PUC Minas

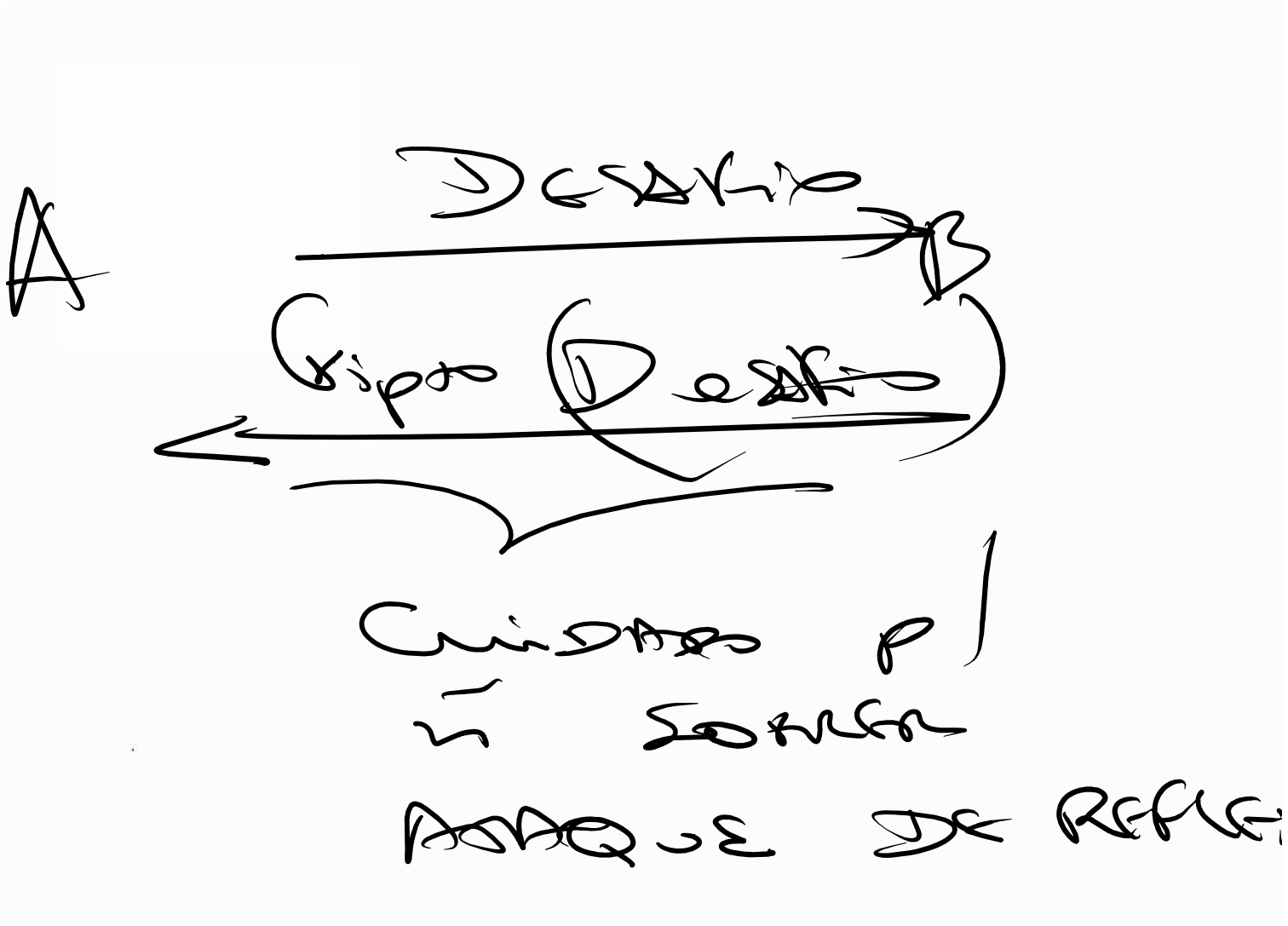
Protocolos de Autenticação

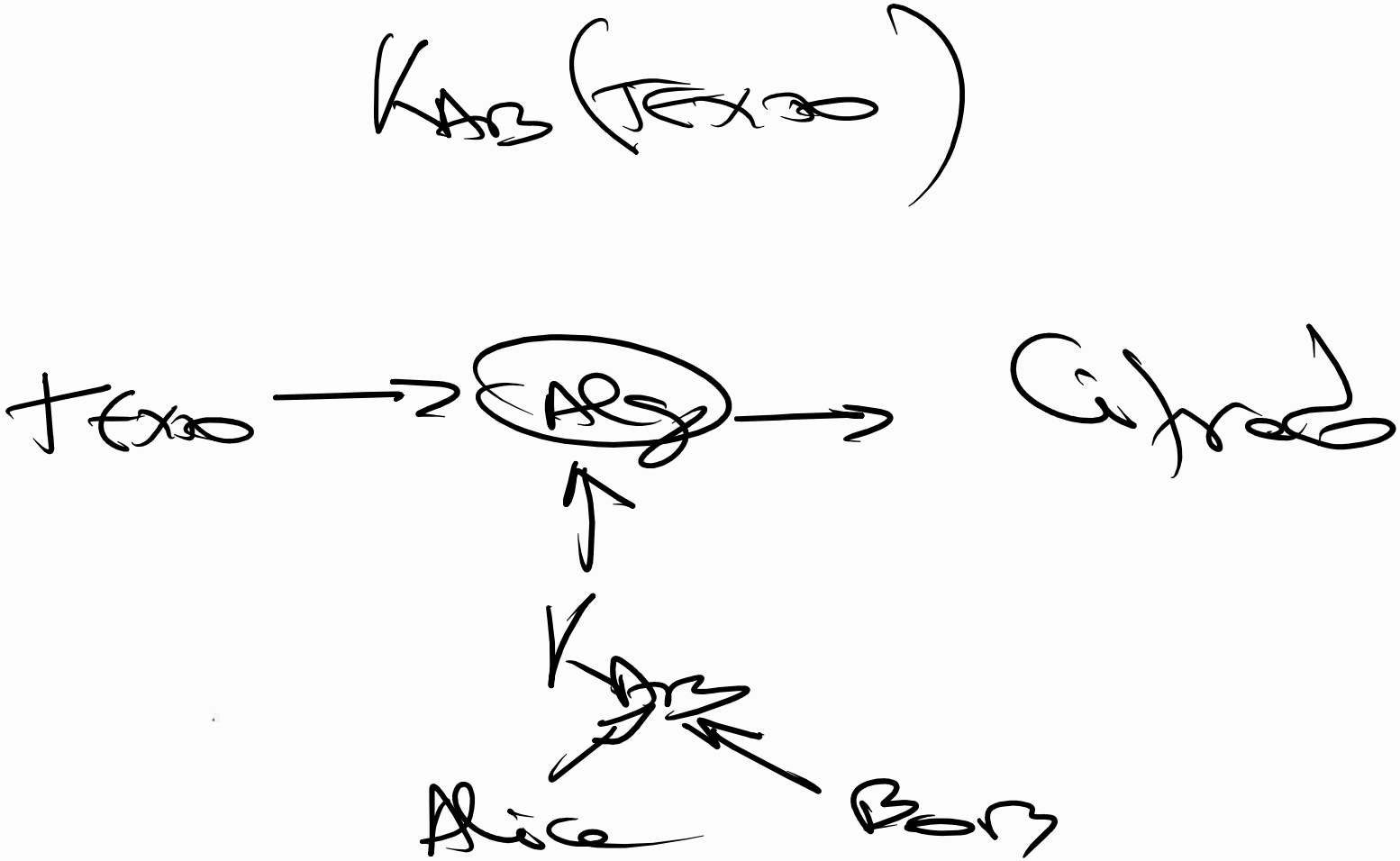
- Autenticação baseada em chave secreta compartilhada
  - Como estabelecer chave compartilhada: a troca de chave Diffie-Hellman
- Autenticação com o uso de centro de distribuição de chaves
  - Autenticação com a utilização de kerberos
- Autenticação com a criptografia de chave pública

