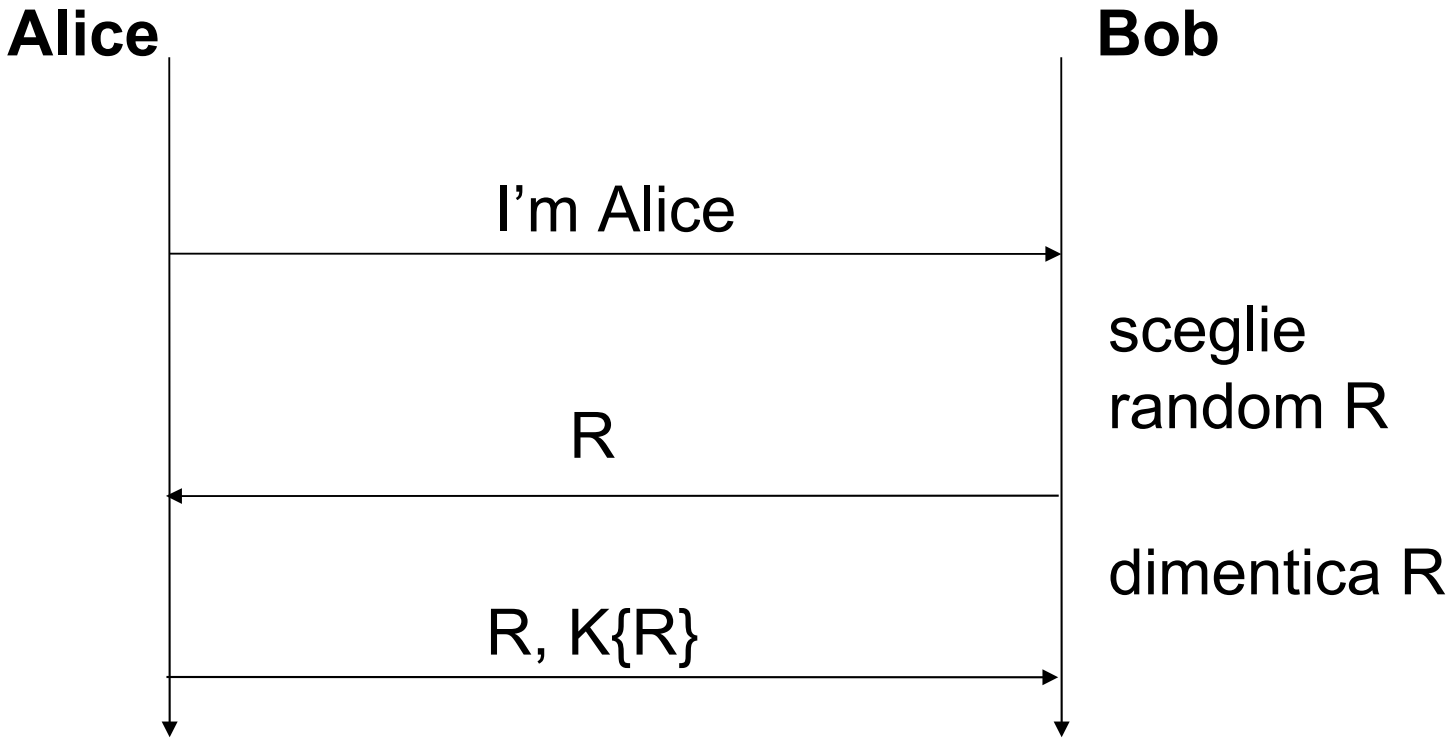
esercizi su metodi crittografici

