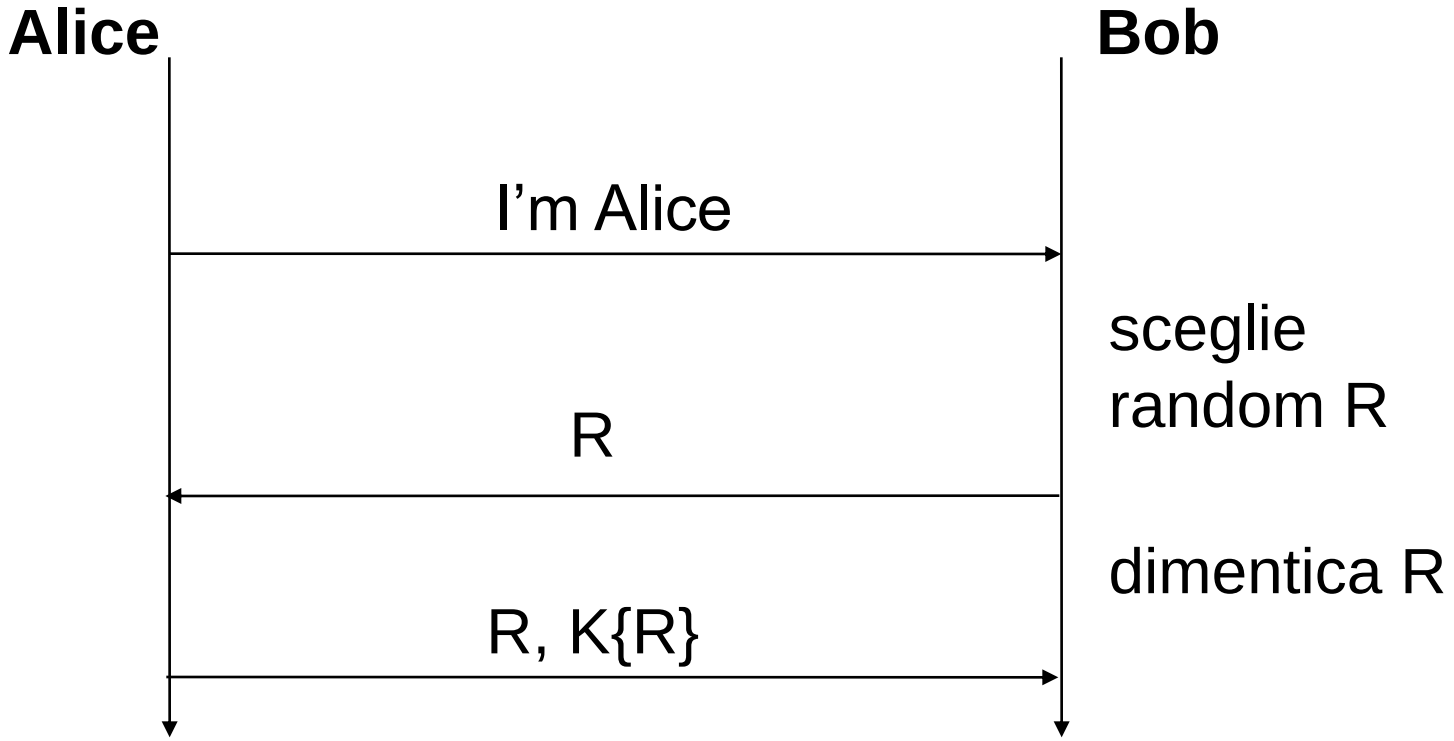
esercizi su metodi crittografici

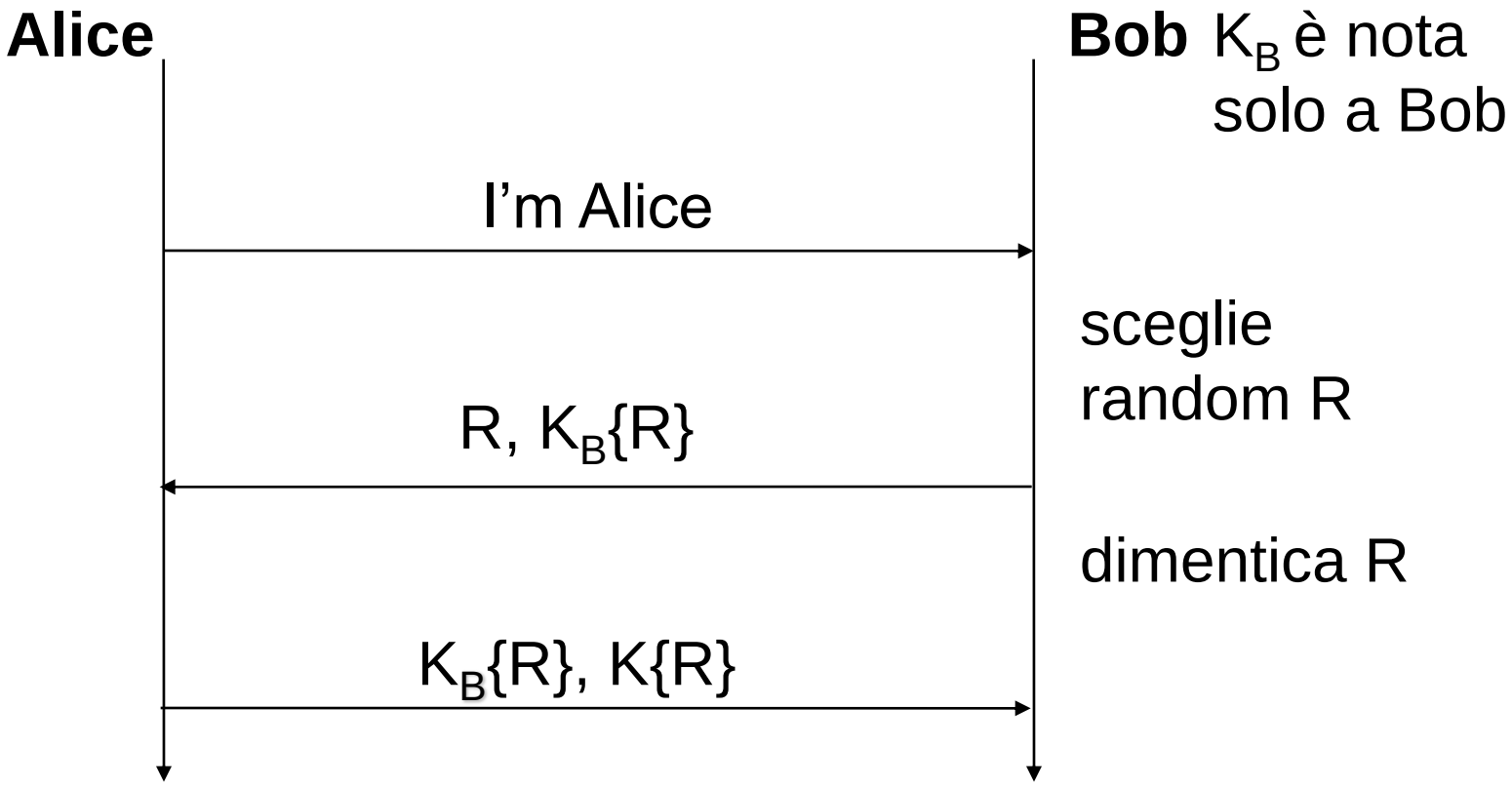
server statelss e autenticazione del client (1)

- supponi che B debba essere è un server stateless per evitare DoS
- K shared secret
- il seguente protocollo è vulnerabile?



