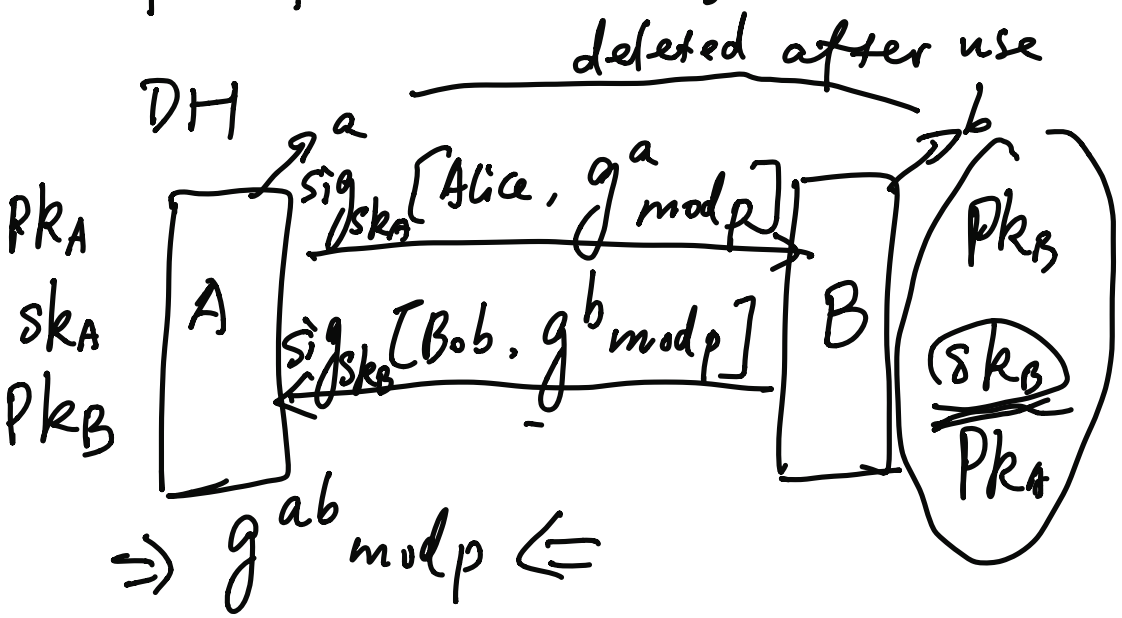
ECE 471/571 PFS, Kerberos

Perfect forward secrecy. (PFS)



$\Rightarrow g^{ab} \bmod p \Leftarrow$

when A & B are overrun

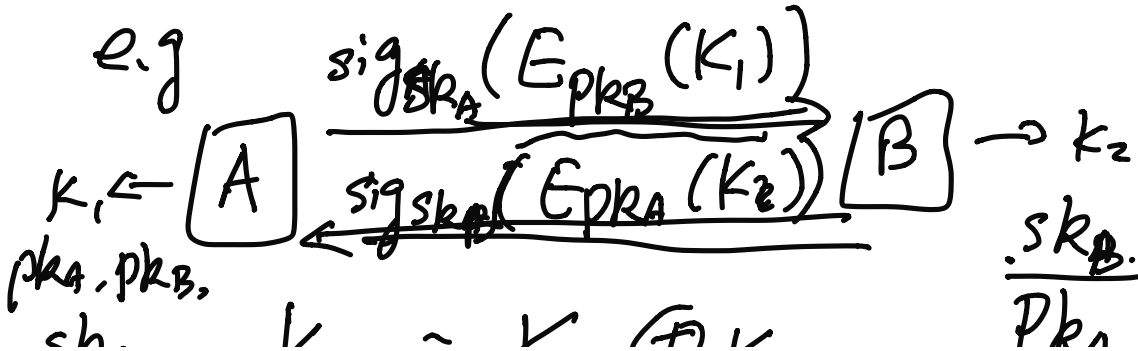
and adv eavesdrop msgs

still cannot decrypt old conver (recorded)

$\Rightarrow$ PFS

---

e.g



DKA. $K_{AB} = K_1 \oplus K_2$.

participatory key agreement

- if A & B compromised:

  obtain K_1, K_2 in the past

  $\Rightarrow K_{AB}$ in the past

  X PFS.

- if only A or B is compromised?

  adv only obtain either K_1 or K_2

  cannot obtain $K_{AB} = K_1 \oplus K_2$.

  ✓ PFS.