Chave secreta compartilhada (1)

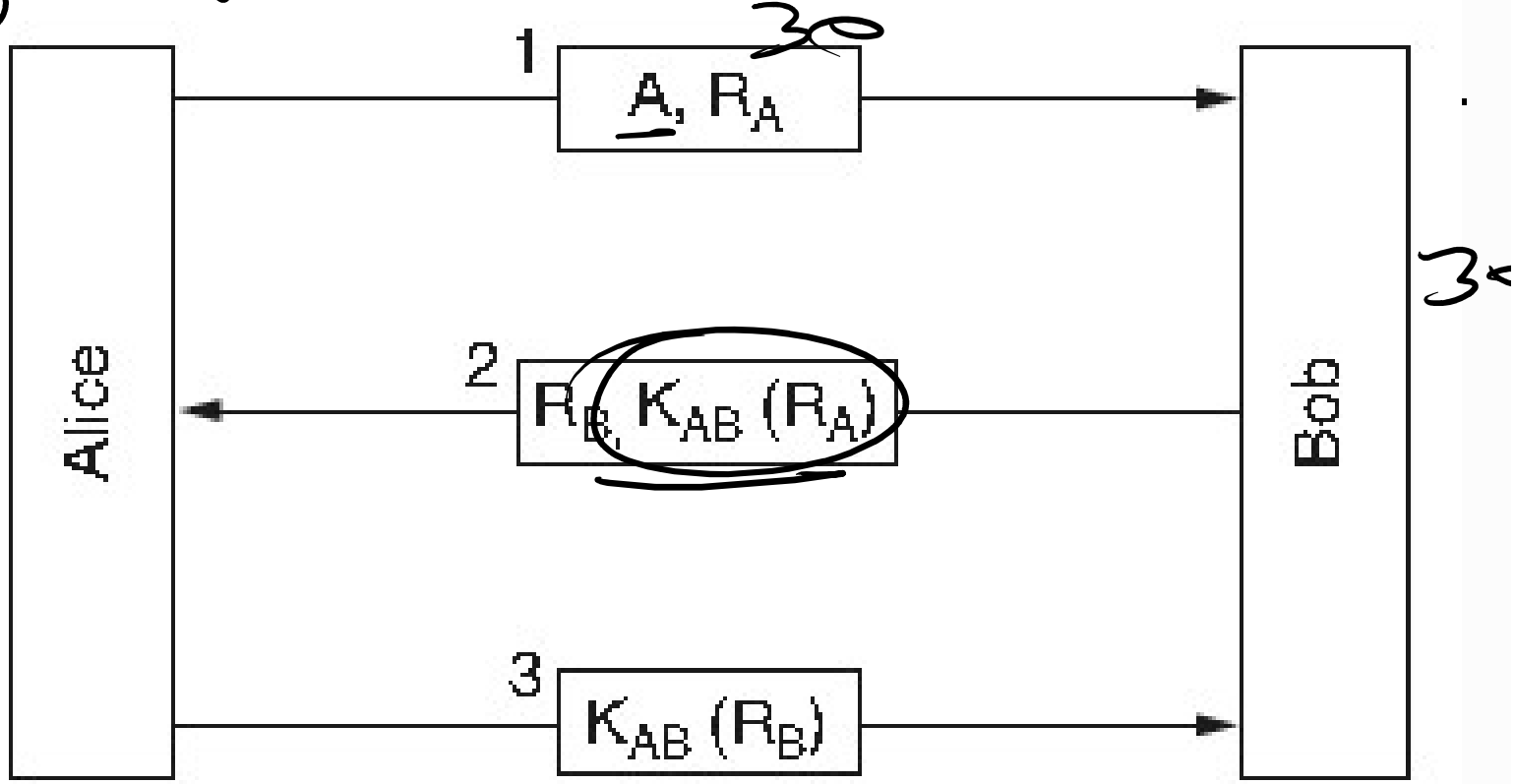
Notação usada nas apresentações subsequentes:

- *A* e *B* são as identidades de Alice e Bob
- R_i são os desafios e *i* identifica o desafiante
- K_i são chaves e *i* indica o proprietário
- K_S é a chave da sessão