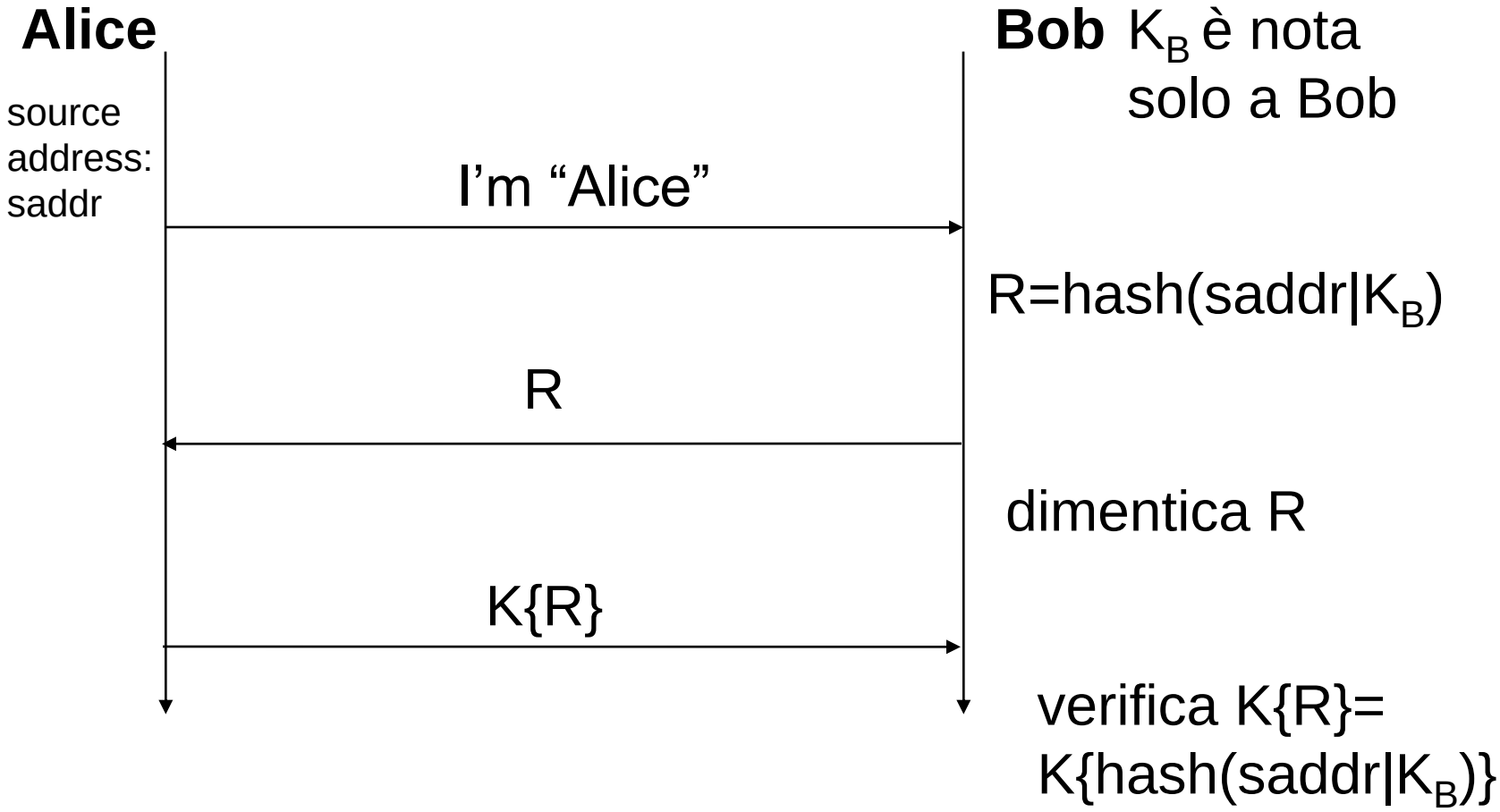
server statelss e autenticazione del client (2)

- il seguente protocollo è vulnerabile?



server statelss e autenticazione del client (3)

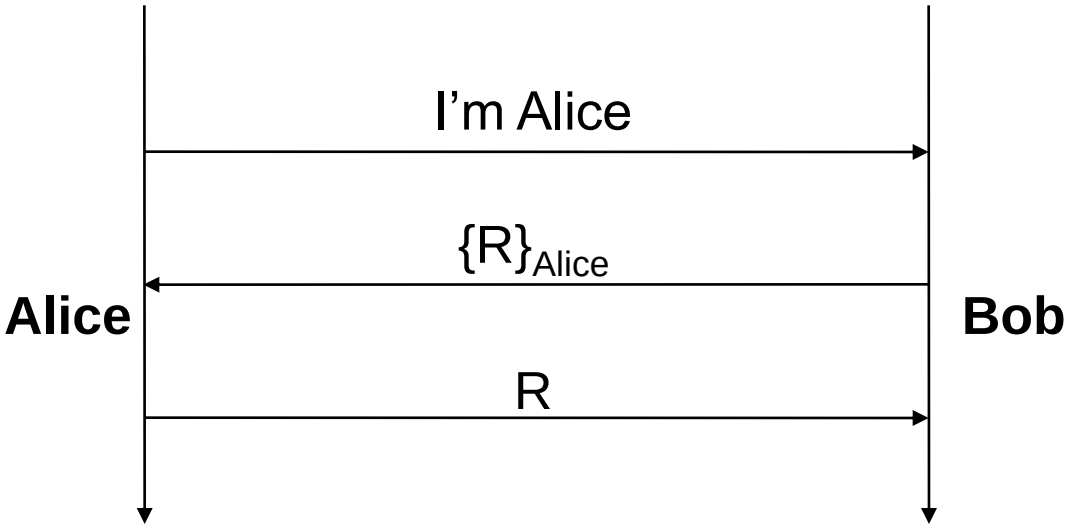
- il seguente protocollo è vulnerabile?



