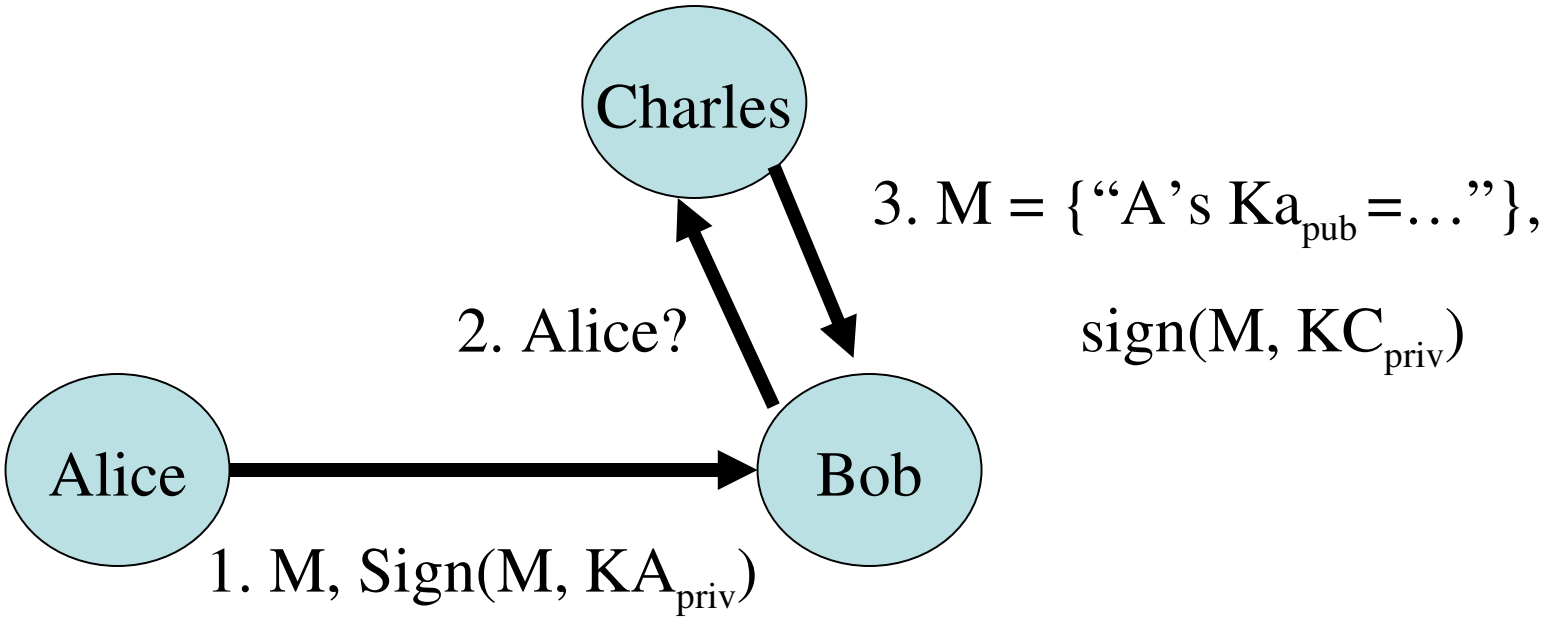
Slides for Key Distribution, Denning Sacco, and SSL