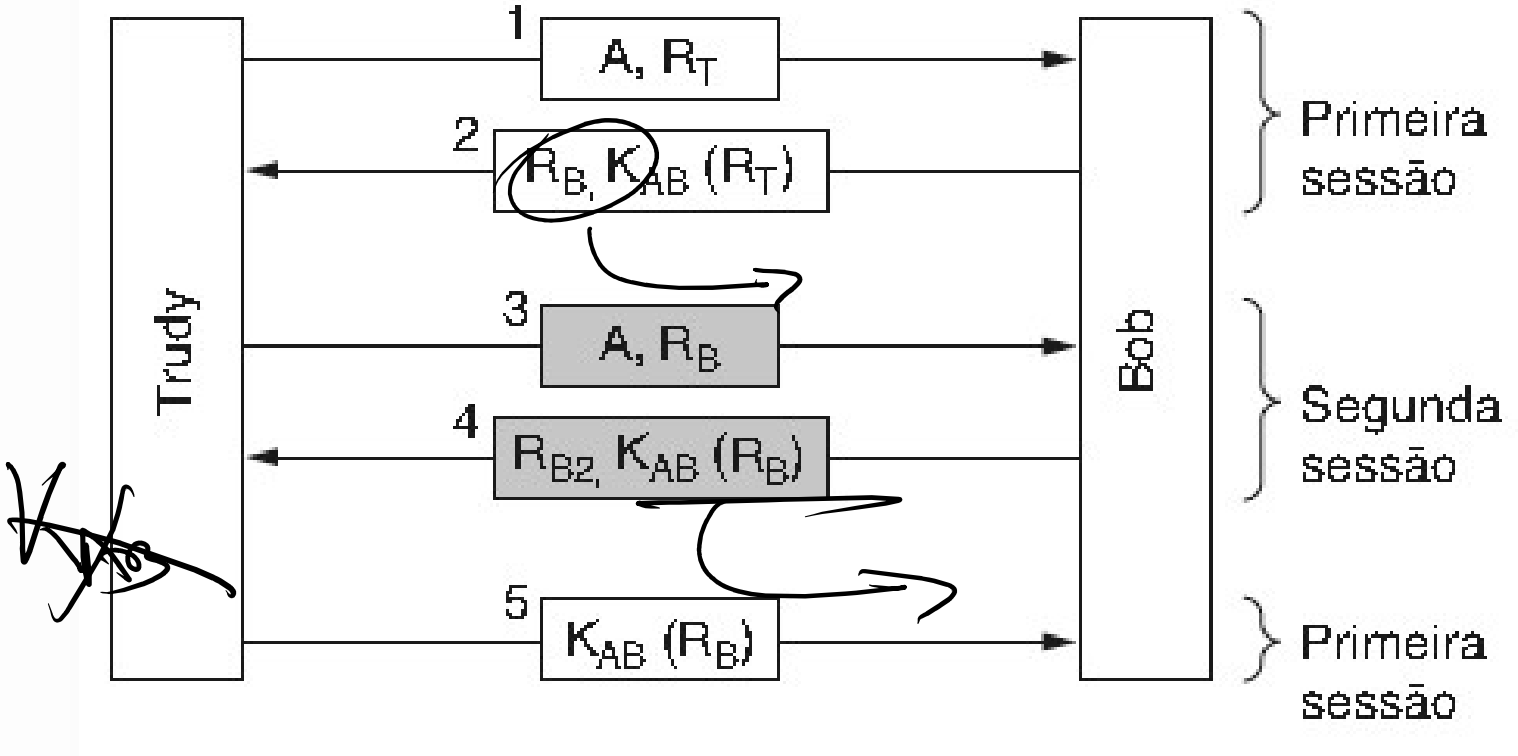


Chave secreta compartilhada (2)