p2 non vulnerabile

- il protocollo p2 permette un attacco known plaintext
- modifica il protocollo in modo che tale attacco non sia possibile

protocollo p2



mutua autenticazone con chiave pubblica

- supponi che sia A e B abbiano ciascuno una chiave privata
- dai un protocollo di mutua autenticazione
- dai un protocollo di scambio di chiavi in cui sia A che B concorrono alla creazione del master secret
- analizza le vulnerabilità rispetto ad attacchi reply, reflection, hijacking

efficienza

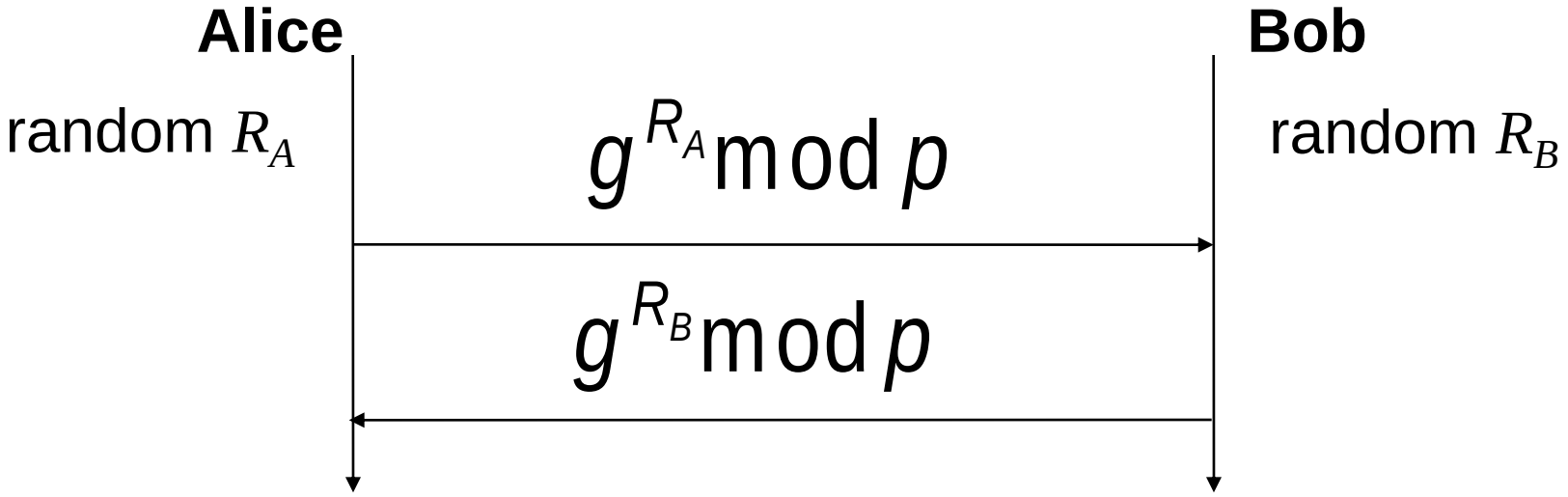
dai un protocollo con le stesse caratteristiche del precedente che preveda due soli messaggi

chiavi effimere

- supponi che sia A e B abbiano ciascuno una chiave privata RSA
- mostra un protocollo di autenticazione e scambio di chiavi con che goda di PFS

diffie-hellman

- p e g due numeri pubblicamente noti
  - devono avere delle proprietà particolari ma non ci interessano
- il logaritmo mod p in base g è difficile da calcolare



$$\left(g^{R_B}\right)^{R_A} = g^{R_A R_B} \bmod p \qquad \left(g^{R_A}\right)^{R_B} = g^{R_A R_B} \bmod p$$

chiavi effimere DH

- generare chiavi effimere RSA è inefficiente
- supponi che sia A e B abbiano ciascuno una chiave privata RSA
- mostra un protocollo di autenticazione e scambio di chiavi che
  - si avvalga di DH
  - goda di PFS usi DH
  - preveda soli due messaggi