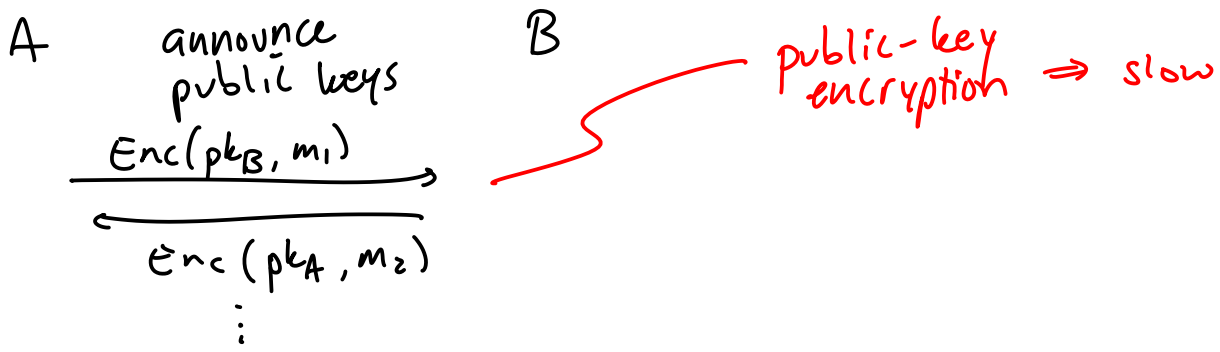
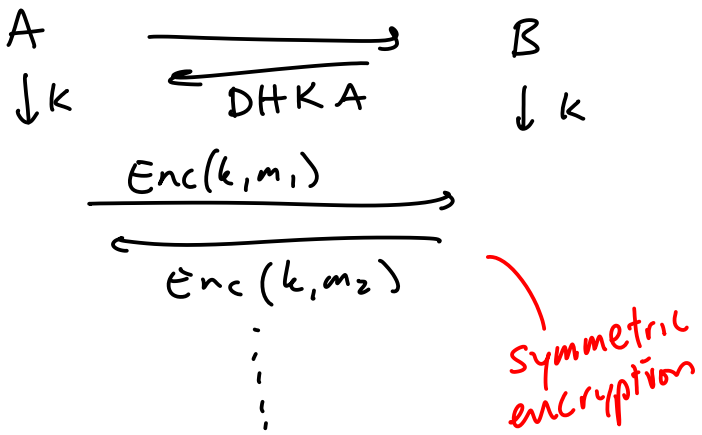
Off-the-Record & Signal

Scenario: Alice & Bob have never spoken before, want to communicate securely

Really Basic:



"Basic" Secure messaging



Pitfalls / properties

② − DHKA doesn't authenticate endpoints

\+ Enc should be CCA secure to protect against outsiders (not Alice / Bob) injecting / modifying messages

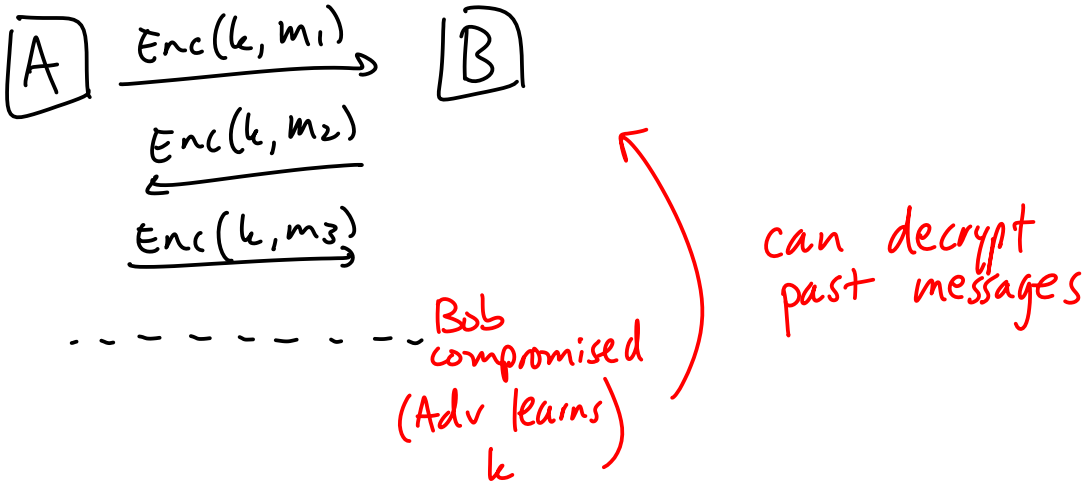
① − if Bob is compromised, attacker can read everything

