

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

- 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)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

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



PUC Minas

Sumário

Criptografia

Alg. de Chave
Simétrica

Alg. de Chave
Pública

Assinaturas
Digitais

Ger. de Chaves
Públicas

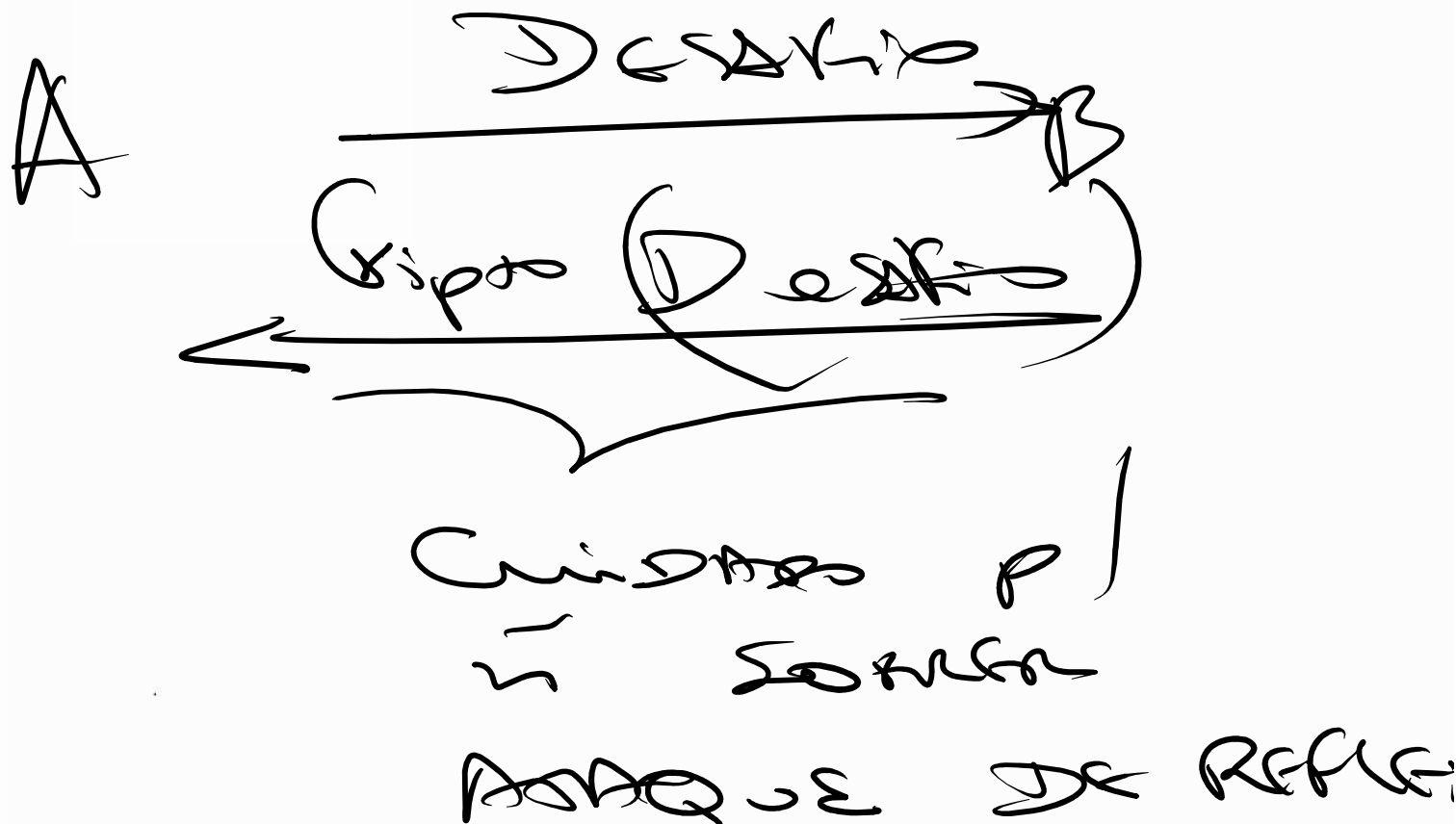
Seg. da
Comunicação

**Protocolos de
Autenticação**