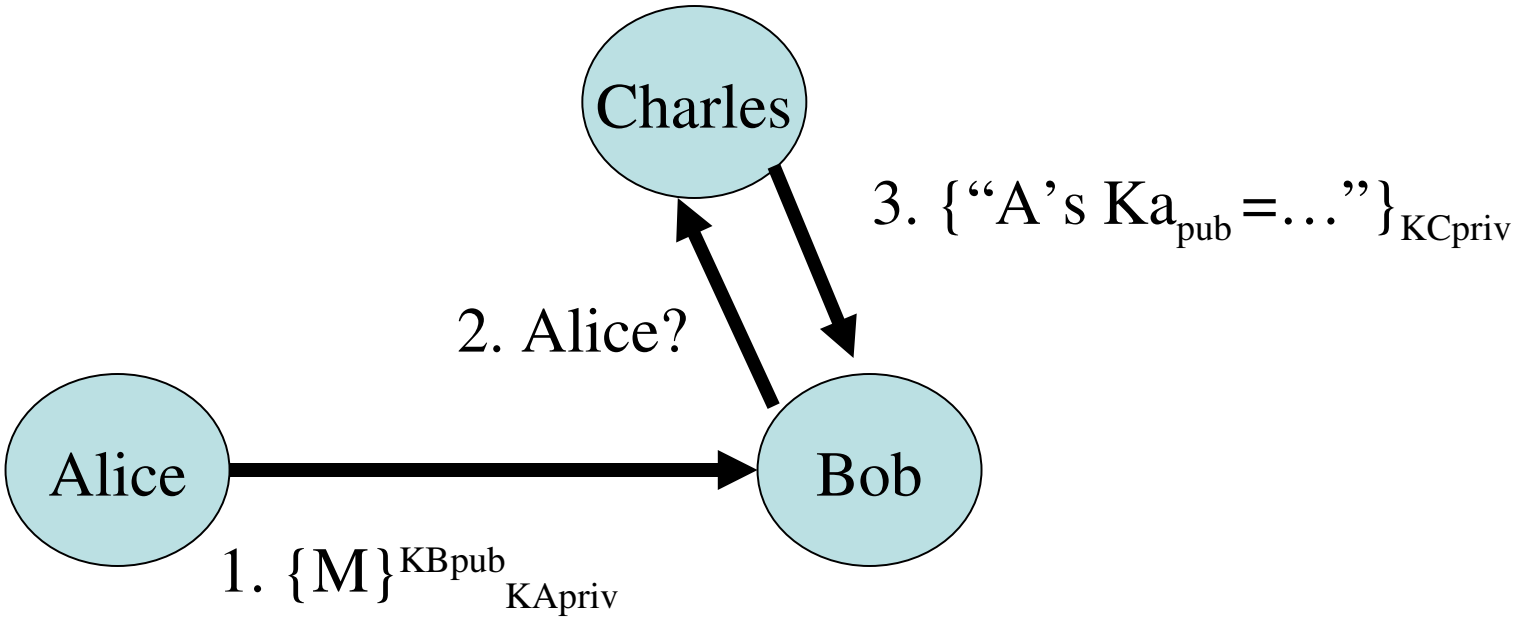
6.033 Spring 2008

key distribution



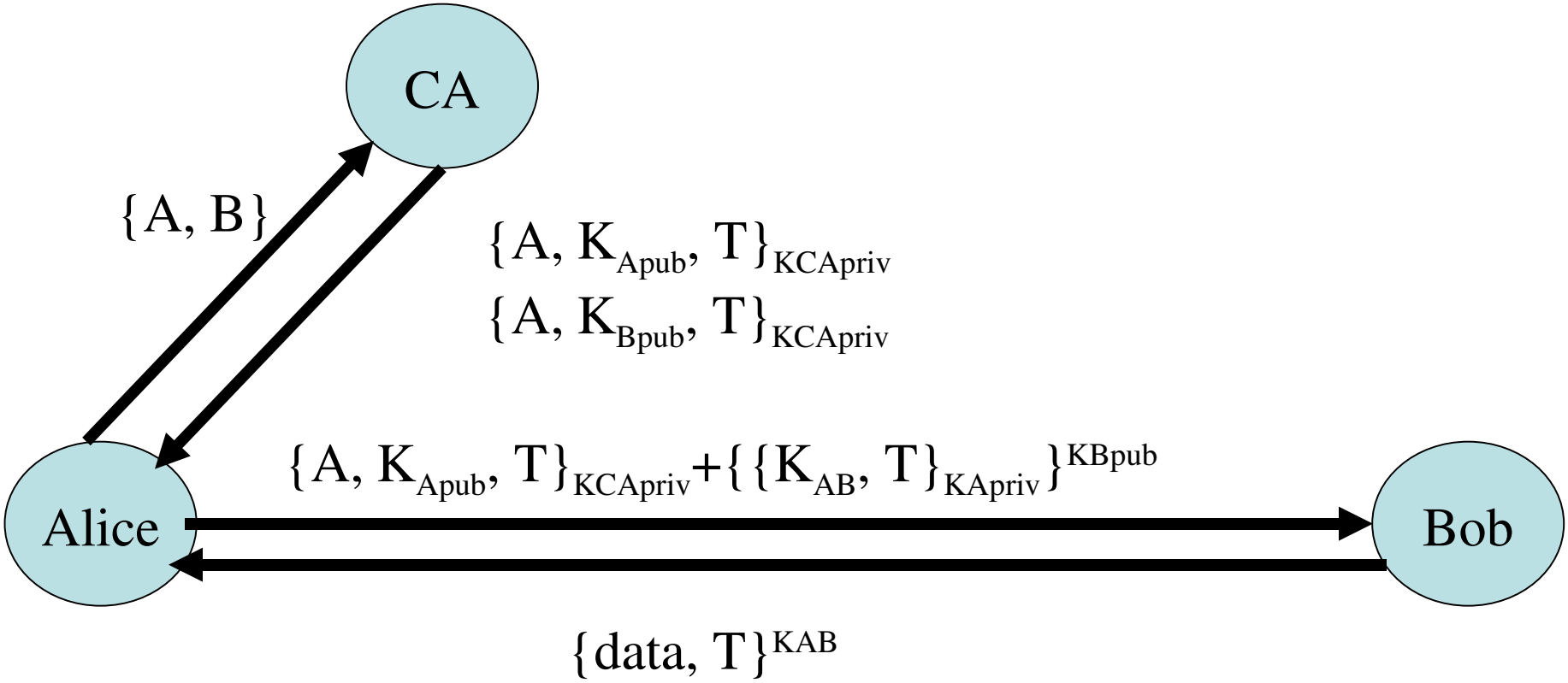
- 3 is a *certificate* for Alice's public key
- Charles is called a *certificate authority*
- The interaction is an example of a *cryptographic protocol*