③ − Bob can blackmail Alice

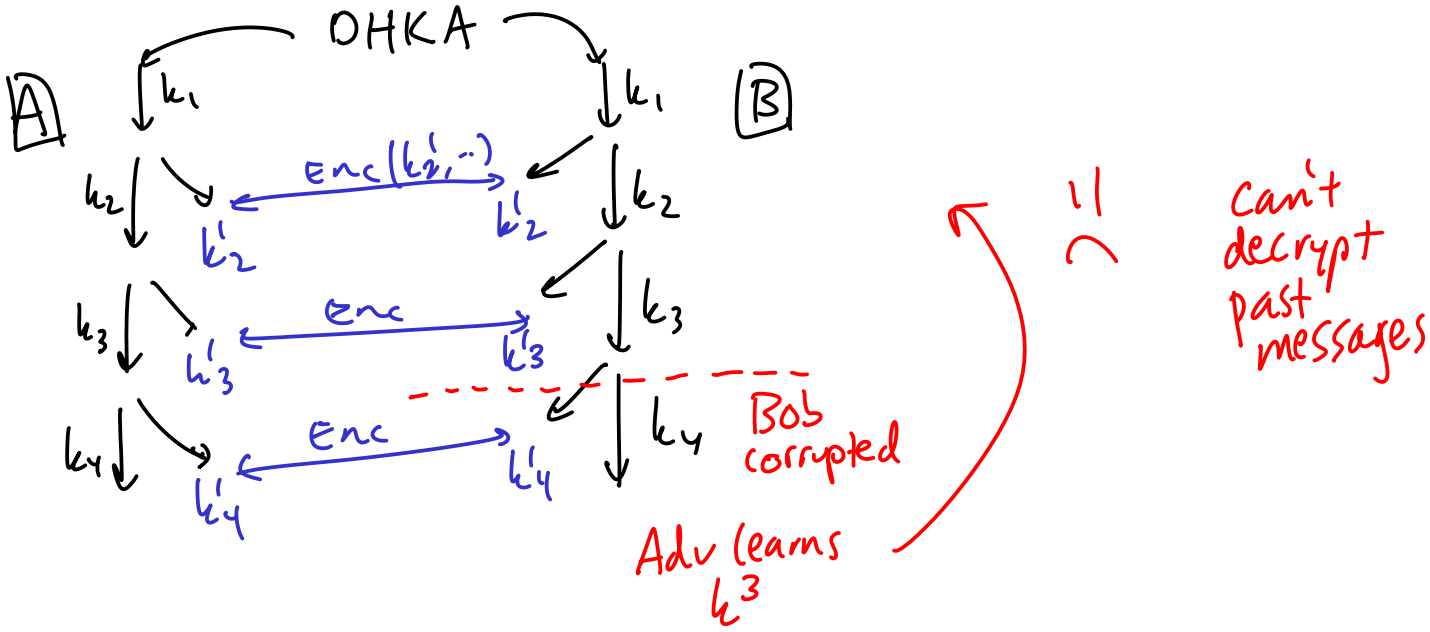
Post-compromise Security

"protect against future compromise"

