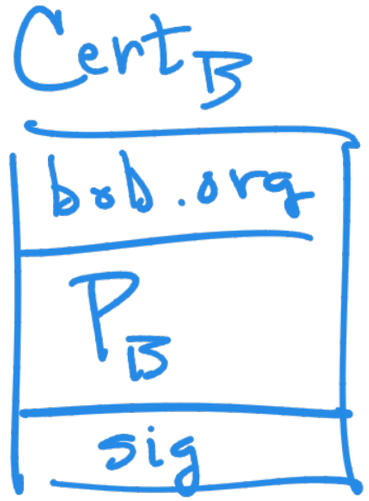
CS 338

Fri, 6 Oct 2023

Assumptions

- Trustworthy CA signed → $Cert_B$



- Only Bob has S_B
- At any time, Alice can validate $Cert_B$ to be confident P_B is really Bob's public key
- Alice's DH secret a; Bob's b

Goals of protocol

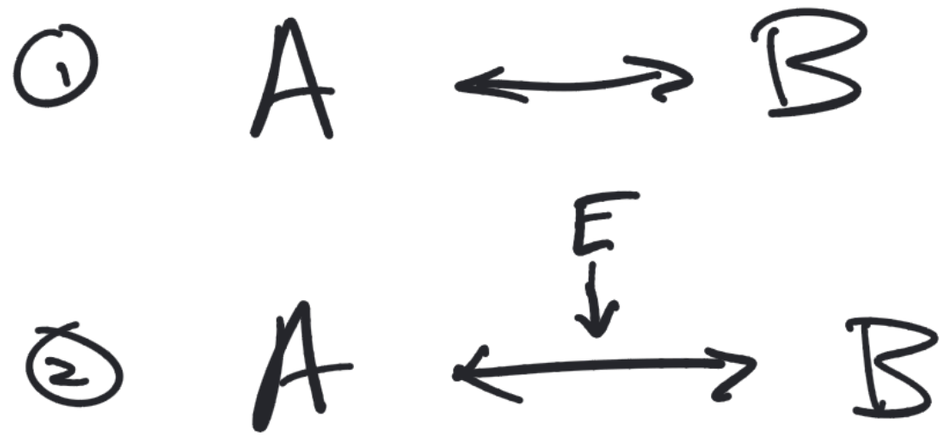
Alice: compute secret K shared with Bob

Bob: compute secret K

Eve: can't know K

Mal: can't know K (*)

