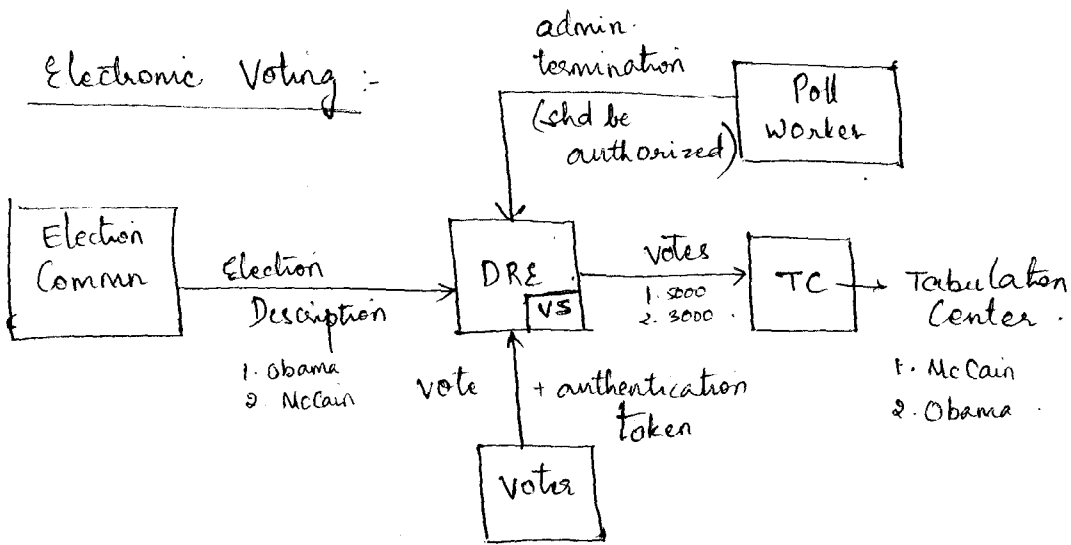


26/4/2007

Electronic Voting :-



Attacks :-

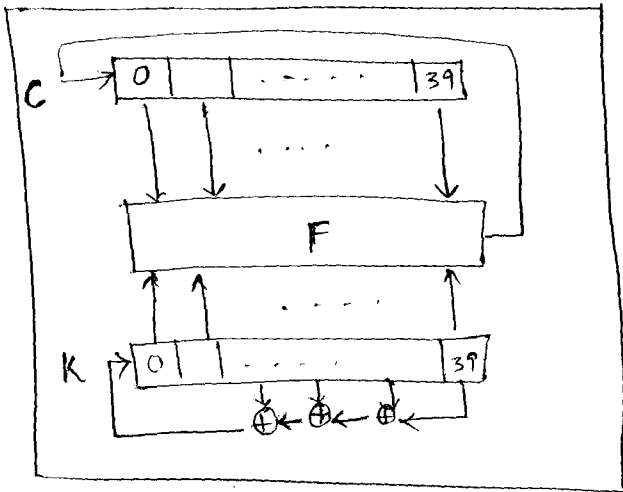
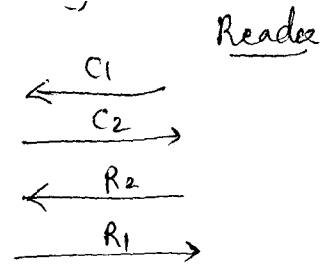
- Multiple Voting :-
 - Forged authorization cards \Rightarrow No secret, easy to do.
- Forged Election Description :-
 - \rightarrow Candidate shuffling attack
 - \rightarrow Confusion attack
- Denial of service via Forged Admin/ender cards.
- Votes transmitted with no authentication from DRE to TC.
- De-anonymize via Vote storage (based on the order in which votes were voted)
- Security by obscurity doesn't work. It is not enough to do just black-box testing.

Cryptanalysis of RFID Device :-

To prevent privacy attacks: we cd authenticate readers $\xrightarrow{\text{RFID}}$

Faraday Cages. -- Remove tags

Disable Tags.



Attack :-

① Reverse engineer E (Encryption function)

② Build a Key Cracker.

ⓐ Given a Fob, V , query V on challenge C_1, C_2 and obtain response $R_1 = E_k(C_1), R_2 = E(k, C_2)$.

ⓑ For each possible k , if $E(k, C_1) = R_1$ & $E(k, C_2) = R_2$, output k .