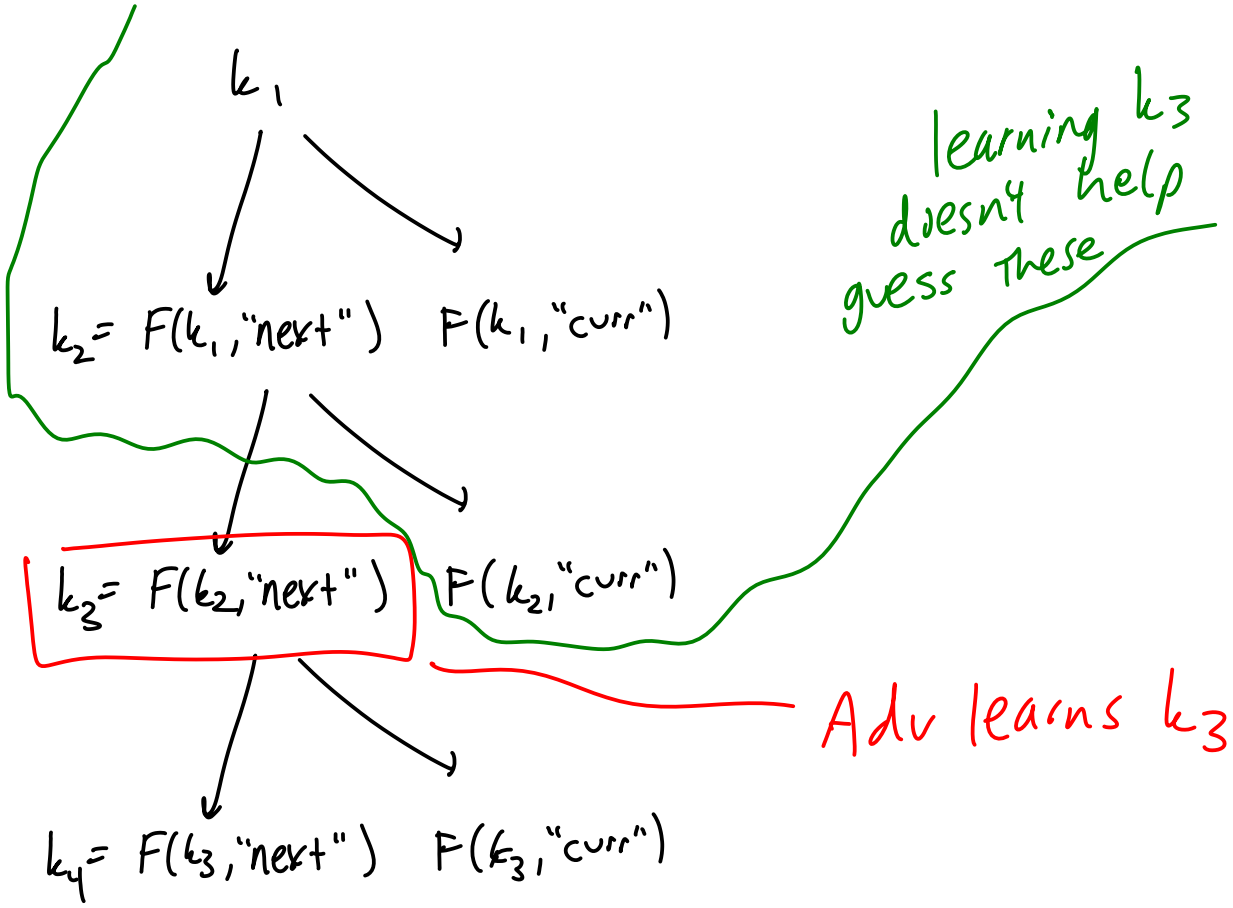
instead of



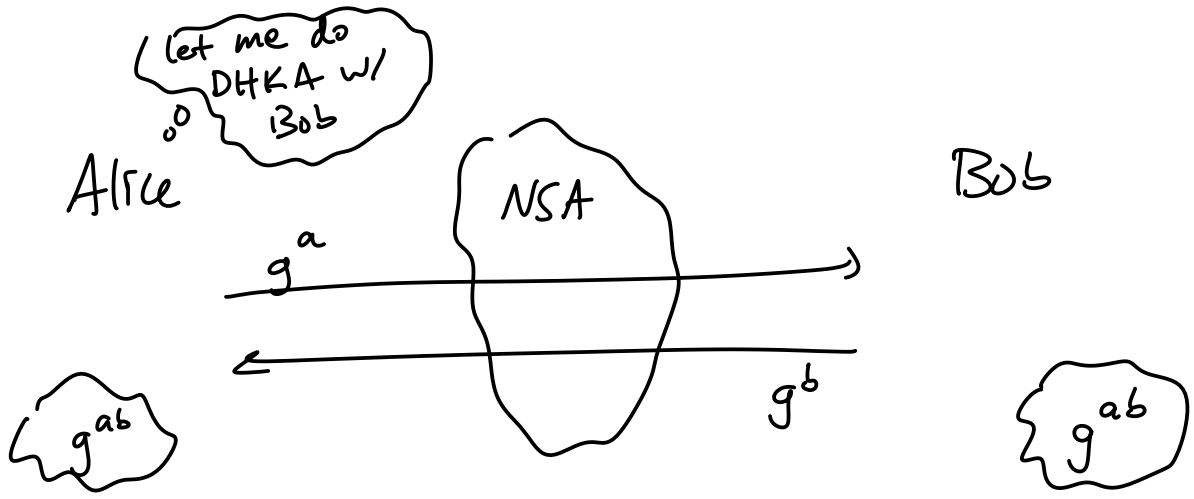
