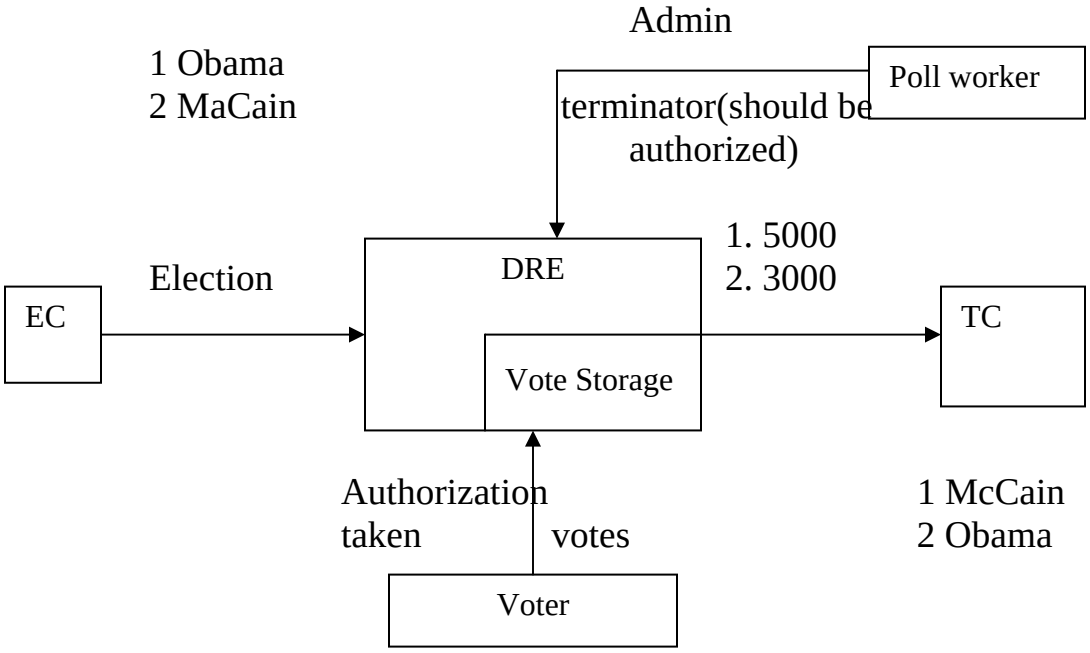
Class note for 4/26

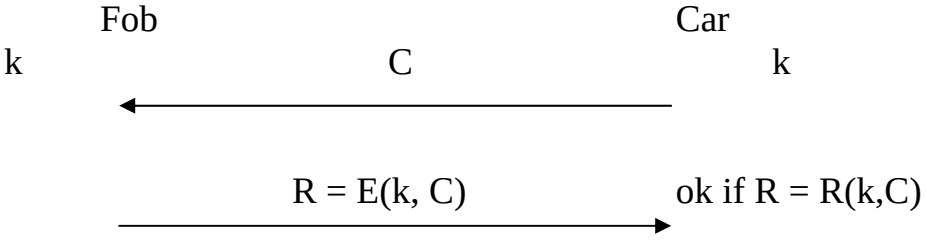
1. Electronic voting



Attacks.

- multiple voting
  - forged authorization cards → no secret, easy to do.
- forged election description
  - candidate shuffling
  - confusion attack
- Denial of Service → forged admin
- Votes transmitted w/ no authorization
- De-anonymize votes via vote storage

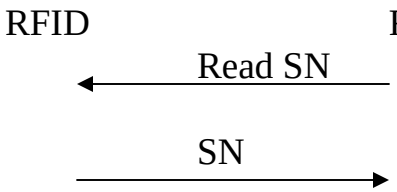
2. Cryptanalysis of RFID Device



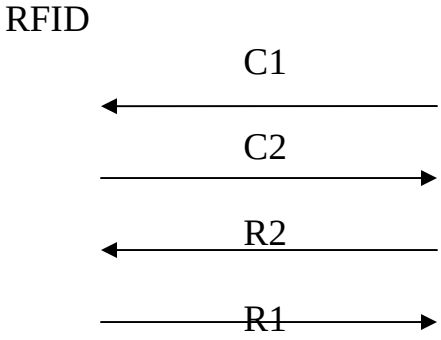
For power
Reader, RFID ~ few car

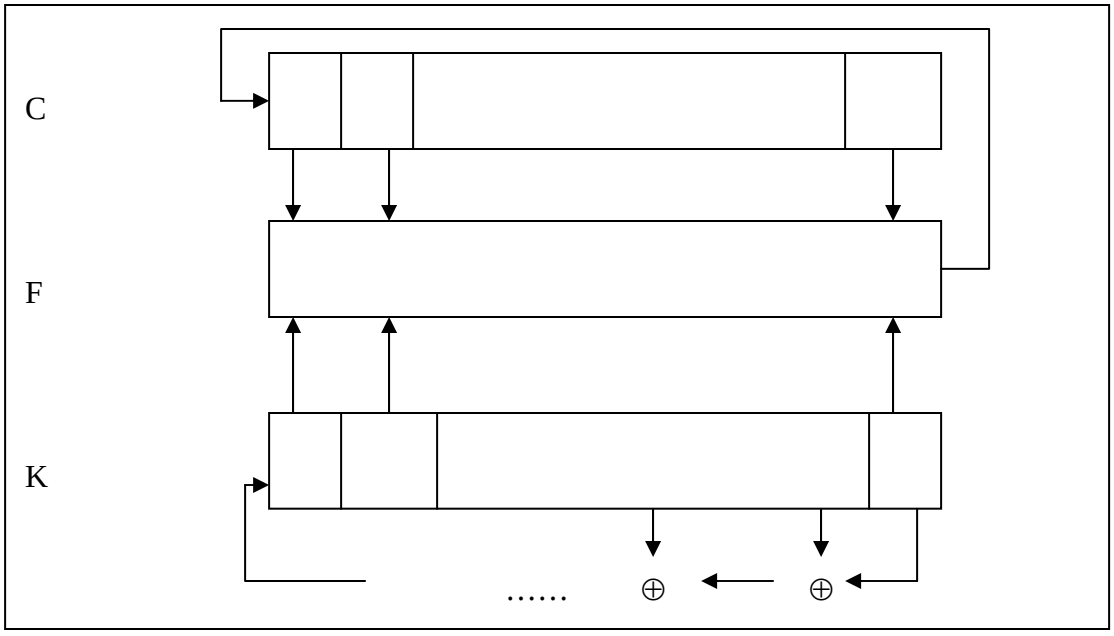
For information
Reader, RFID ~ few meters

RFID types
- cryptographic
- barcode



- applications
  - retail
  - libraries
  - passports
- privacy
  - thieves prescreen houses via RFID on goods inside
  - Obtain patron's reading list
  - Identity theft
  - Target screening
- Defenses
  - Authenticate readers
  - Faraday cages, remove tags (disable tags)





Attack

1. Reverse engineer E
2. Build a key cracker
    a. Give Fob, V, query V on challenge C1, C2 and obtain response R1 = E(k,C1), R2 = E(k, C2)
    b. For each possible k,
    If E(k, C1)=R1 output k
    && E(k, C2)=R2