Class note for 4/26

1. Electronic voting

\[
\begin{array}{c}
\text{Election} \\
\text{EC} \\
\text{Admin} \\
\text{Poll worker (should be authorized)} \\
\text{DRE} \\
\text{Vote Storage} \\
\text{Authorization taken votes} \\
\text{Voter} \\
\text{1 McCain} \\
\text{2 Obama} \\
\text{1. 5000} \\
\text{2. 3000} \\
\text{TC}
\end{array}
\]

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

2. Cryptanalysis of RFID Device

\[
\begin{array}{c}
\text{Fob} \\
k \\
C \\
\text{Car} \\
k \\
\text{ok if } R = R(k, C)
\end{array}
\]

\[
R = E(k, C)
\]

For power
Reader, RFID \~\ few car
For information
Reader, RFID ~ few meters

RFID types
- cryptographic
- barcode

RFID Reader

Read SN

SN

- applications
  o retail
  o libraries
  o passports

- privacy
  o thieves prescreen houses via RFID on goods inside
  o Obtain patron’s reading list
  o Identity theft
  o Target screening

- Defenses
  o Authenticate readers
  o 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