Do this: (symmetric ratchet)



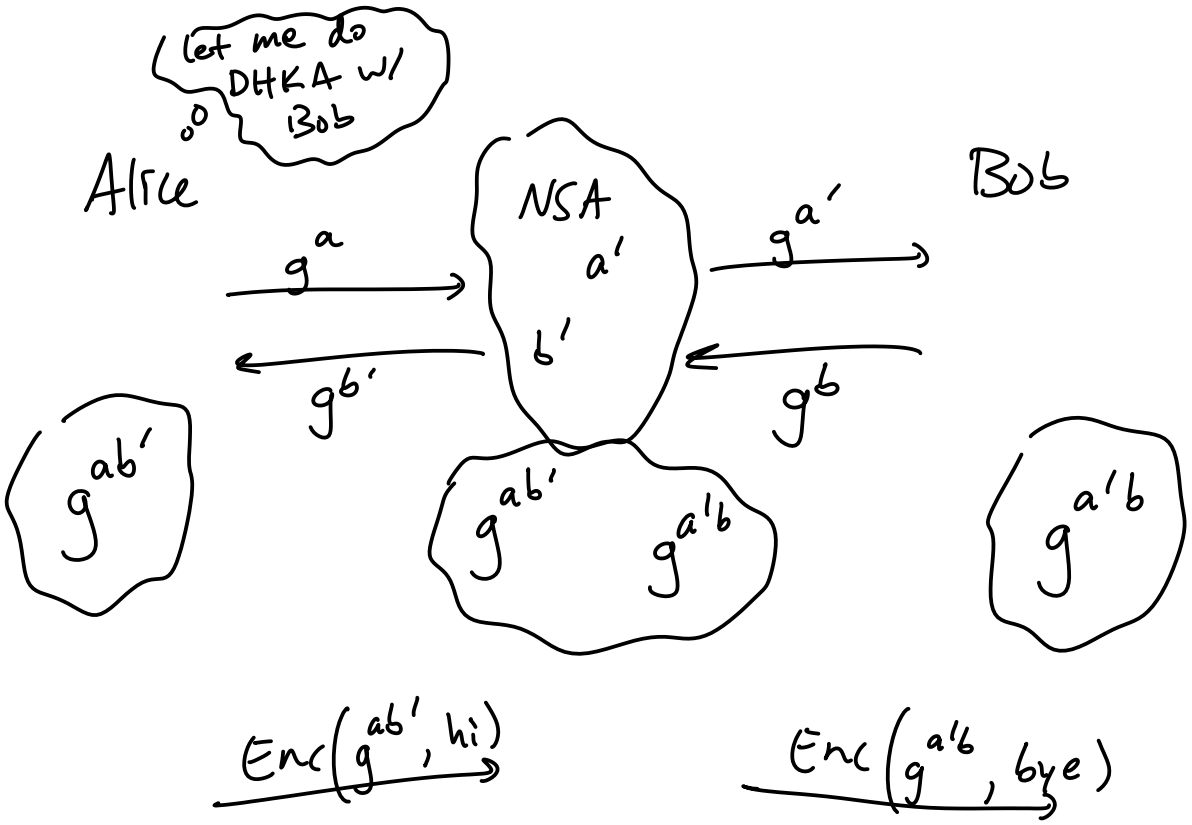
(assuming parties erase past keys)