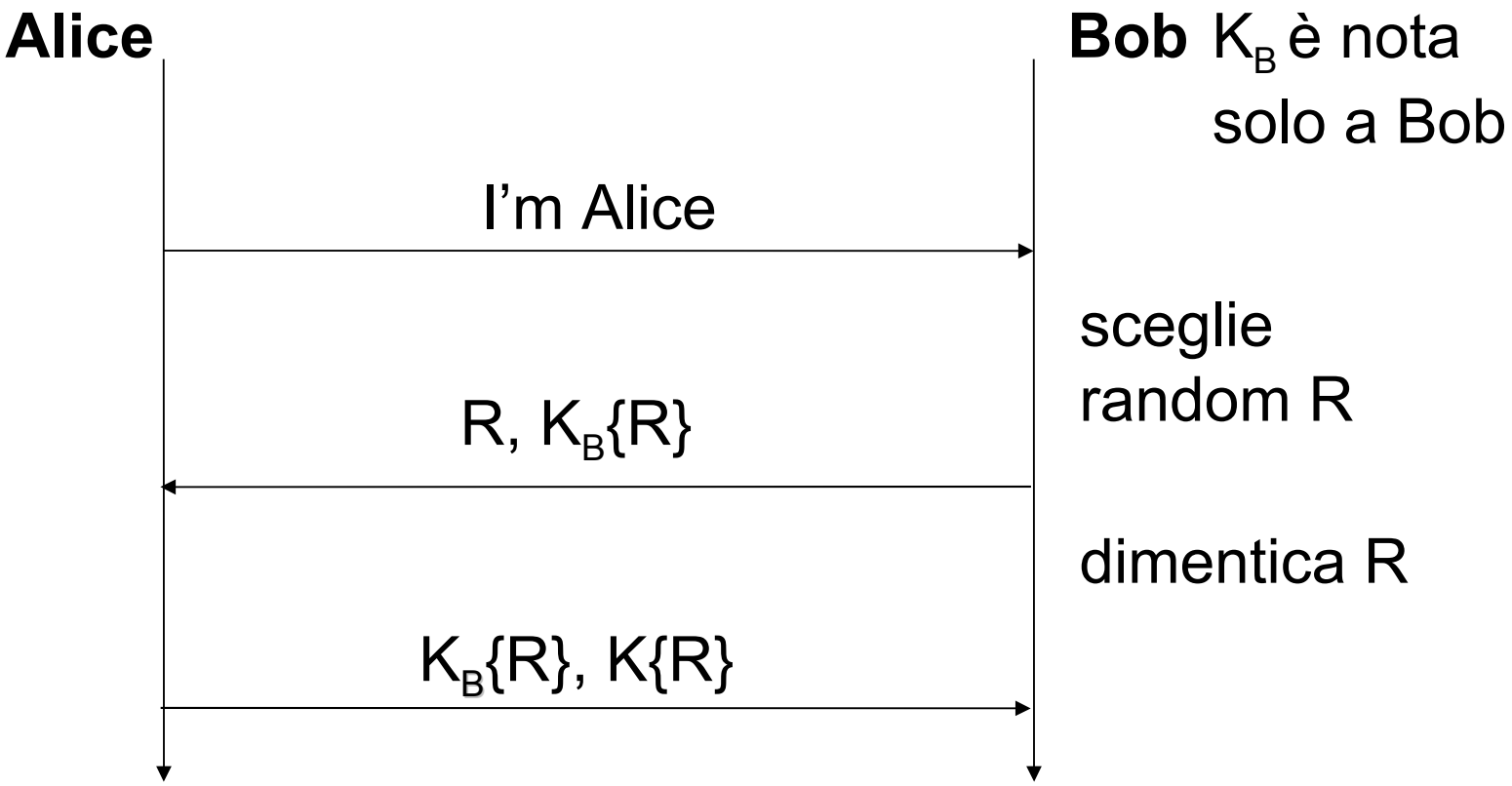
server statelss e autenticazione del client (1)

