Authenticated Key Exchange Protocols

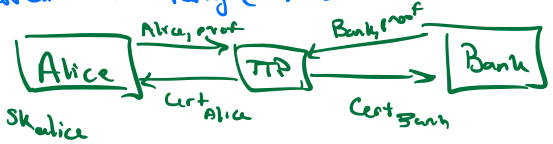
Key exchange should be secure against active attacks.

Def. Active adversary: complete control of network,
can modify, delete, inject packets

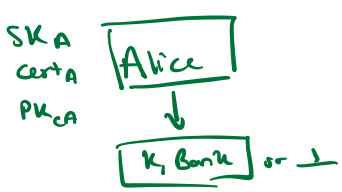
ex. MITM attacks

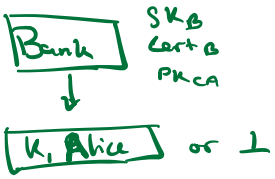
+ some honest and corrupt users, controlled by adv
→ key exch w/corrupt users should not affect other sessions

Trusted Third Party (TTP)



→ Offline TTP (CA): contacted only during registration, revocation
→ Online TTP: actively participates in every key exch (Kerberos)
→ only need symmetric crypto





Basic AKE security (informal)

Suppose Alice successfully completes AKE to obtain (K, Bank)
If Bank not corrupt then:
Alice authenticity: (same for Bank)
→ Alice key only shared w/ Bank

Secrecy:
→ To adv, keys K indistinguishable from rand.
(even if adv. sees other keys in other sessions)

Consistency
→ If bank completes AKE it obtains (K, Alice)

Forward secrecy:

→ if adv learns SK_B at time $\bar{T}$, then all sessions w/Bank from $t < \bar{T}$ remain secret

HSM security:

→ If adv. queries HSM holding SK_B n times, then at most n sessions are compromised.