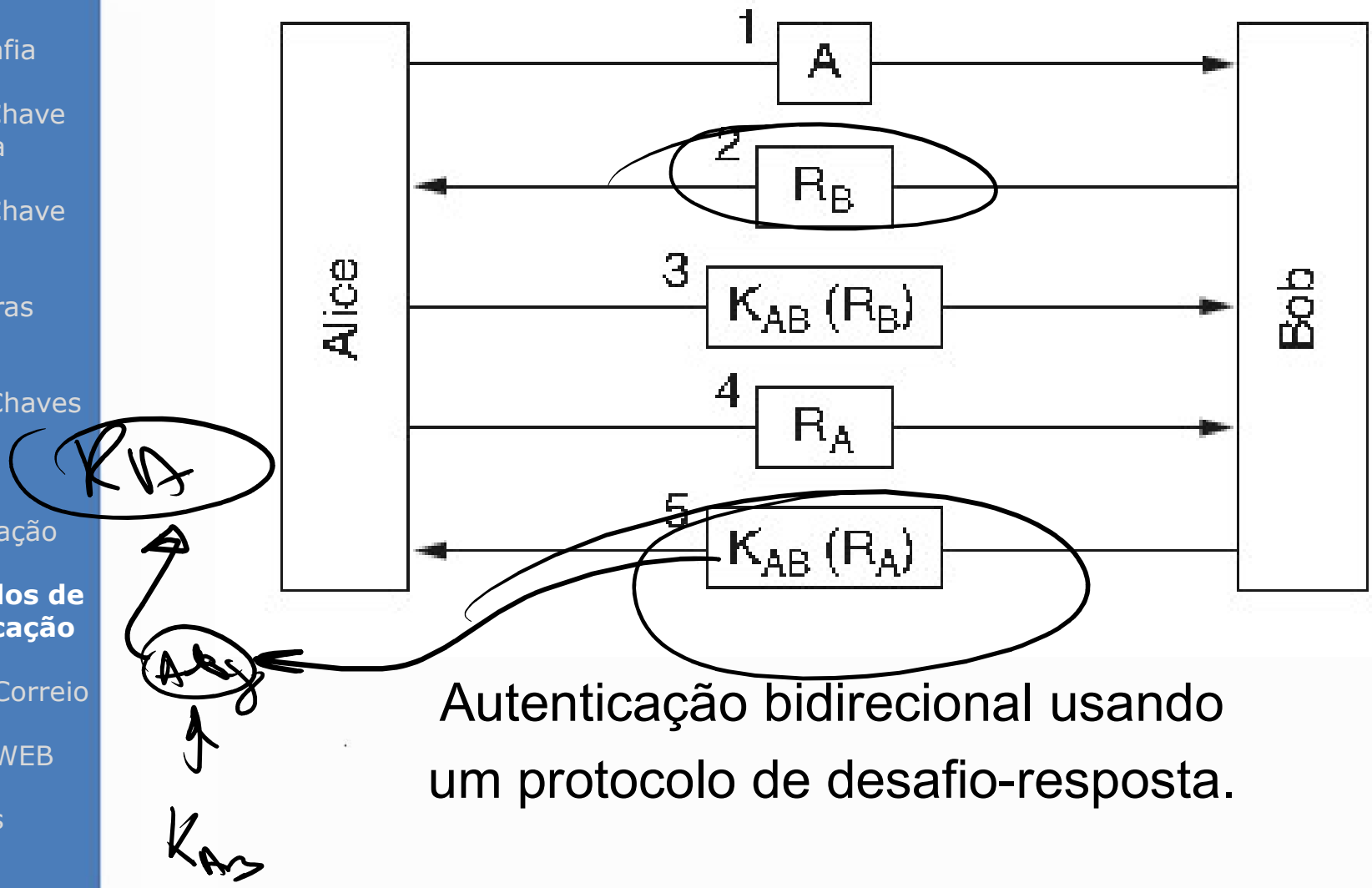


Chave secreta compartilhada (3)

O ataque por reflexão.

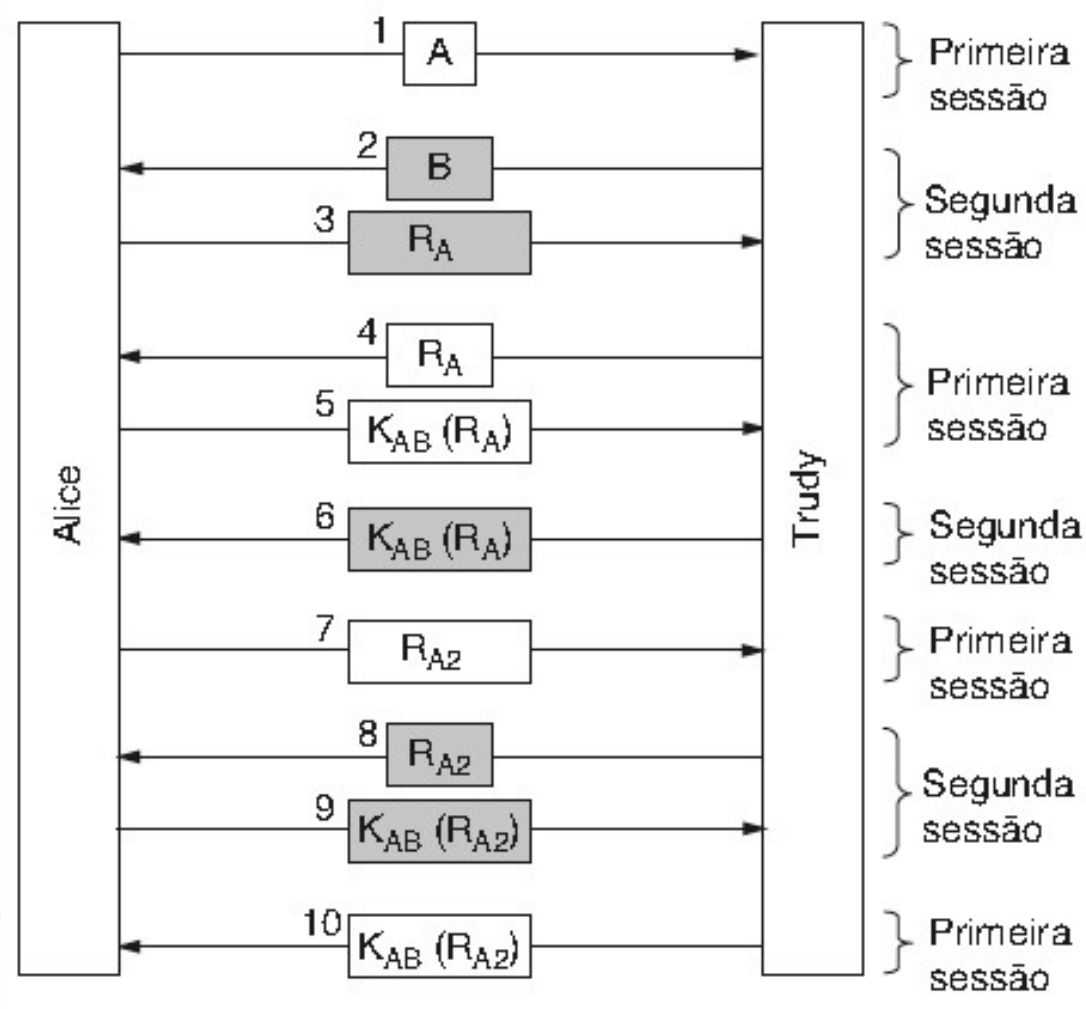


Chave secreta compartilhada (4)



Autenticação bidirecional usando um protocolo de desafio-resposta.

Chave secreta compartilhada (5)



