CS 338

Wed, 4 Oct 2023

Potential shared secret sharing

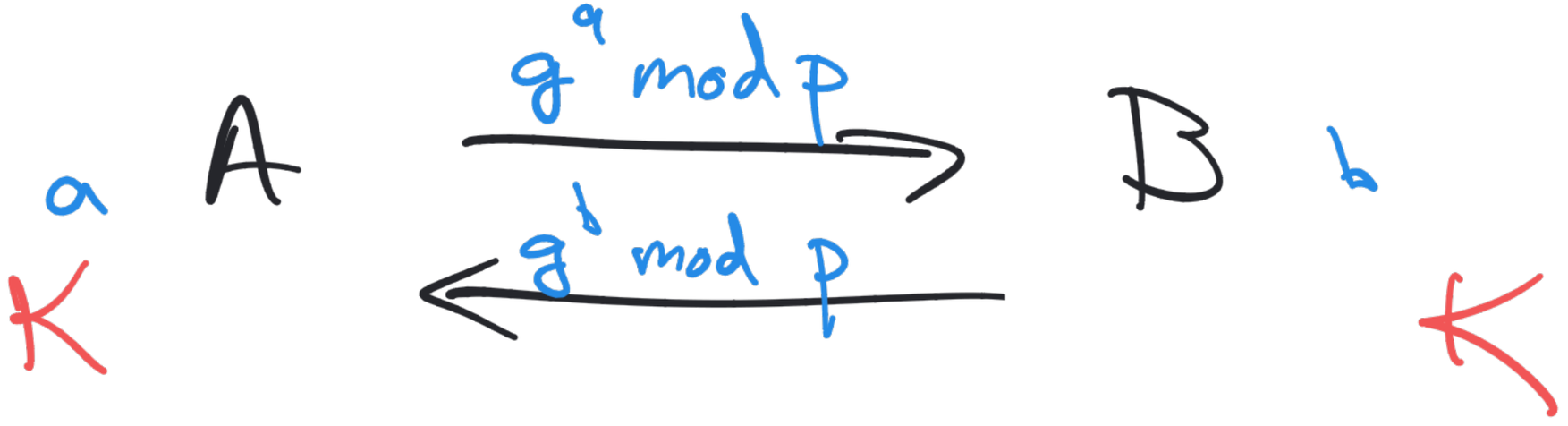
1. A generates random K
2. A $\xrightarrow{E(P_B, K)}$ B

B: S_B ← Secret

Achieves
- A + B share a secret
- Nobody else has it

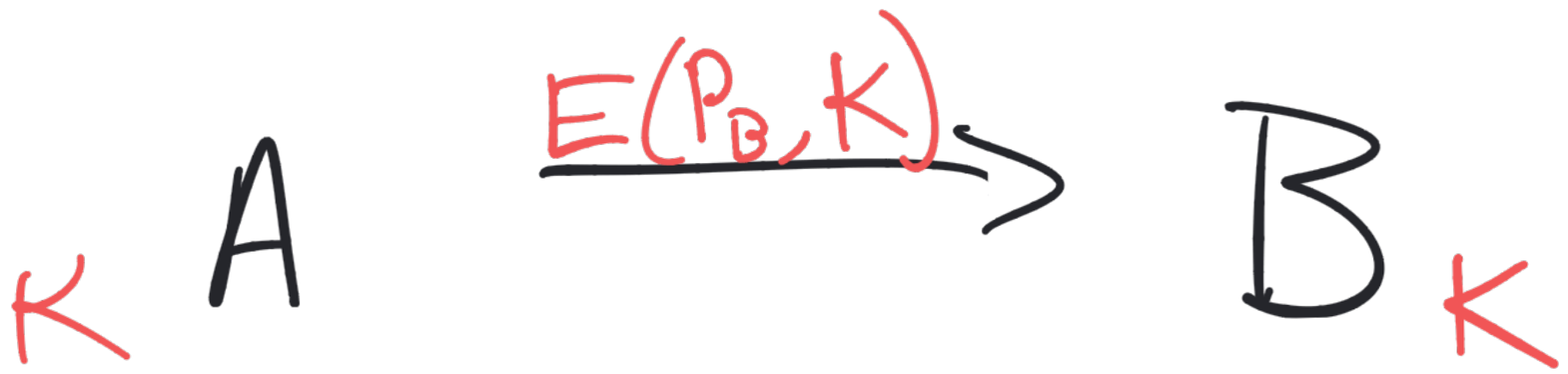
But: A got to choose the secret

Protocol 1: Just DH



Bad: AITM

Protocal 2:



Bad: only A determines the key

Protocol 3:

① DH

② Challenge + response w/ certificate

Challenge + response

R = random

K A

$E(P_B, R)$

$E(S_B, R)$

B

K

cert.

bob.com

P_B

CA sig

A

$E(P_B, R)$

M

E(

B

cert

Subject: bob.com
Public key:
P_B

$E(S_{CA}, H(TBS))$

TBS
"to be signed"

Scᴀ
only CA has it

(If this is legit, this is what it looks like)

cert

Subject: bob.com
Public key:
P_B

TBS "to be signed"

$E(S_{CA}, H(TBS)) = sig$

A "validates" this cert. If yes, somebody with S_{CA} created the signature

① $h = H(TBS)$

② $x = E(P_{CA}, sig)$

③ $x == h$?