Seg. de Correio

Seg. da WEB

Questões
Sociais





PUC Minas

Sumário

Criptografia

Alg. de Chave
Simétrica

Alg. de Chave
Pública

Assinaturas
Digitais

Ger. de Chaves
Públicas

Seg. da
Comunicação

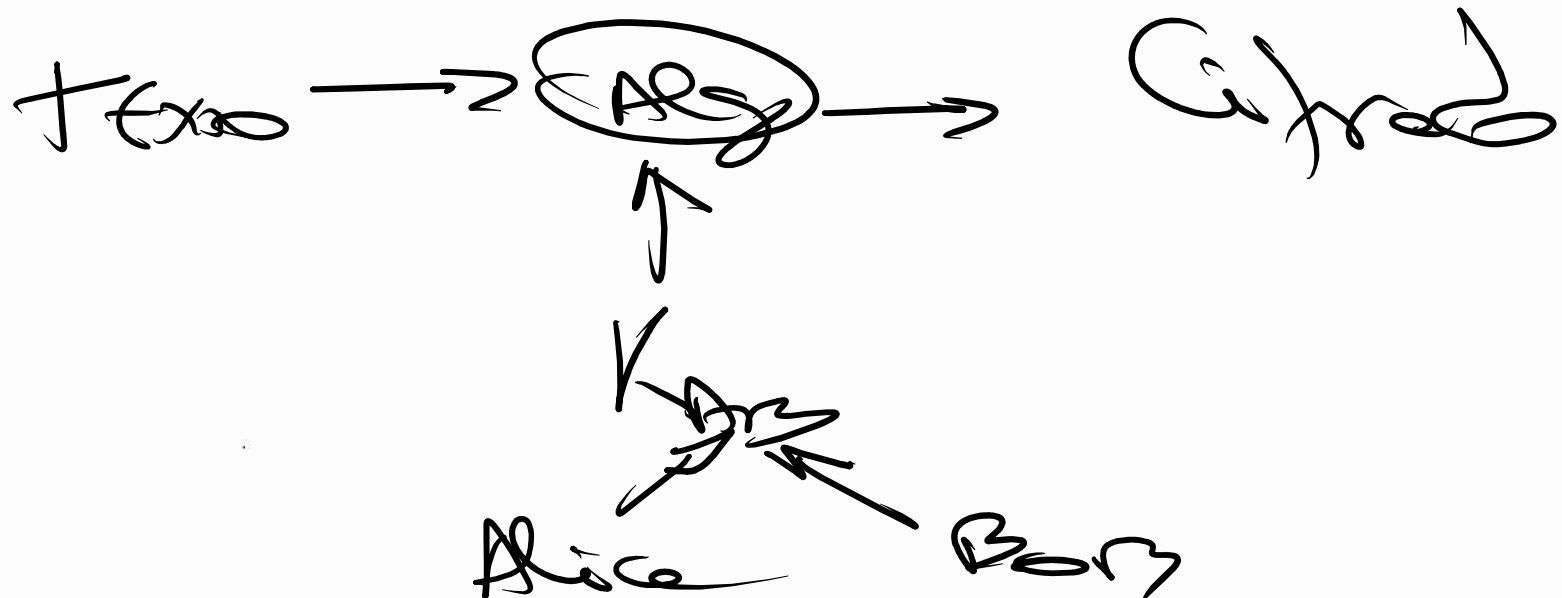
**Protocolos de
Autenticação**

Seg. de Correio

Seg. da WEB

Questões
Sociais

$K_{AB}(\text{Texto})$





PUC Minas

Chave secreta compartilhada (2)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