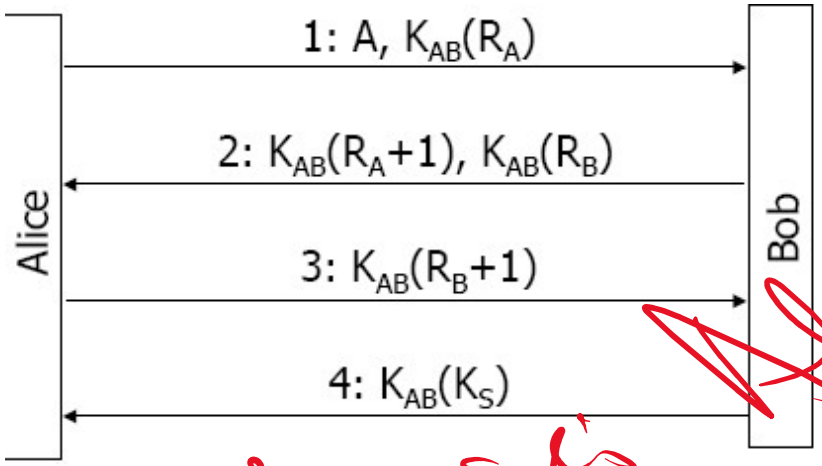
Ataque por reflexão

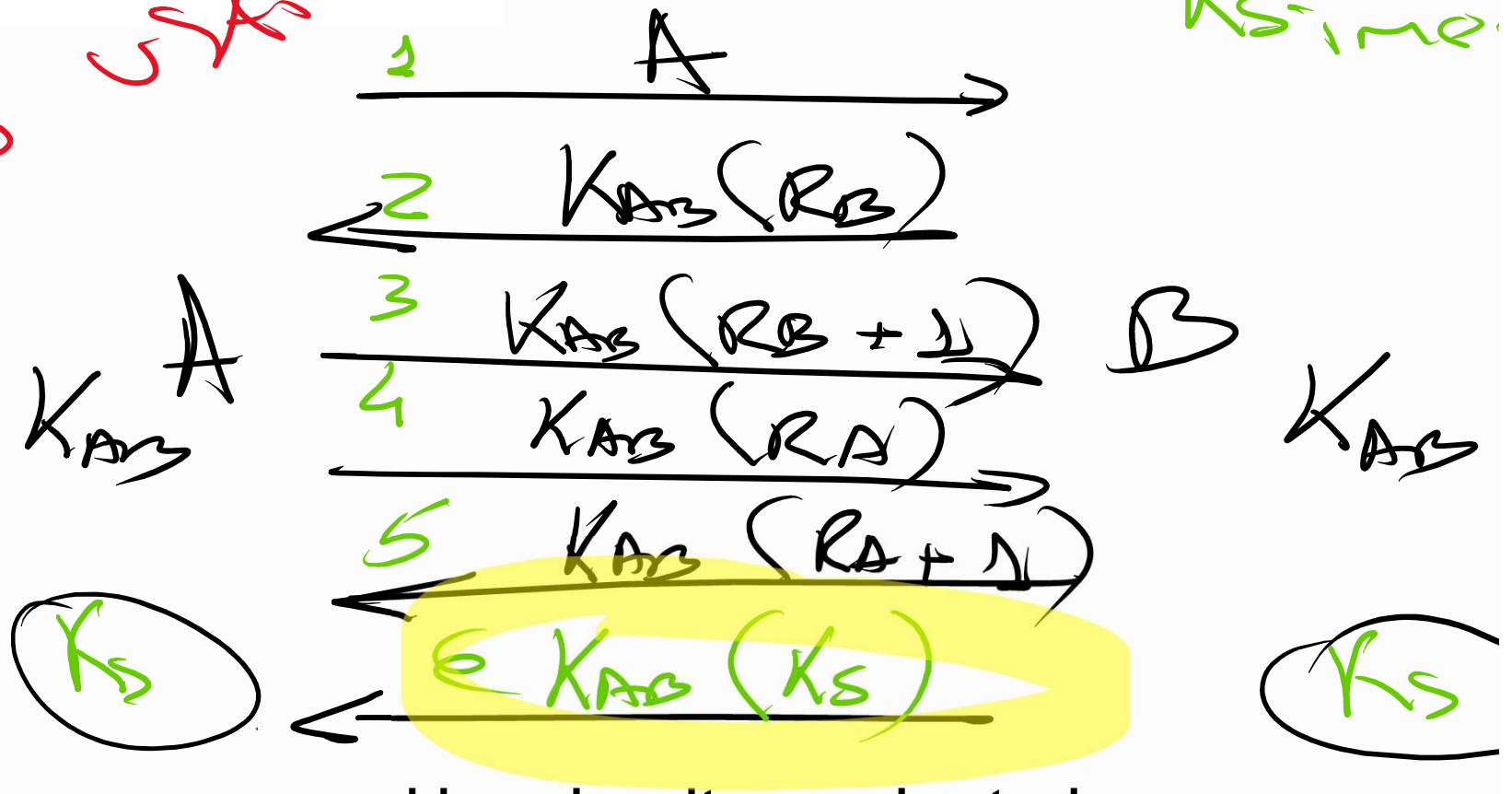
Chave secreta compartilhada (6)

Regras gerais de projeto:

1. Transmissor deve provar quem é antes de o receptor responder
2. Extrair os desafios de conjuntos distintos
3. Tornar o protocolo resistente a ataques por segunda sessão em paralelo