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



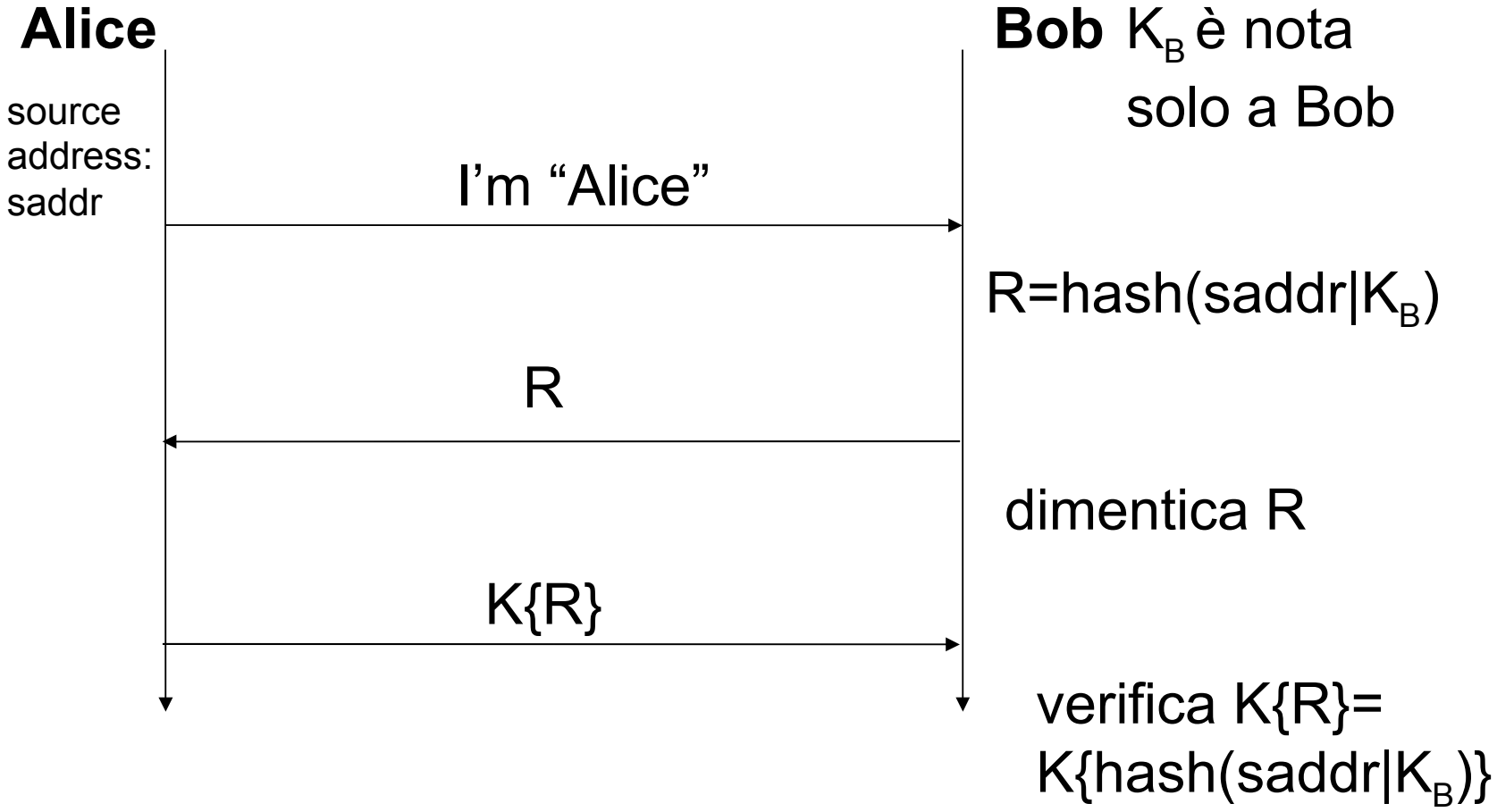
server statelss e autenticazione del client (2)

1 il seguente protocollo è vulnerabile?



server statelss e autenticazione del client (3)

1 il seguente protocollo è vulnerabile?

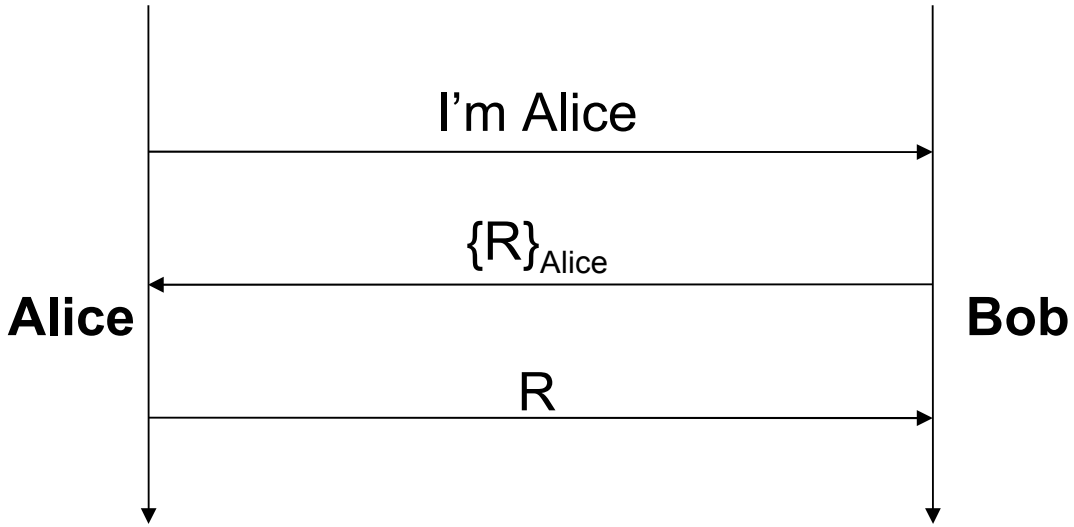


p2 non vulnerabile

1 il protocollo p2 permette un attacco known plaintext

2 modifica il protocollo in modo che tale attacco non sia possibile

protocollo p2



mutua autenticazone con chiave pubblica

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

efficienza

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

intercettazioni legali (key escrow)