Seg. da Comunicação

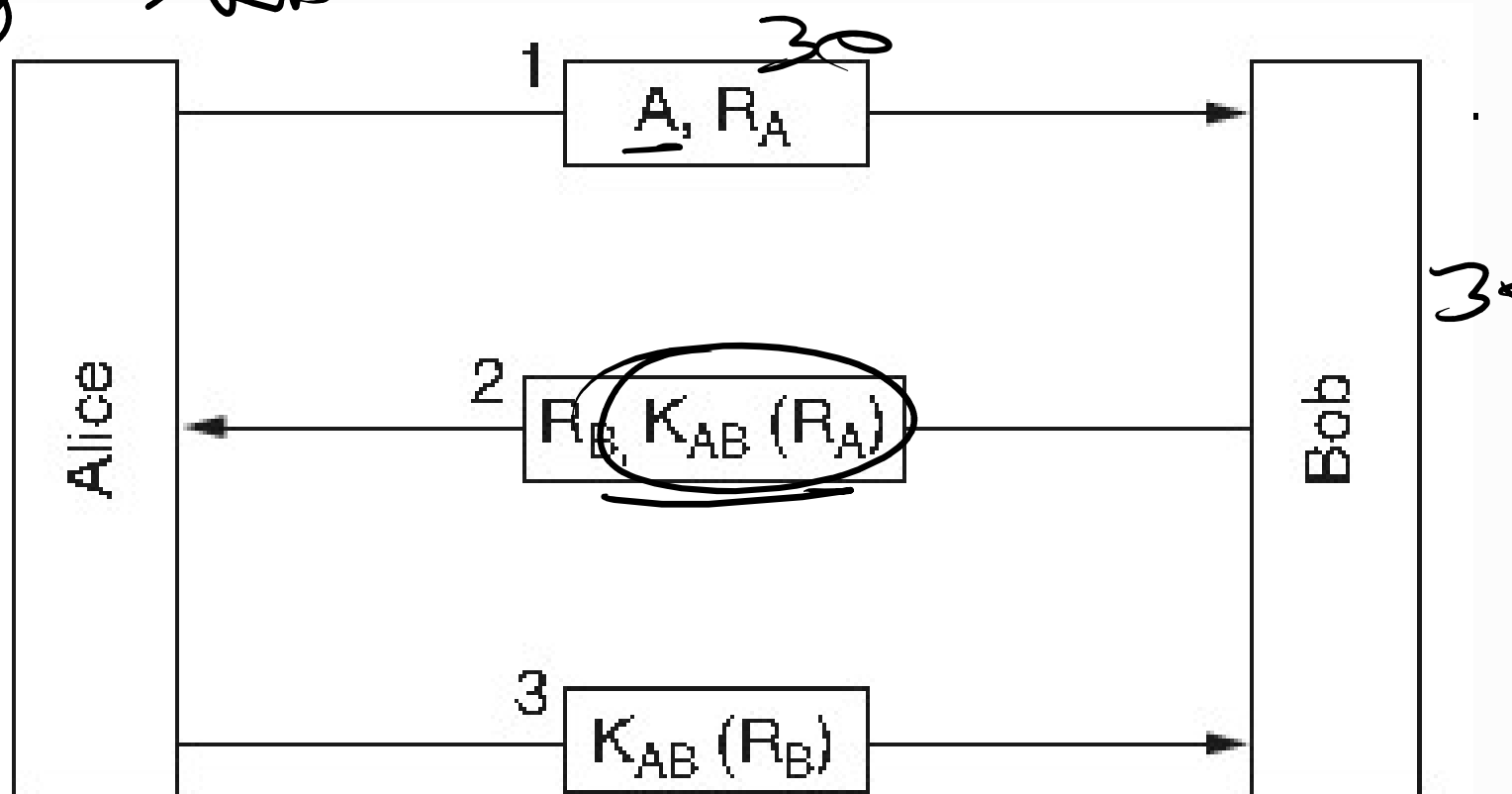
Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

~~K_{AB}~~
Alg → RA





PUC Minas

Chave secreta compartilhada (3)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

Seg. da Comunicação

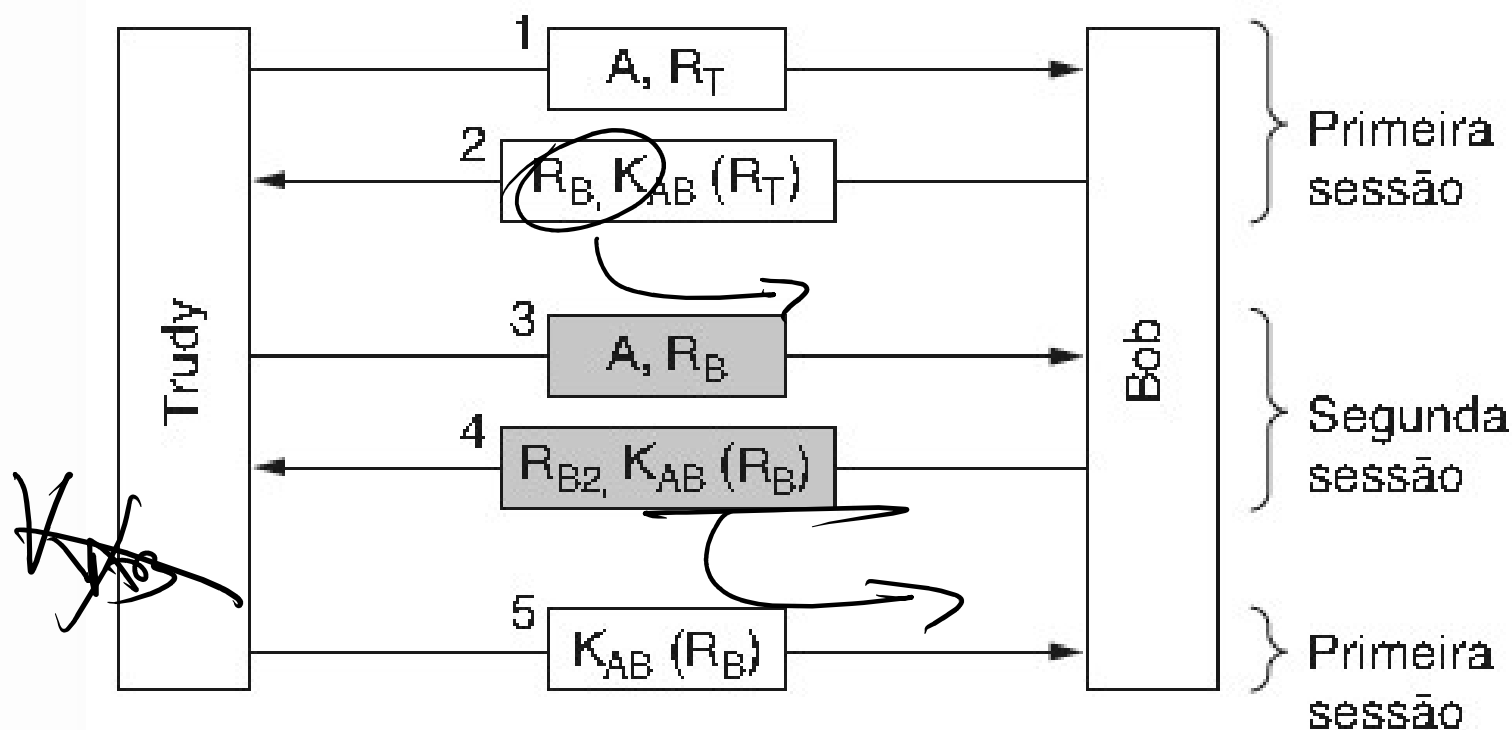
Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