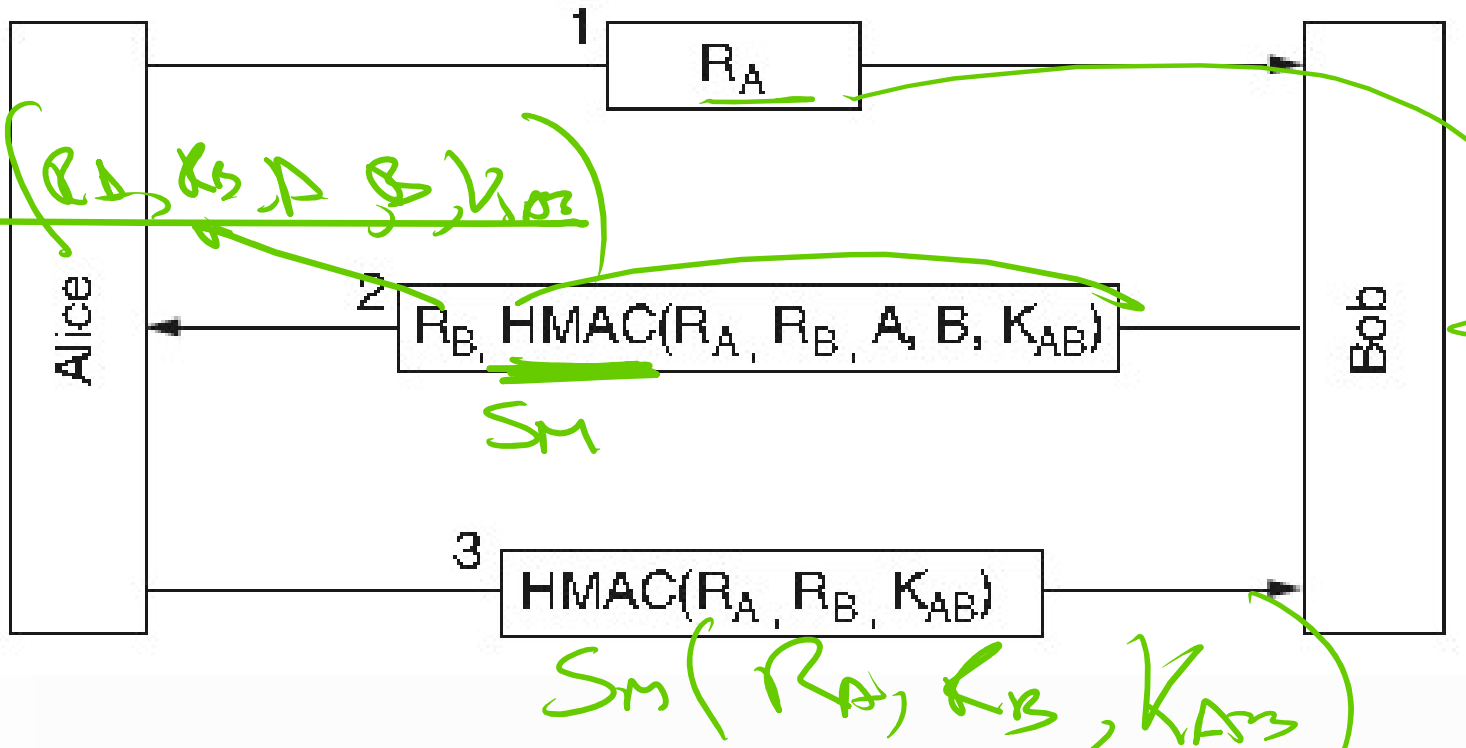
Chave secreta compartilhada (7)





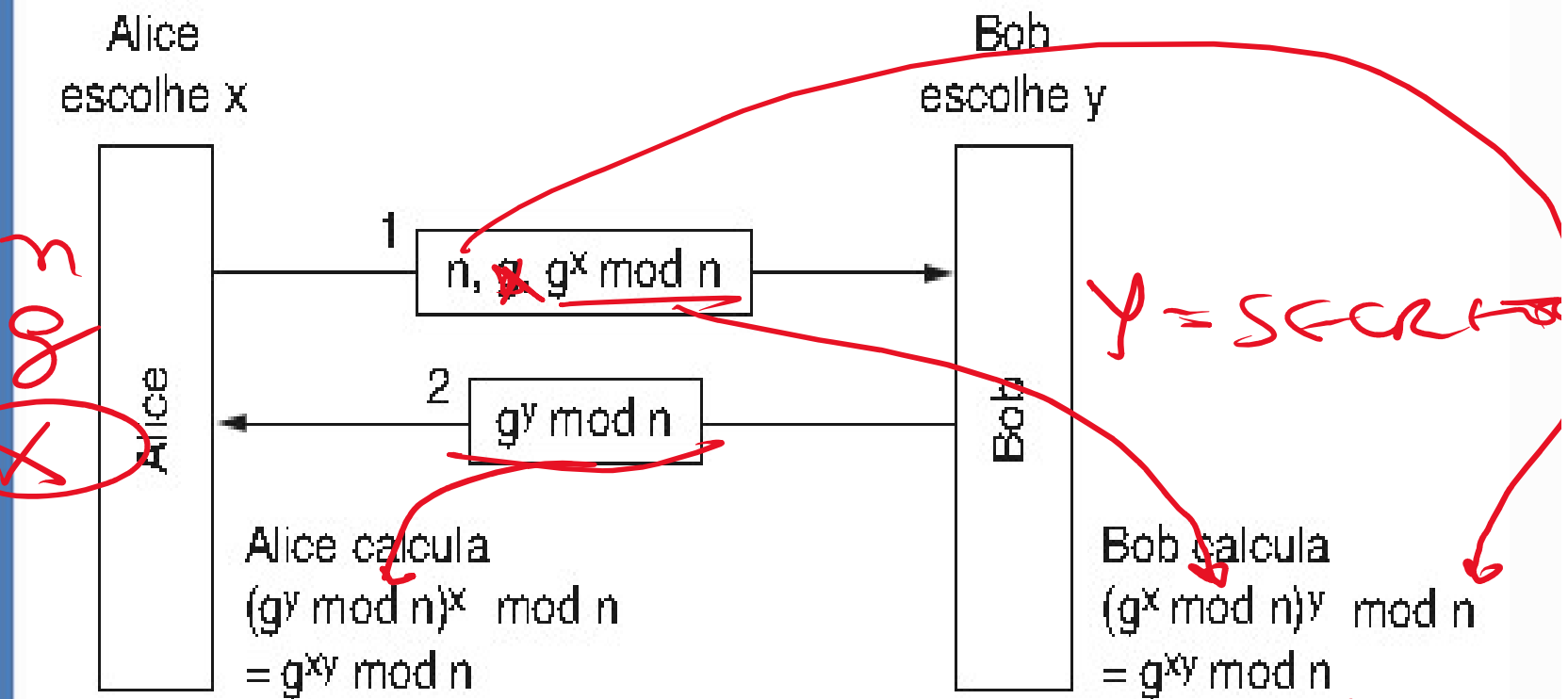
Um algoritmo adaptado

Chave secreta compartilhada (7)



