letting Victor or Eve see which one.
- Each time, after Peggy has chosen, Victor calls out (randomly) by which corridor Peggy should return.
- If Peggy knows the combination, she will always succeed in returning as asked, and by repeating the experiment, Victor can become as certain as she wants of Peggy's knowledge.
- But Eve, who can't tell if Peggy and Victor are colluding, can't really be sure.