O ataque por reflexão.





PUC Minas

Chave secreta compartilhada (4)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

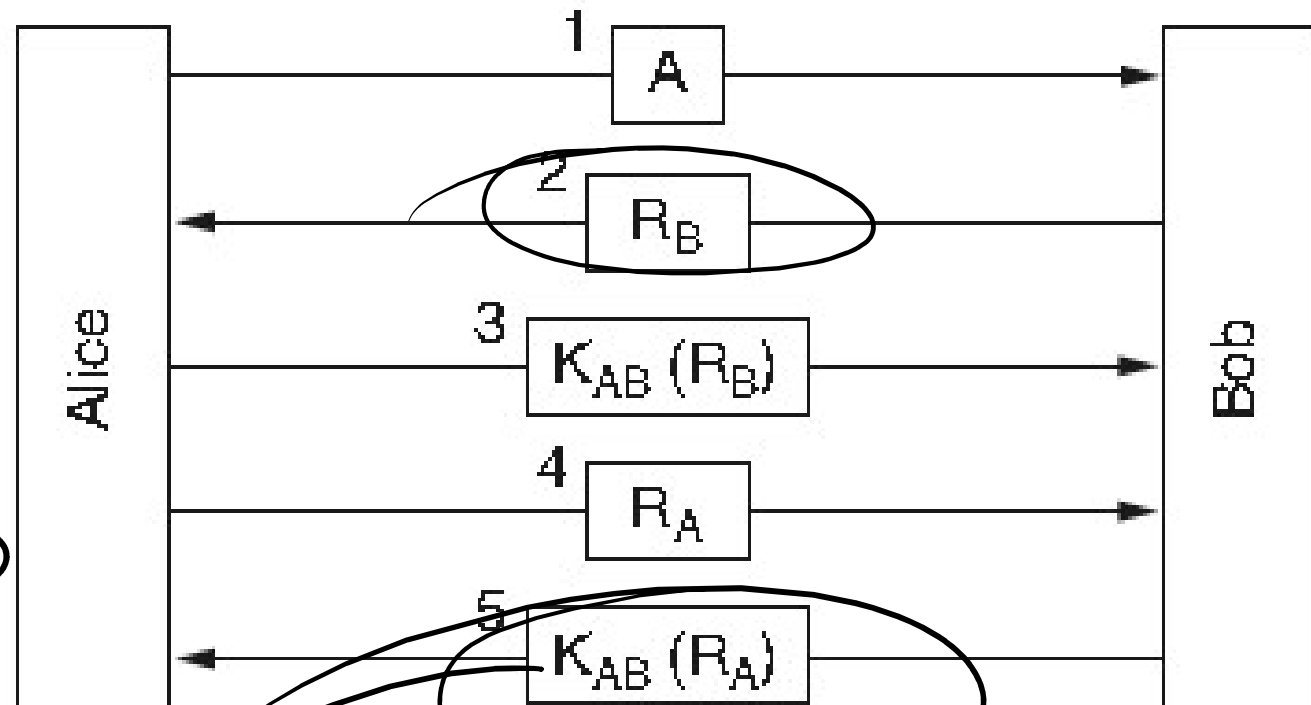
Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais



Autenticação bidirecional usando um protocolo de desafio-resposta.



