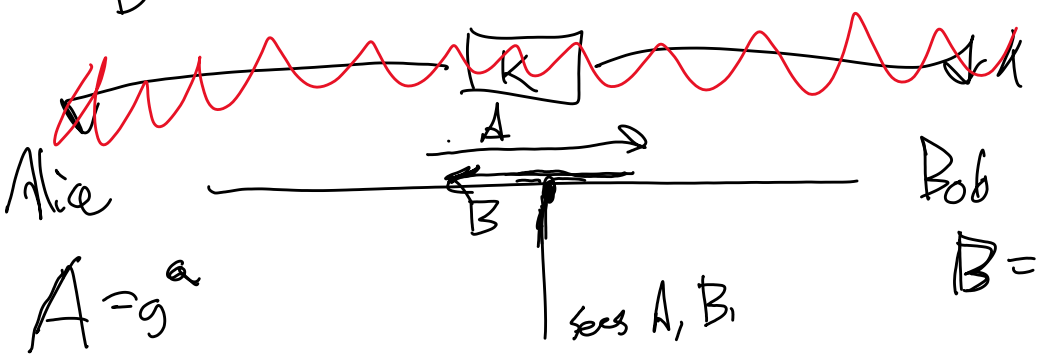
Diffie Hellman

Monday, October 11, 2021 12:23 PM

Diffie-Hellman key Exchange

What if no shared key to start with?



Eve

Goal: Alice and Bob get a shared key, K, Eve has no information about K, even seeing all comms between them.

$$B^a = (g^b)^a = g^{ab} = (g^a)^b = A^b$$

$K = g^{ab}$

- IF CDH is hard, Eve cannot compute K given A, B.
- IF DDH is hard, Eve cannot distinguish K from a random group element.

- Once Alice, Bob have a shared secret, Can use it for MAC, sym. encryption, etc.