

# Lecture 5: Logs and Trees



# Menu

- Ron Rivest's talk
  - Mixnets and voting
  - Public-key cryptography (dynamic programming)
- Trees
- PS1

# MIXes

Encrypted Votes

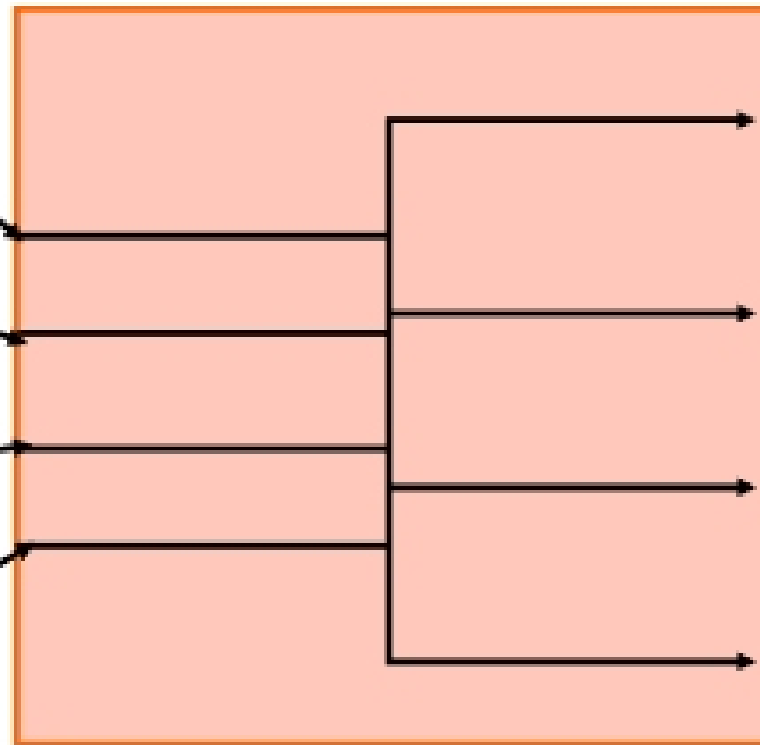
Decrypted Votes

C1

C2

C3

C4



M1

M2

M3

M4

Random, secret permutation