PUC Minas

Chave secreta compartilhada (5)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

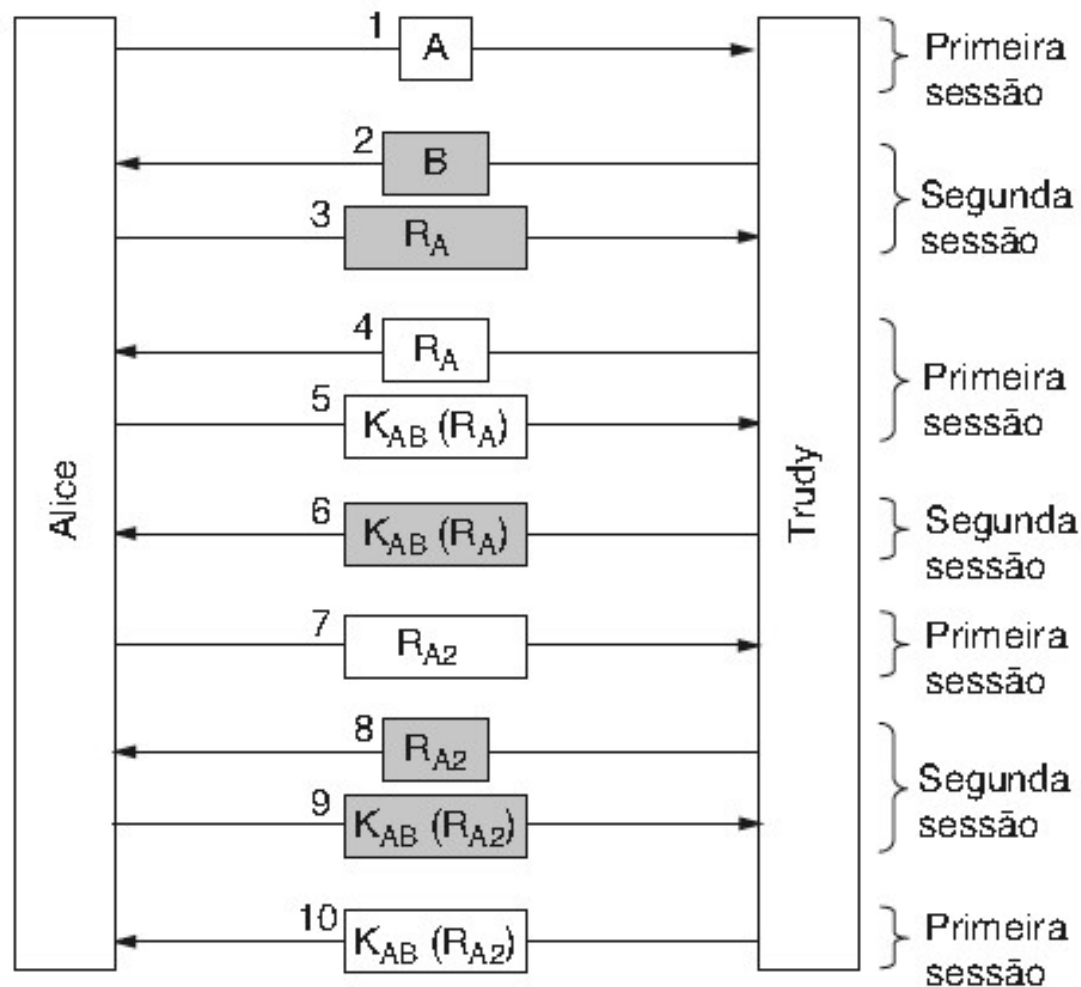
Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais



Ataque por reflexão

Sumário

Criptografia

Alg. de Chave
Simétrica

Alg. de Chave
Pública

Assinaturas
Digitais

Ger. de Chaves
Públicas

Seg. da
Comunicação

**Protocolos de
Autenticação**

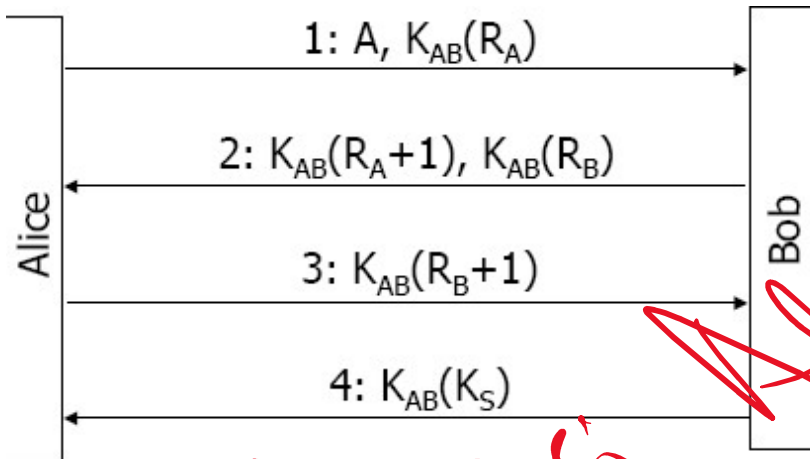
Seg. de Correio

Seg. da WEB

Questões
Sociais

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)