Shorter notation



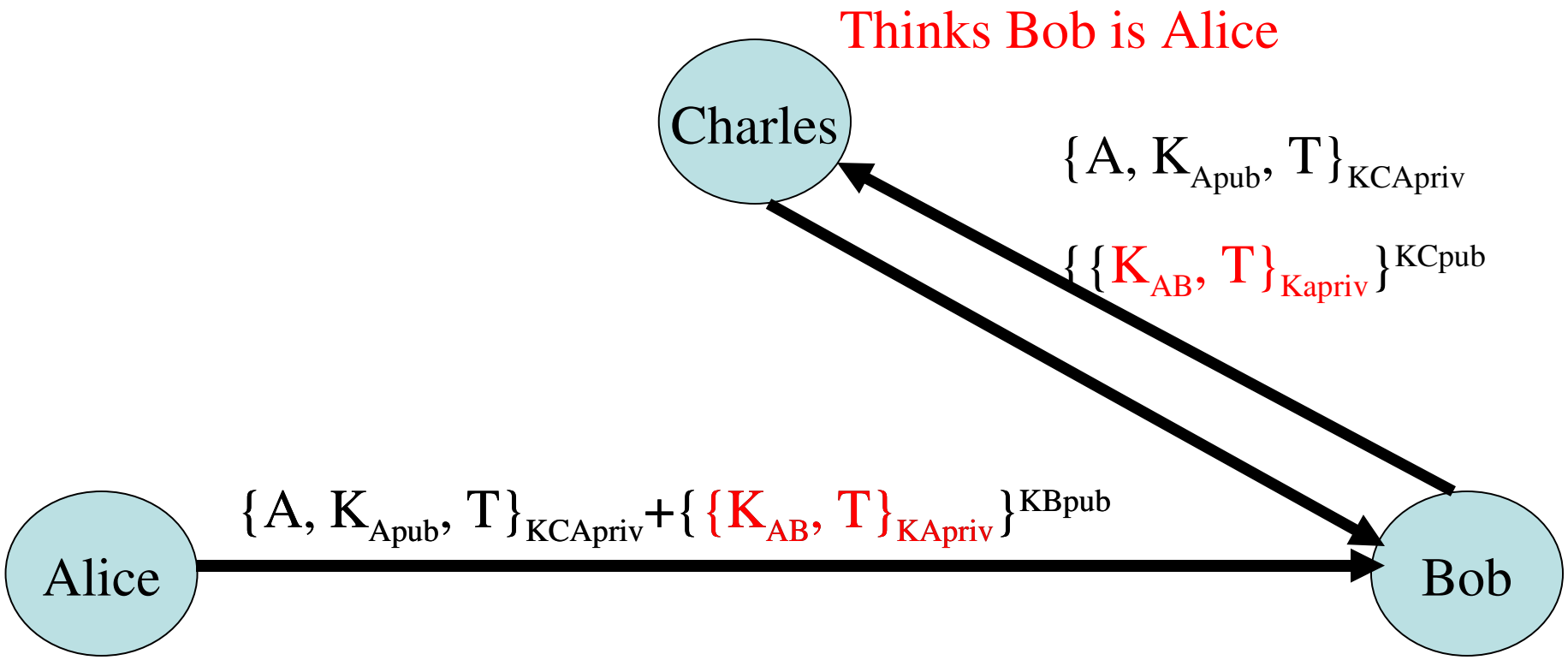
- Subscript for signing
- Superscript for encrypting