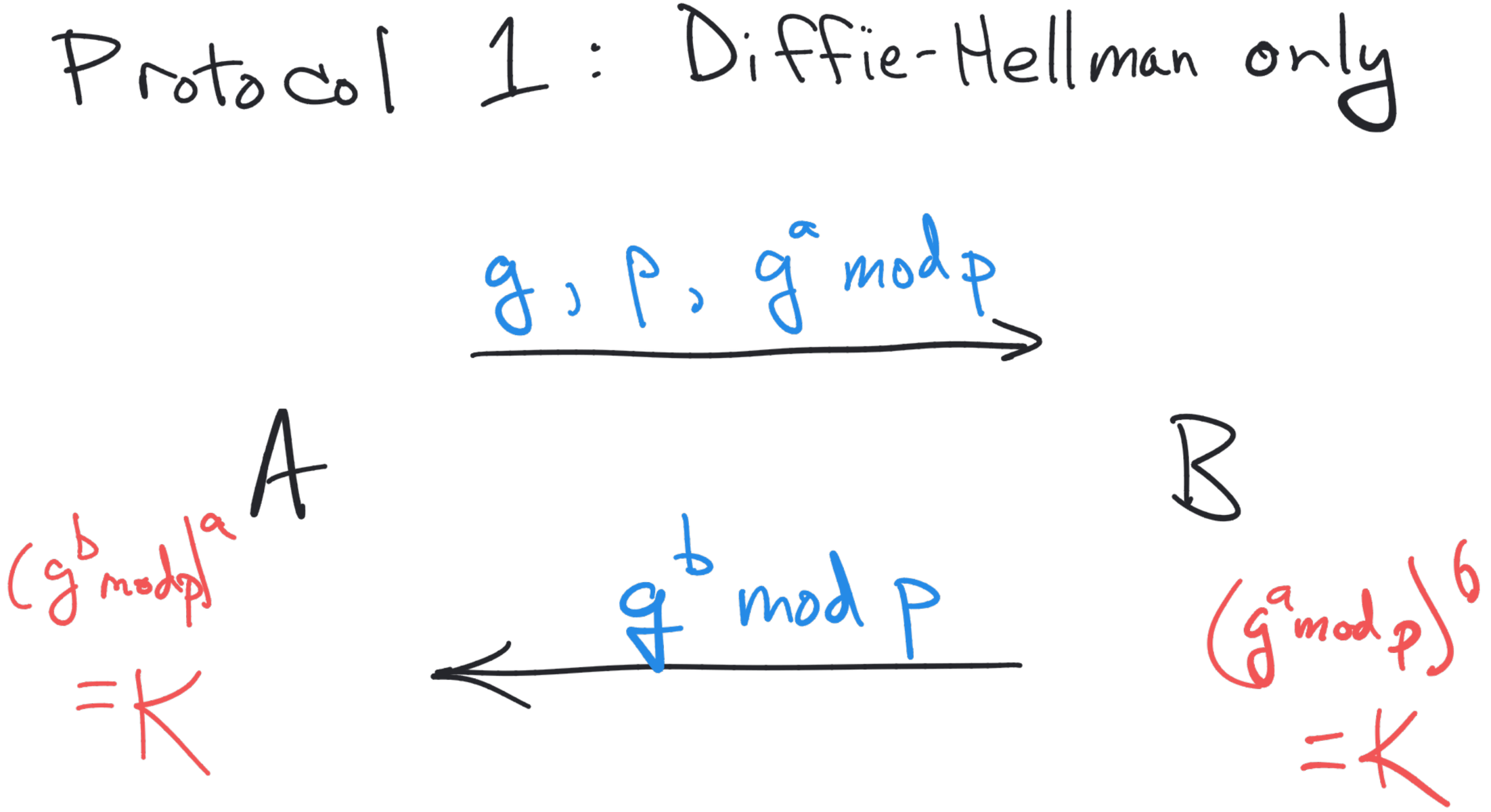
Scenarios

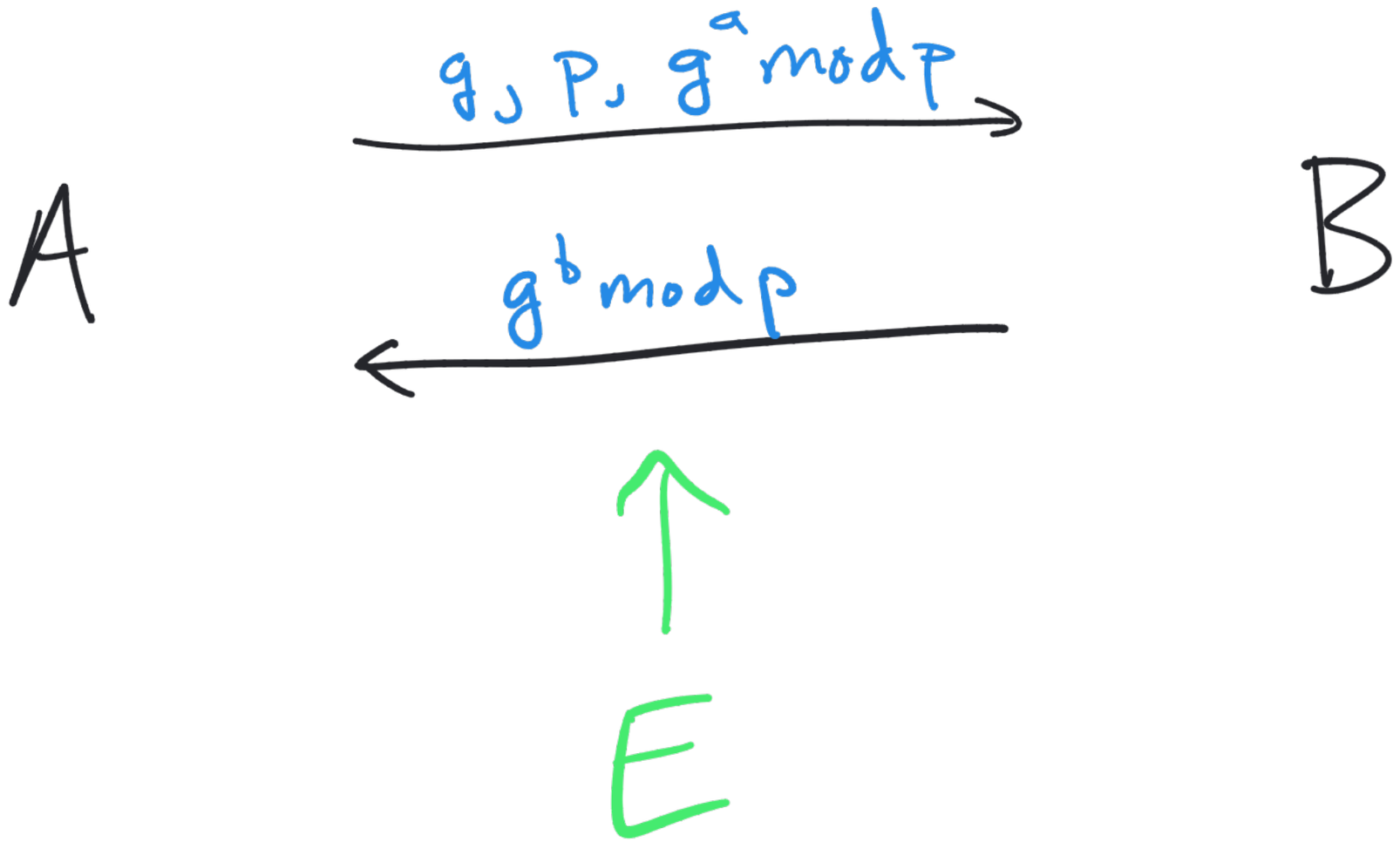


Questions for each scenario

- Who else knows A's K?
- Who else knows B's K?
- Is Alice's K == Bob's K?
- Can B notice trouble?
- Can A notice trouble?
- Can E or M read messages A sends w/ AES + K?
- Can M modify/replace/drop packets encrypted w/ AES + K?