K_S não

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

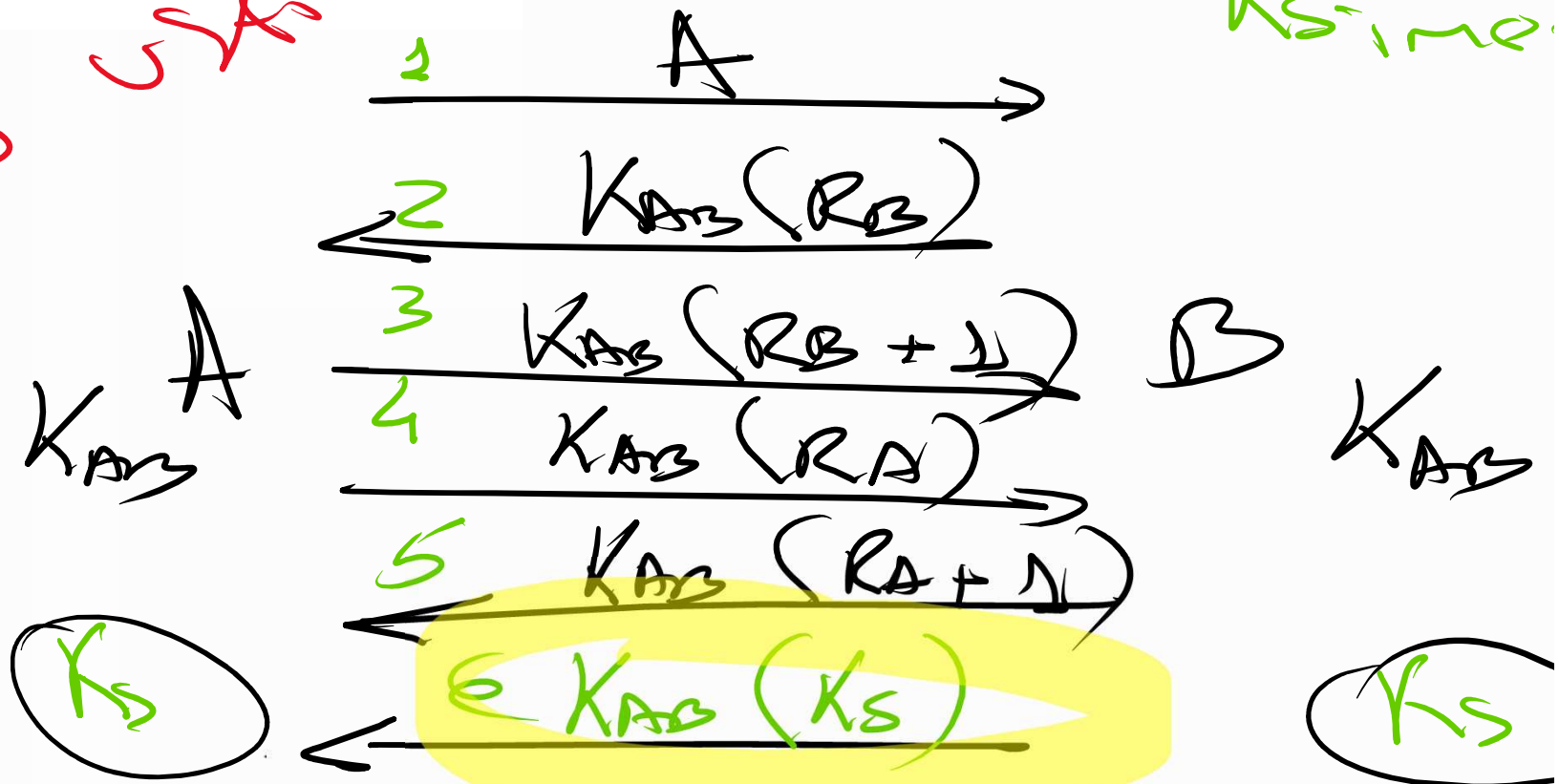
Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais



Um algoritmo adaptado



PUC Minas

Chave secreta compartilhada (7)