Man-in-the-Middle



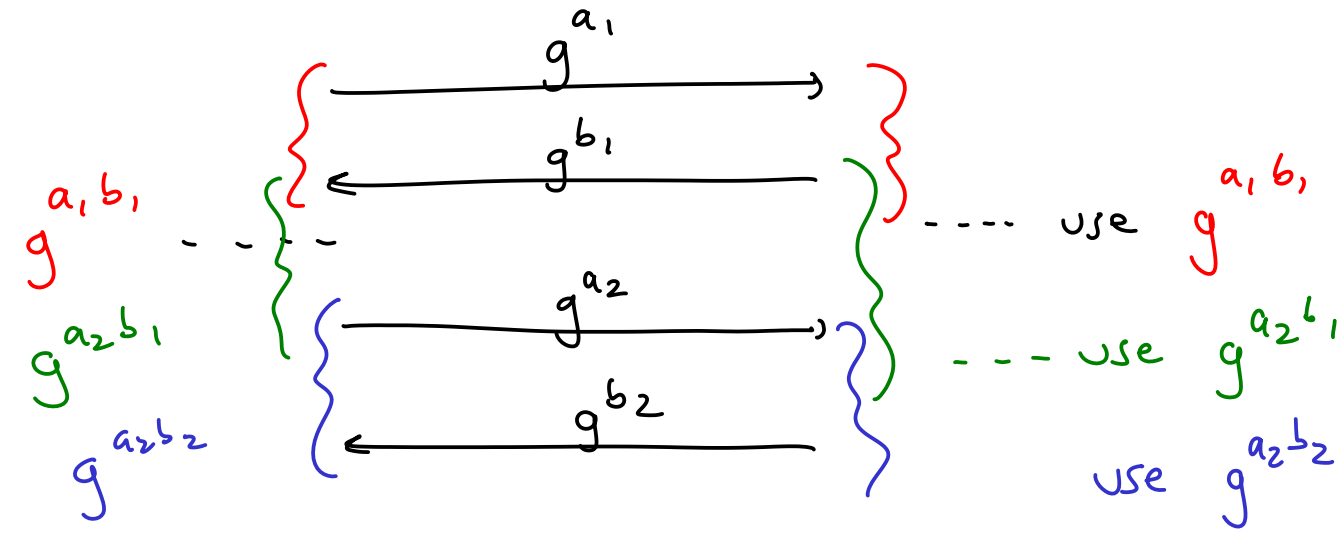
NSA just watches ⇒ NO PROBLEM!



When NSA actively doing MitM ⇒ problem

Recover from past compromise?

DH ratchet:



If MitM stops actively changing messages
⇒ regain security

Repudiation:

goal: Anyone should be able to come up with a valid transcript in which Alice says any message