How to share a secret

- This part of the discussion is based on the article
  - Adi Shamir, "How to share a secret", Communications of the ACM, 22(11):612–613, Nov. 1979
  - This short paper is a reading assignment
  - This paper will help understand how shares can be used in the discussion of survivable storage

How to share a secret

- Liu[4] considers the following problem:

"*Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet so that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must carry?*"

Minimal solution: 462 locks and 252 keys per scientist

How to share a secret

- Shamir's (*k,n*) threshold scheme problem statement
  - divide data *D* into *n* pieces *D*1,...,*Dn* in such a way that:

    (1) knowledge of any *k* or more *Di* pieces makes *D* easily computable;

    (2) knowledge of any *k* - 1 or fewer *Di* pieces leaves *D* completely undetermined (in the sense that all its possible values are equally likely).

How to share a secret

- Applications
  - Storage of cryptographic keys
    - » Solution: keep key in <u>trusted</u> computer, brain or safe
      - problem if computer crashes, sudden death, or sabotage the key will be inaccessible
    - » Solution: store multiple copies in different places
      - problem: increases danger of security breaches
    - » Solution: use (k,n)-threshold scheme

How to share a secret

- We will derive the approach on the board