USG: *Summary of MS*
+ K since $\Rightarrow K_{AB}$

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

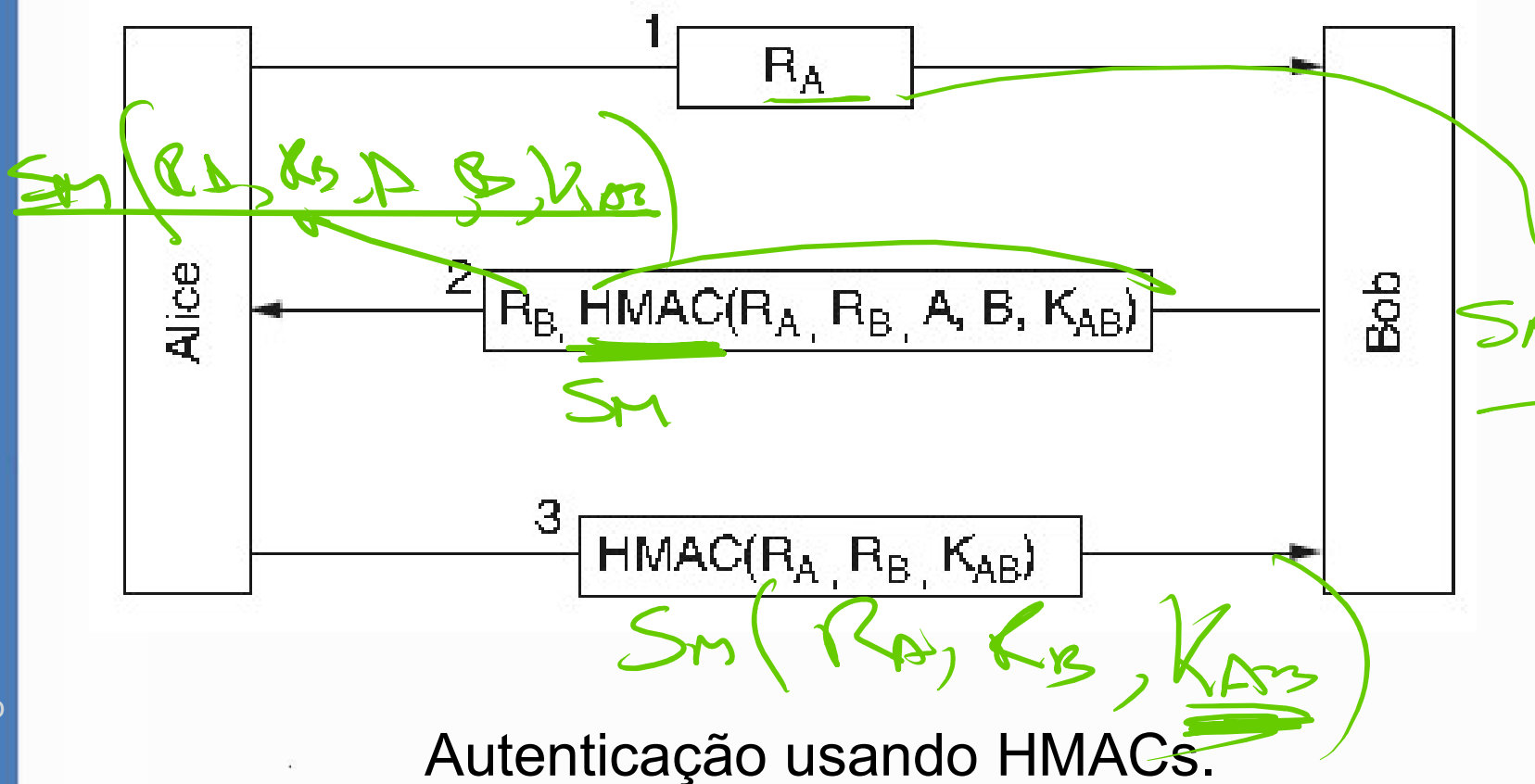
Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais



A troca de chaves de Diffie-Hellman (1)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

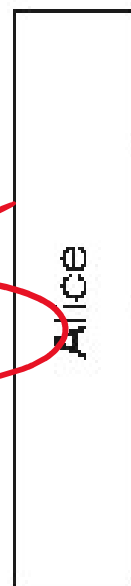
Seg. de Correio

Seg. da WEB

Questões Sociais

Alice
escolhe x

Bob
escolhe y



1 $n, g^x \bmod n$

2 $g^y \bmod n$

Alice calcula
 $(g^y \bmod n)^x \bmod n$
 $= g^{xy} \bmod n$

Bob calcula
 $(g^x \bmod n)^y \bmod n$
 $= g^{xy} \bmod n$

Troca de chaves de Diffie-Hellman.

$$K_{AB} = g^{xy} \bmod n$$

$$K_{AB} = g^{xy} \bmod n$$

A troca de chaves de Diffie-Hellman (2)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