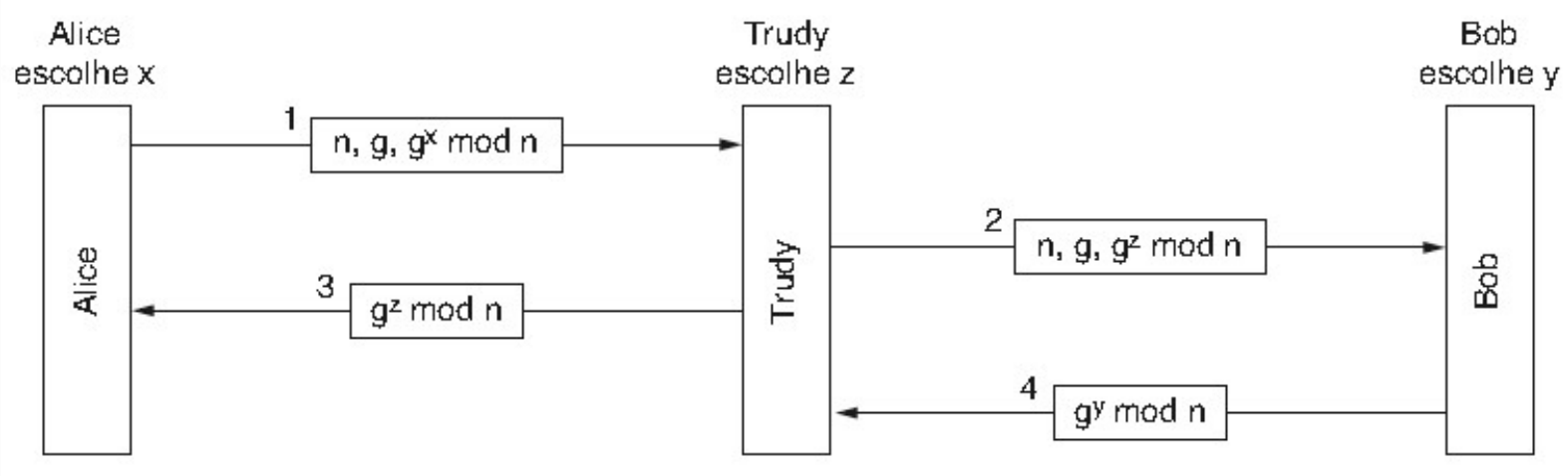
Autenticação usando HMACs.

A troca de chaves de Diffie-Hellman (1)



Troca de chaves de Diffie-Hellman.

A troca de chaves de Diffie-Hellman (2)



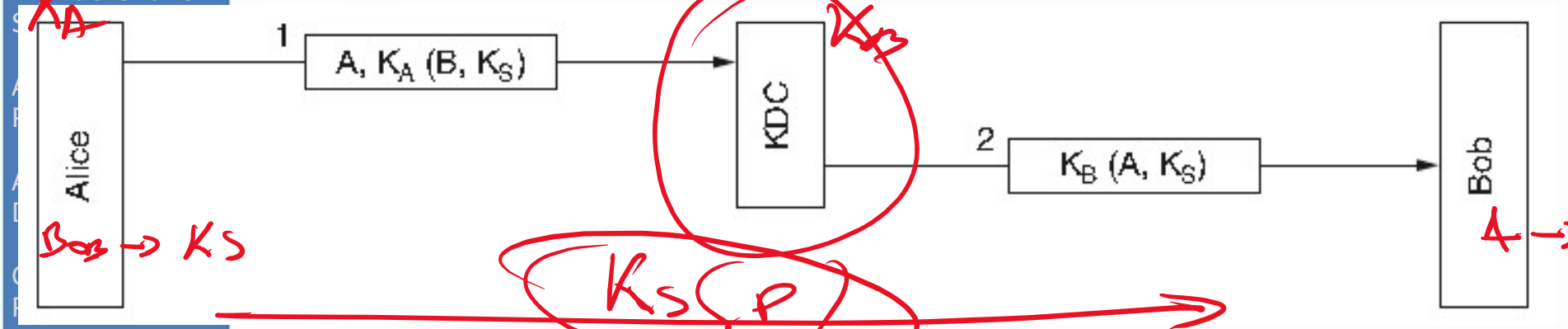
O ataque do homem no meio ou brigada de incêndio.

Resumo de protocolos de Autenticação até este momento

PUC Minas

- Ataques:
  - Reflexão
  - Homem do Meio
- Autenticação
  - Usando apenas alg simétrico
  - Usando Sumário de Msg e chave simétrica
- Diffie-Hellman para trocar chaves simétricas

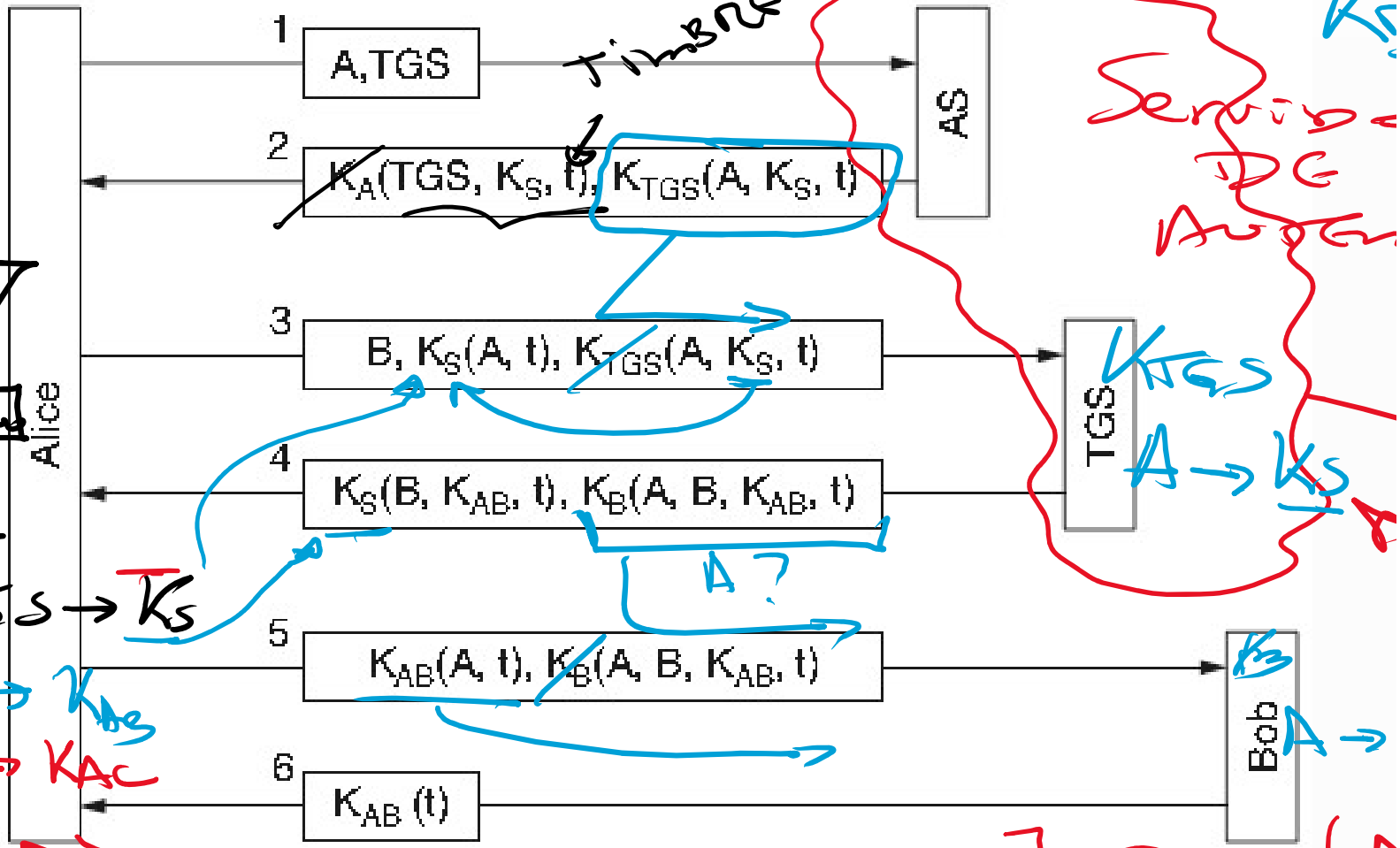
Centro de distribuição de chaves (1)