1. supponi che per legge esista un repository “fidato” di tutte le chiavi private (key escrow)
2. la magistratura può autorizzare una intercettazione e richiedere le corrispondenti chiavi private
3. la tecnologia dovrebbe permettere alla magistratura di
   - decifrare le trasmissioni a partire dalla data di autorizzazione
   - impedire di decifrare trasmissioni precedenti alla data di autorizzazione (le autorizzazioni di intercettazione non sono retroattive)

esercizio: pubblicazione delle chiavi

1. dopo che le chiavi sono state usate possono essere pubblicate senza alterare la confidenzialità delle trasmissioni precedenti?
2. la domanda è importante: considera i seguenti casi pratici
   - supponi che un eavesdropper **registri** una trasmissione e poi ottenga la/le chiavi di A, B o di entrambi, può risalire al contenuto della trasmissione?
   - tipicamente le chiavi hanno una **scadenza** dopo la quale vanno cambiate, alla scadenza le chiavi private sono pubblicabili?
   - key escrow: la magistratura può ottenere il contenuto di registrazioni precedenti all'autorizzazione?

(perfect) forward secrecy (PFS)

1 un protocollo si dice avere la proprietà PFS se non permette di decifrare una trasmissione registrata pur avendo i segreti a lungo termine (chiavi di autenticazione) a disposizione.

2 analizza i protocolli precedenti rispetto a questa proprietà

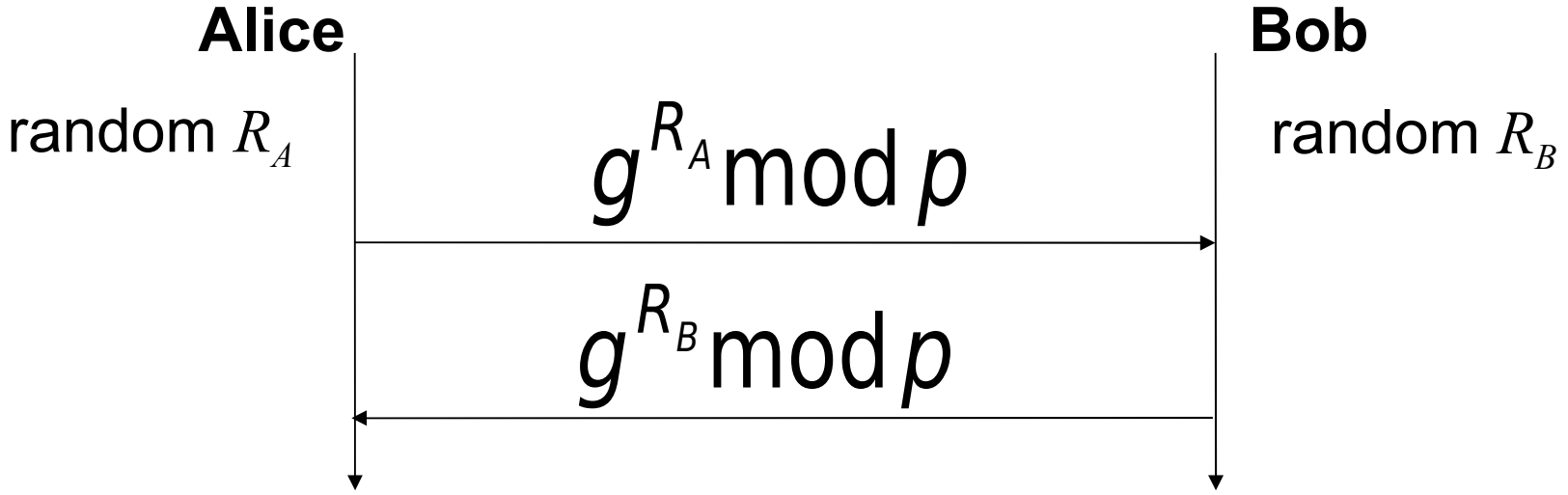
chiavi effimere

1 supponi che sia A e B abbiano ciascuno una chiave privata

2 mostra un protocollo con che goda di PFS

diffie-hellman

1. p e g due numeri pubblicamente noti
   - devono avere delle proprietà particolari ma non ci interessano
2. 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

1 supponi che sia A e B abbiano ciascuno una chiave privata

2 mostra un protocollo di autenticazione e scambio di chiavi che
  - si avvalga di DH
  - goda di PFS usi DH
  - preveda soli due messaggi