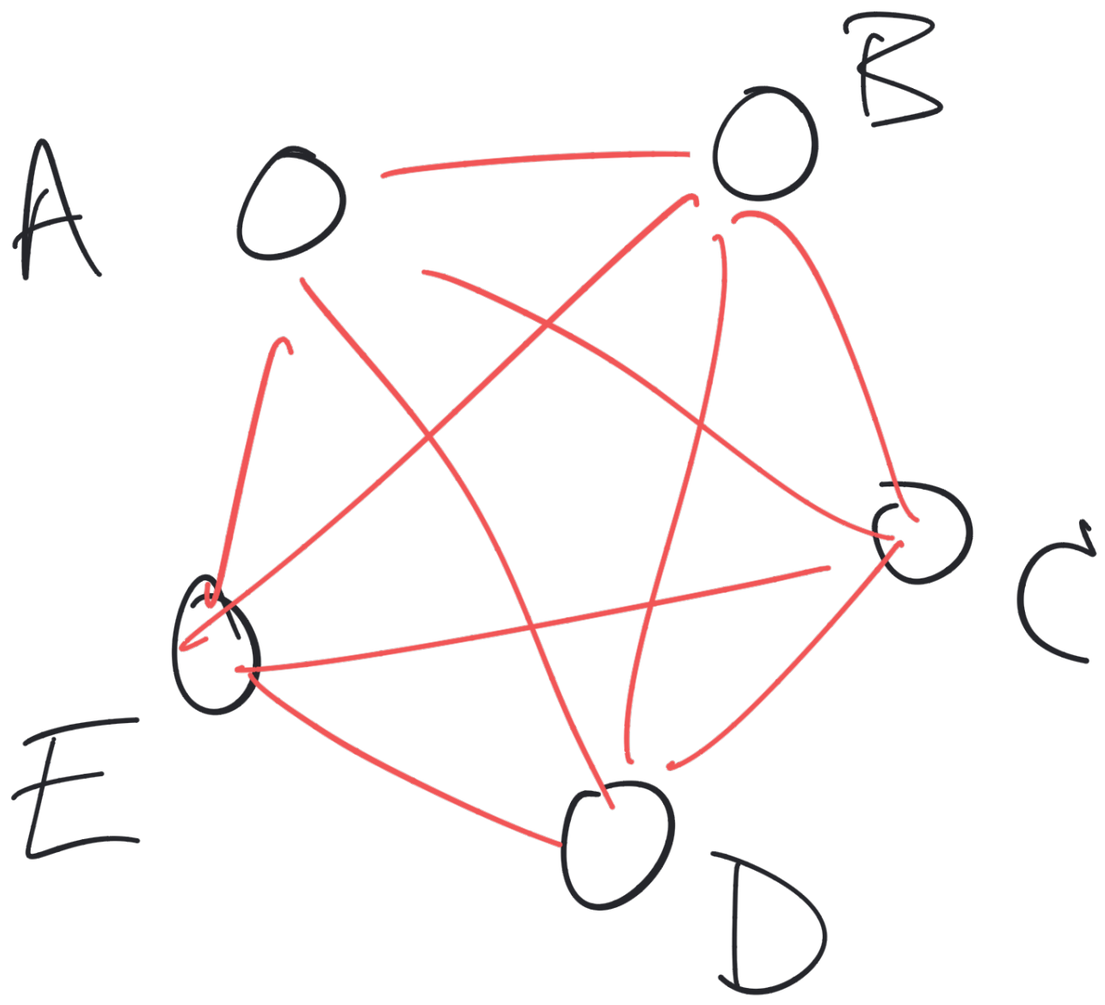
CS 338

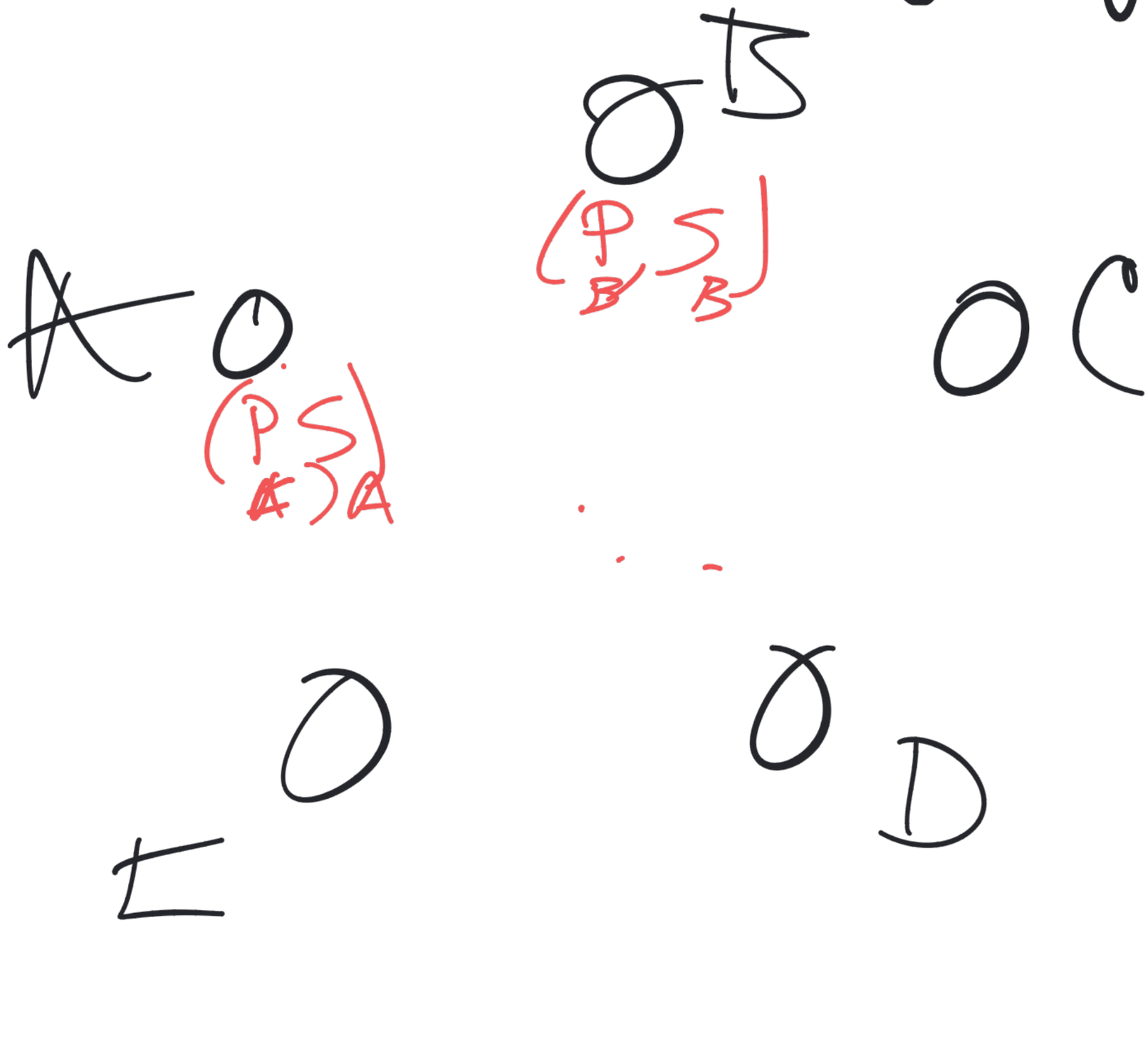
Mon, 2 Oct 2023

AES: how many keys?



$$\frac{N(N-1)}{2} \sim \frac{1}{2}N^2$$

RSA: how many keys?



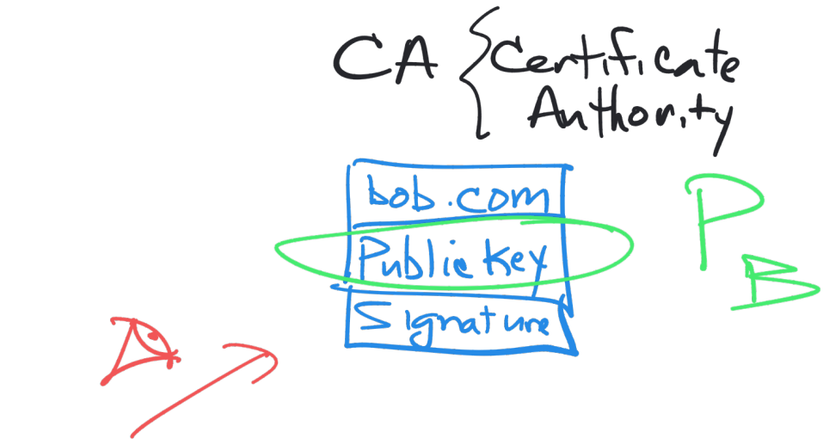
AES vs. RSA

AES Faster (encr., decr.)

AES same security, shorter keys

RSA depends on "one-way trapdoor functions"