Primeira tentativa de protocolo de autenticação usando um KDC.

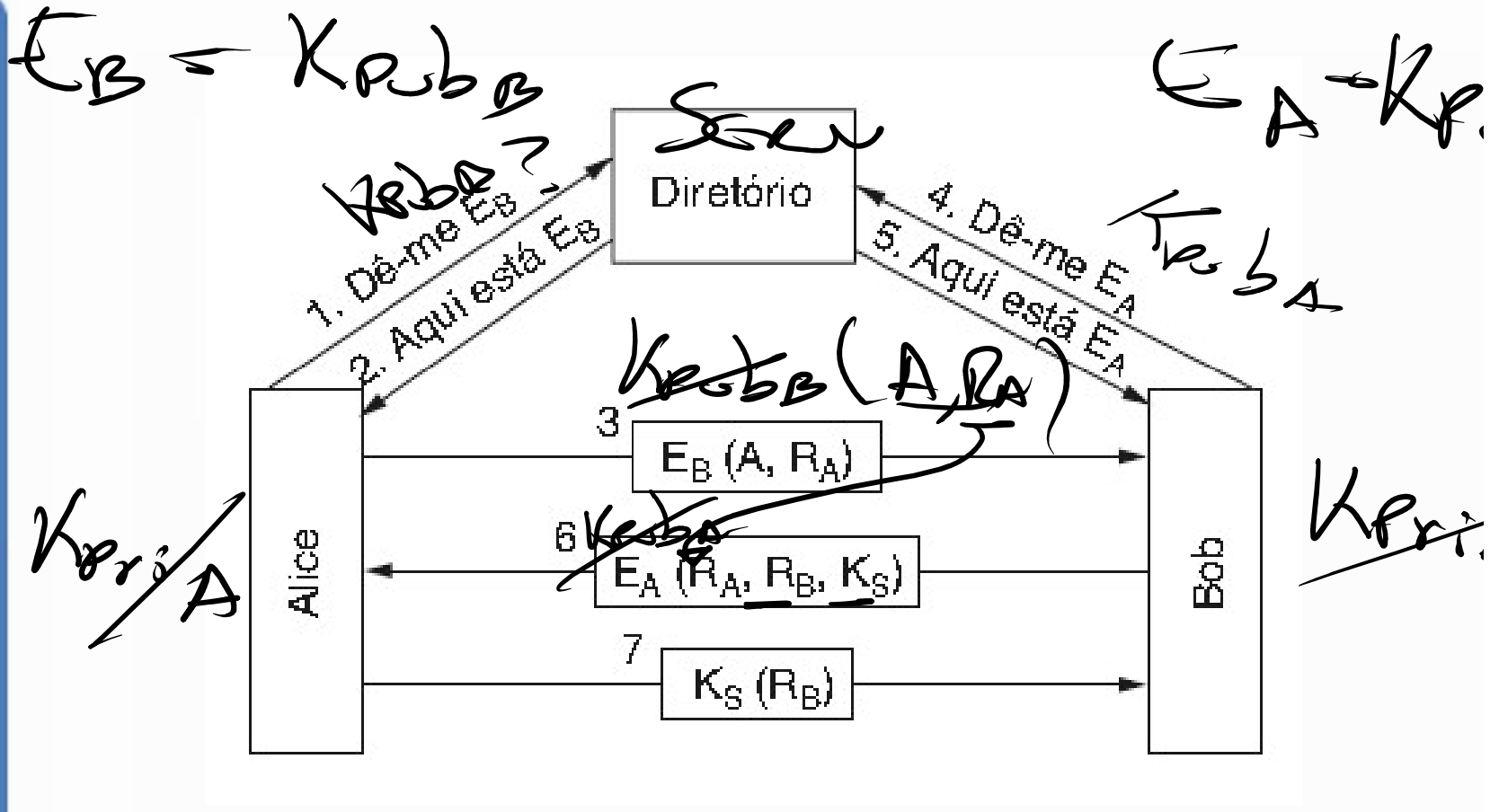
PROBLEMA: Ataque por Repetição!

Kerberos



Operação do Kerberos V5

Criptografia de chave assimétrica



Autenticação mútua usando criptografia de chave pública.

Resumo de protocolos de Autenticação

- Ataques:
  - Reflexão
  - Homem do Meio
  - Repetição para isto começo a colocar o t
- Autenticação
  - Usando apenas alg simétrico
  - Usando Sumário de Msg e chave simétrica
  - Usando Centro de Distribuição de Chaves == kerberos (KDC)
  - Usando Alg assimétricos
- Diffie-Hellman para trocar chaves simétricas