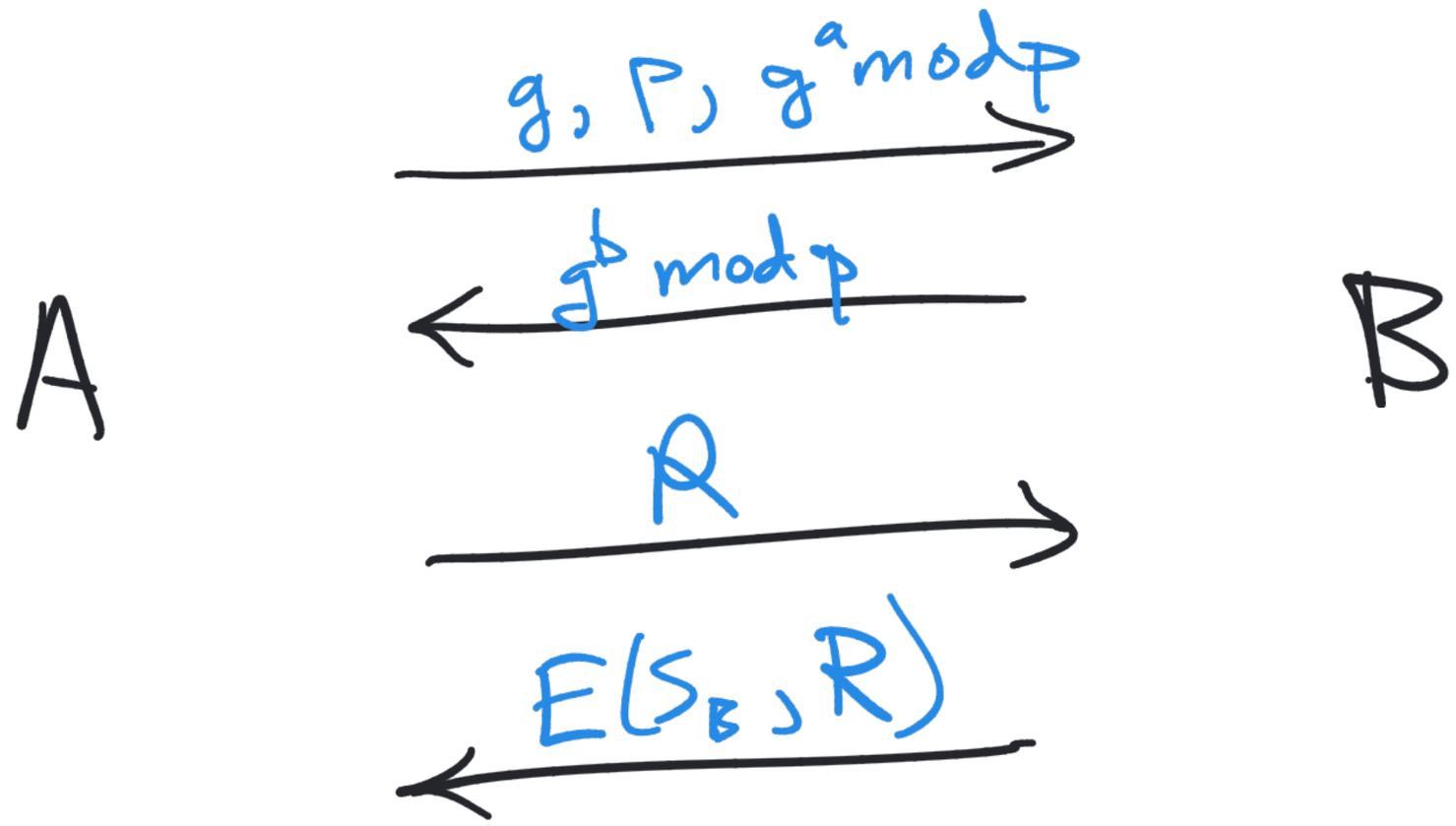
Protocol 1: Diffie-Hellman only

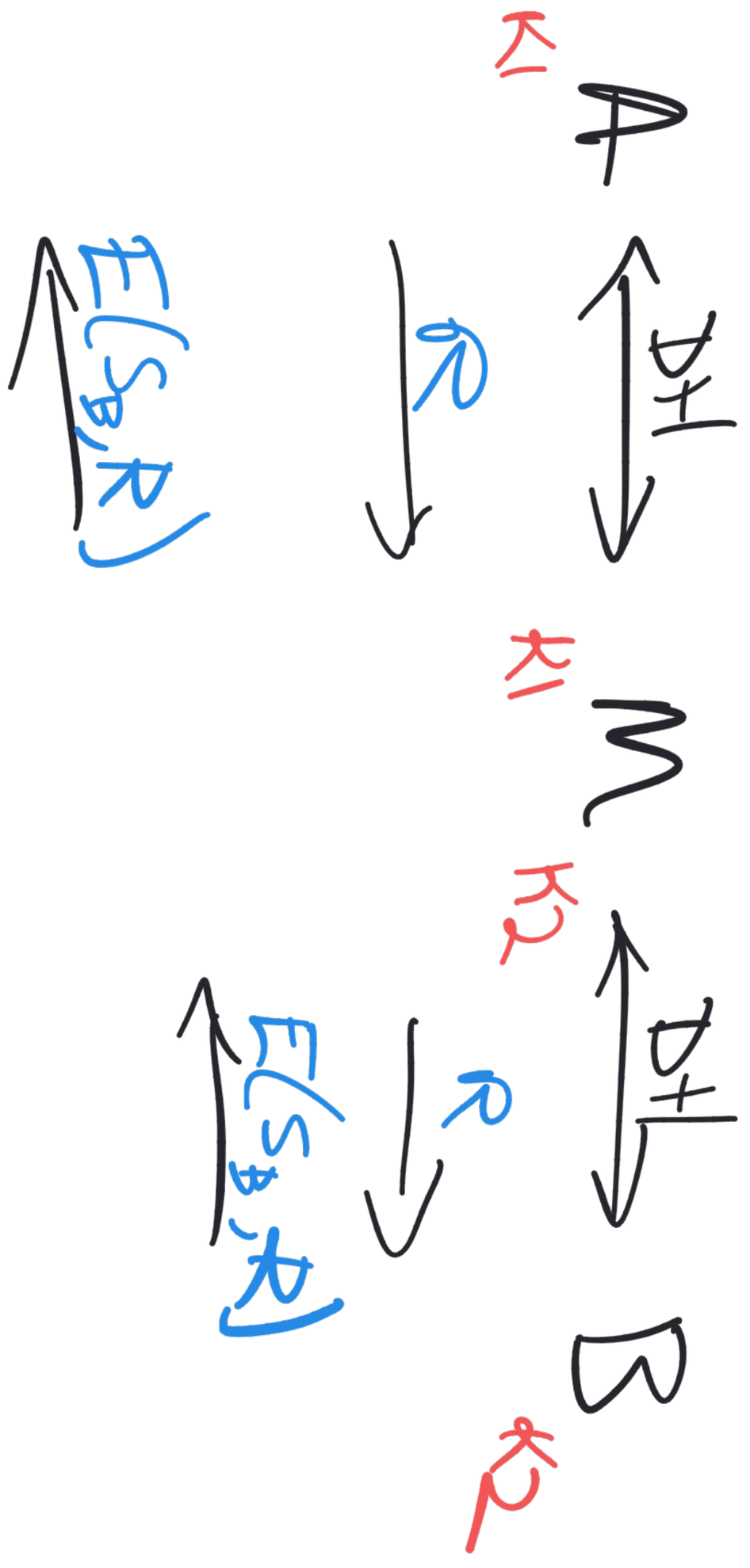



g, p, g^a mod p
A
B
g^b mod p
E