Denning-Sacco

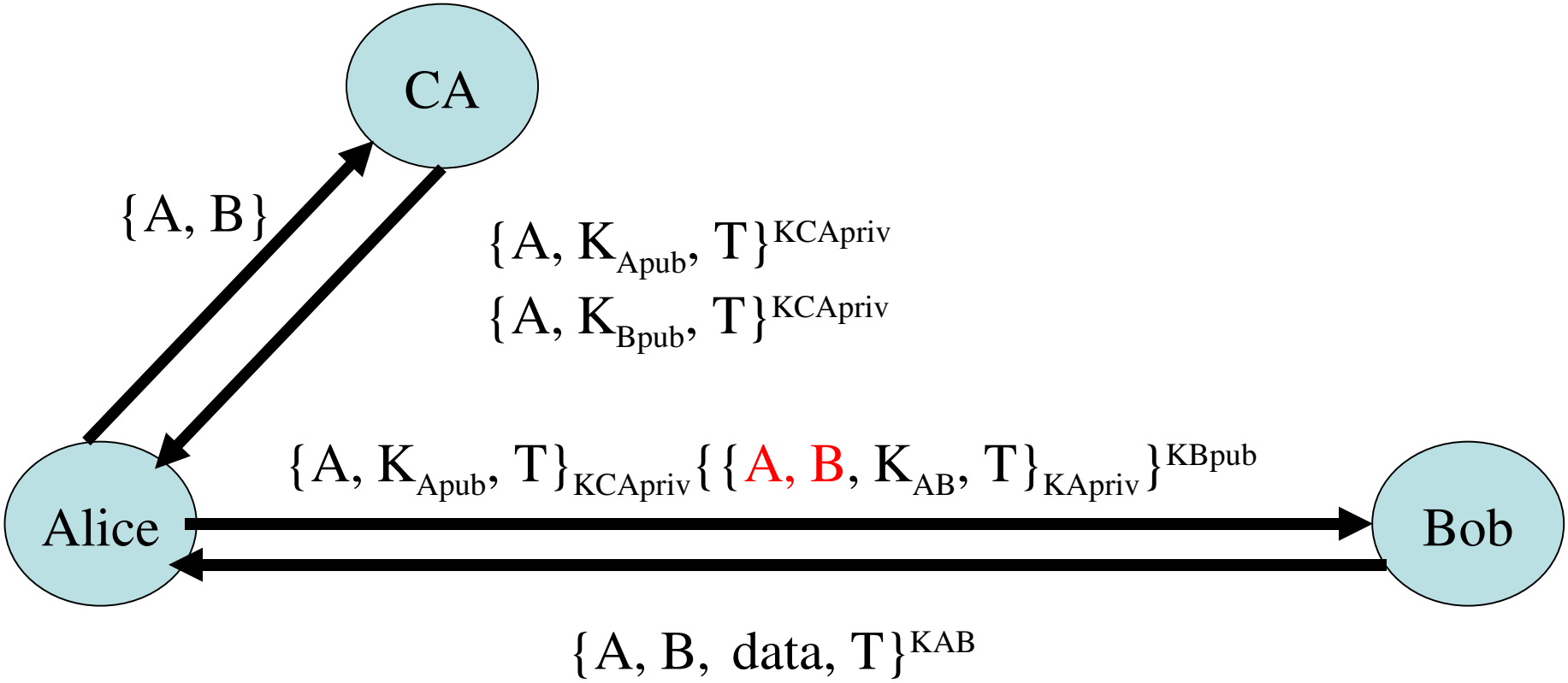


1. Authenticate Alice to Bob and Bob to Alice
2. Set up a shared-secret key

Impersonation Attack



Denning-Sacco (fixed)



Be explicit!

Web (SSL simplified)

- U: https://www.amazon.com
- B →W: {random$_c$, session-id, ciphersuites}
- B ← W: {random$_s$, session-id, {amazon.com, $K_{pub\text{-}amazon}$}$_{Kversign}$}
- B: verify({amazon.com, $K_{pub\text{-}amazon}$}$_{Kversign}$, $K_{pub\text{-}verisign}$)?
- B →W: {pre-master-secret}$^{Kpub\text{-}amazon}$
- .....