(we need one such fn per key)

to get this, you introduce mathematical attack vectors



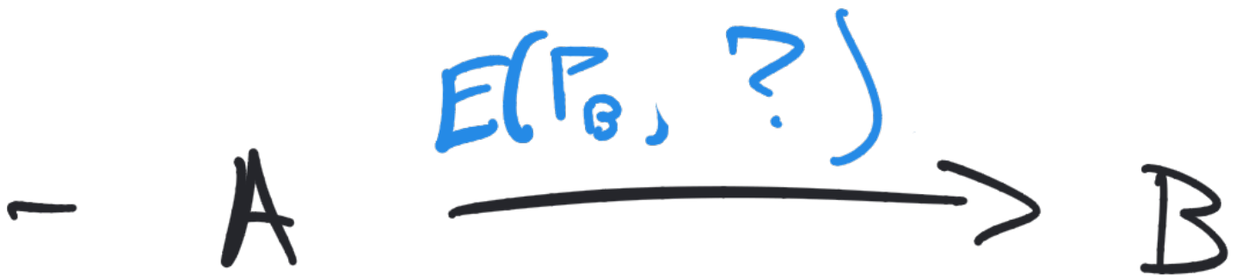
A

B

Goal: ① get a shared AES key between A + B

② B proves to A that he has S_B (secret key)

Steps?


E(P_B, ?)
A
B

- A + B do DH
to agree on K
[Problem: AITM]

- A poses a challenge
to B.

... to be continued
...