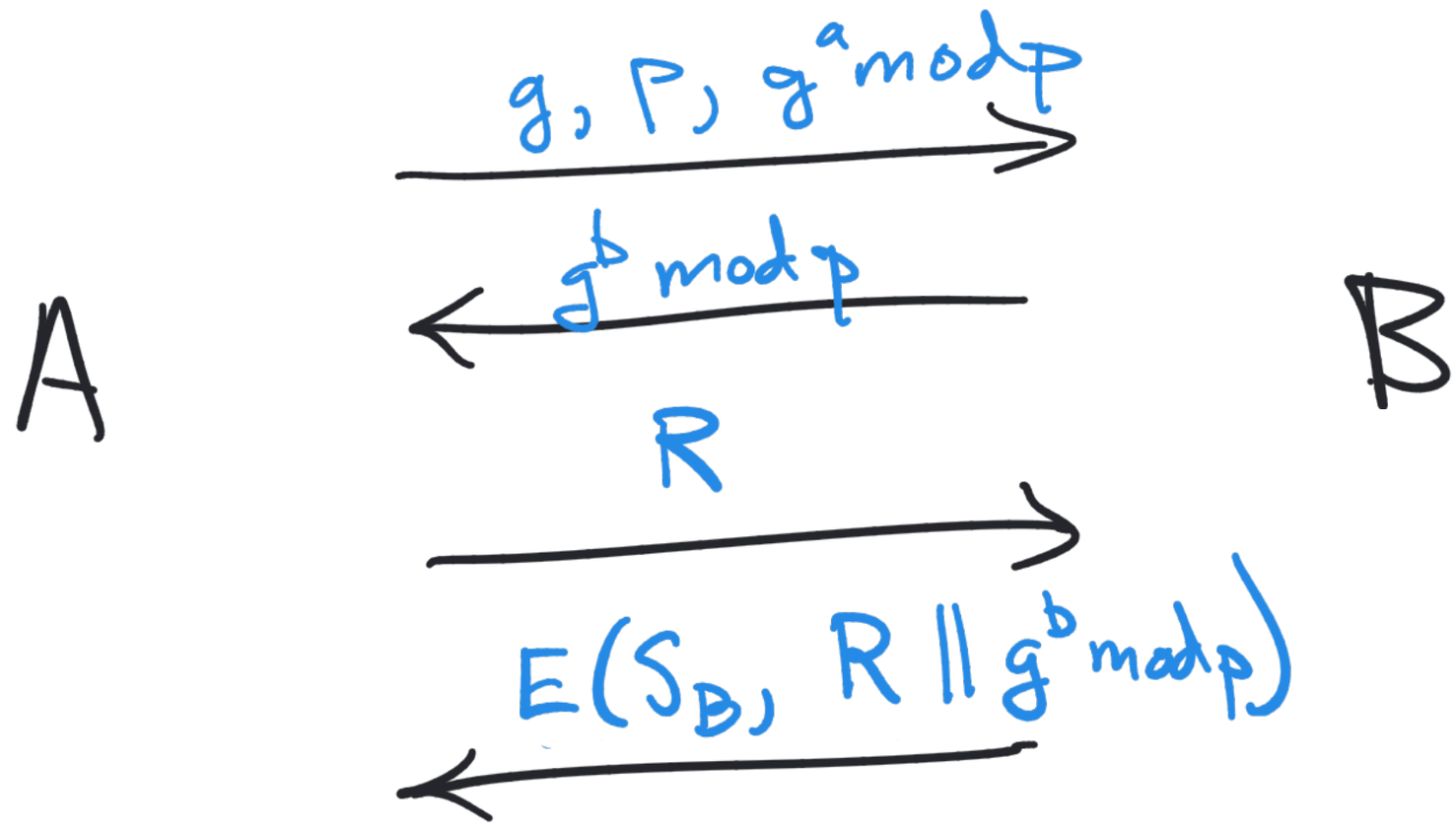

A
M
B
K1
K1
≠
K2
K2

Protocol 2.1 : DH + challenge

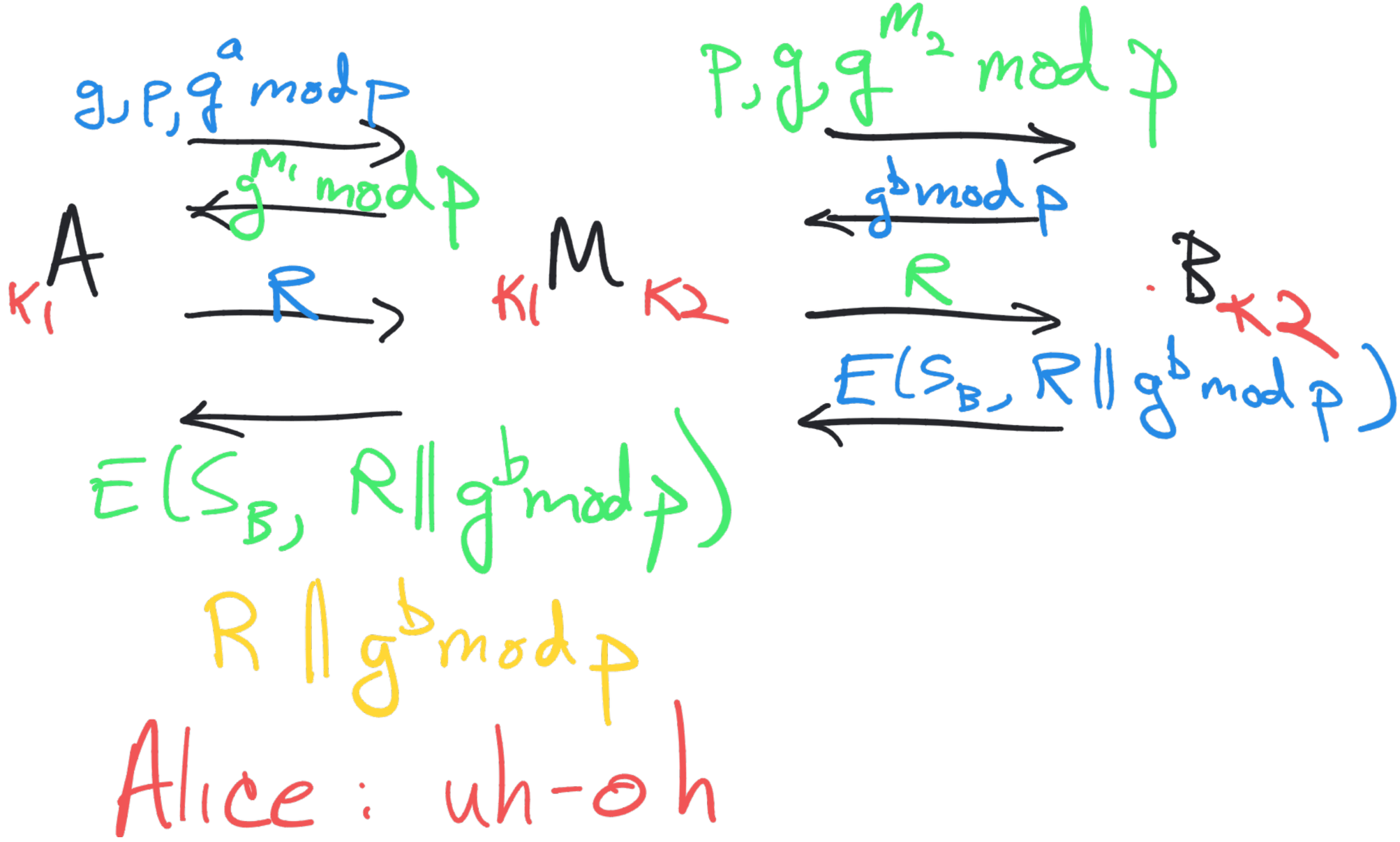




Protocol 2.2: DH + challenge



Realistically: $E(S_B, H(R \| g^b \bmod p))$



$R \| g^b \bmod p$

Alice: uh-oh

TLS 1.3 RFC 8446

(ECDHE (Elliptic Curve Diffie-Hellman Exchange)

vs.

PSK Pre-shared key