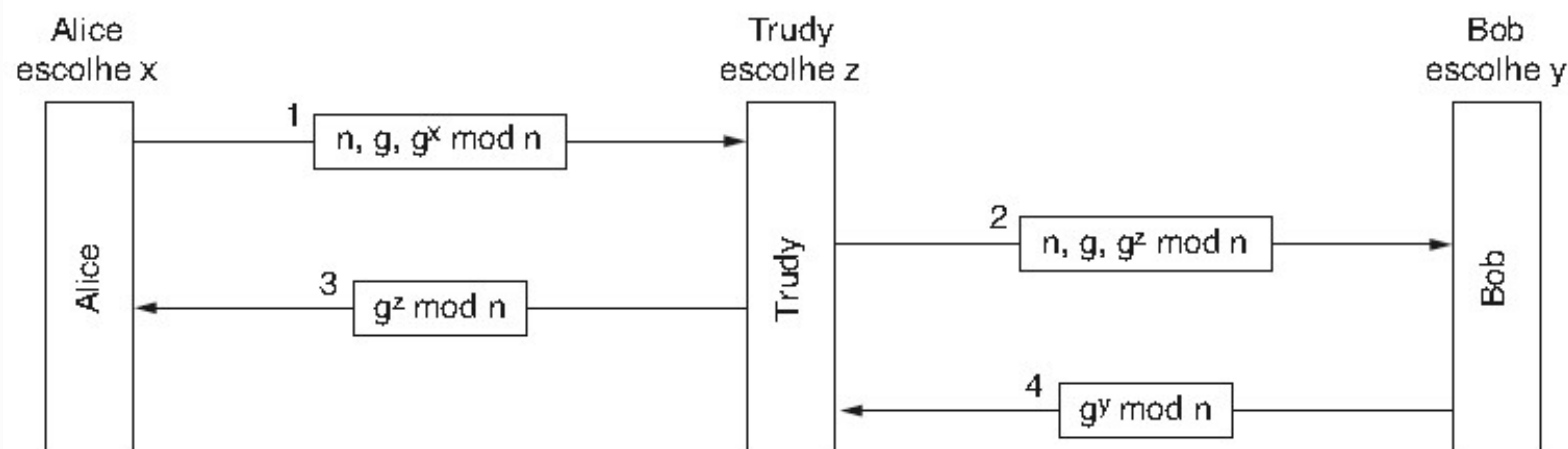
Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais



O ataque do homem no meio ou brigada de incêndio.

Resumo de protocolos de Autenticação até este momento

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

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



PUC Minas

Centro de distribuição de chaves (1)

Sumário

Criptografia

Algoritmo de Chave

Alice

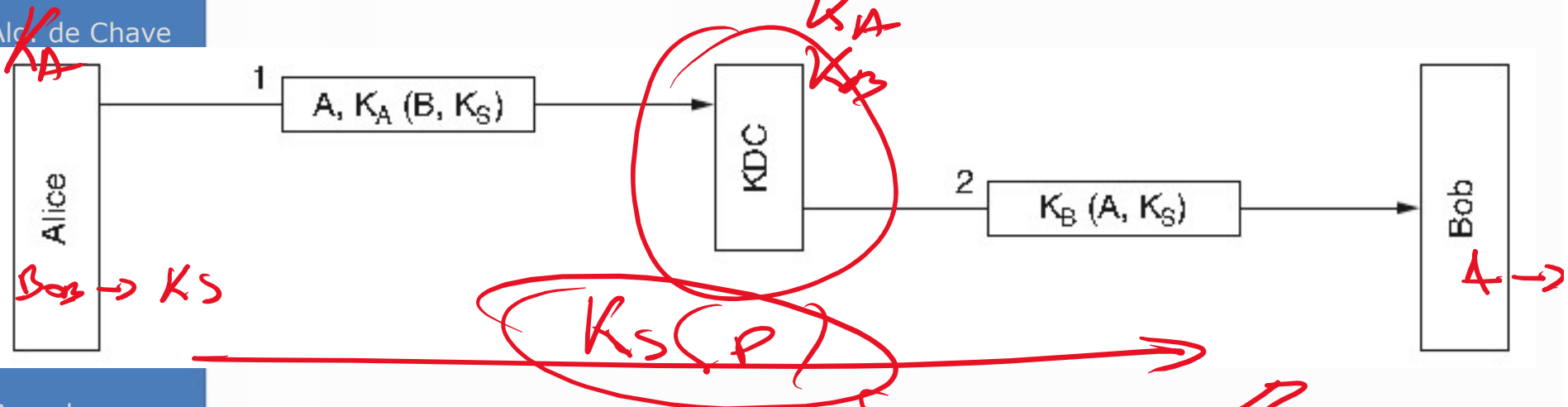
Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais



Primeira tentativa de protocolo de autenticação usando um KDC.

PROBLEMA: Ataque por Repetição!



USAD = *red*
Windows = *red*

AS = AUTHENTICATING
Kerberos

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves
Públicas

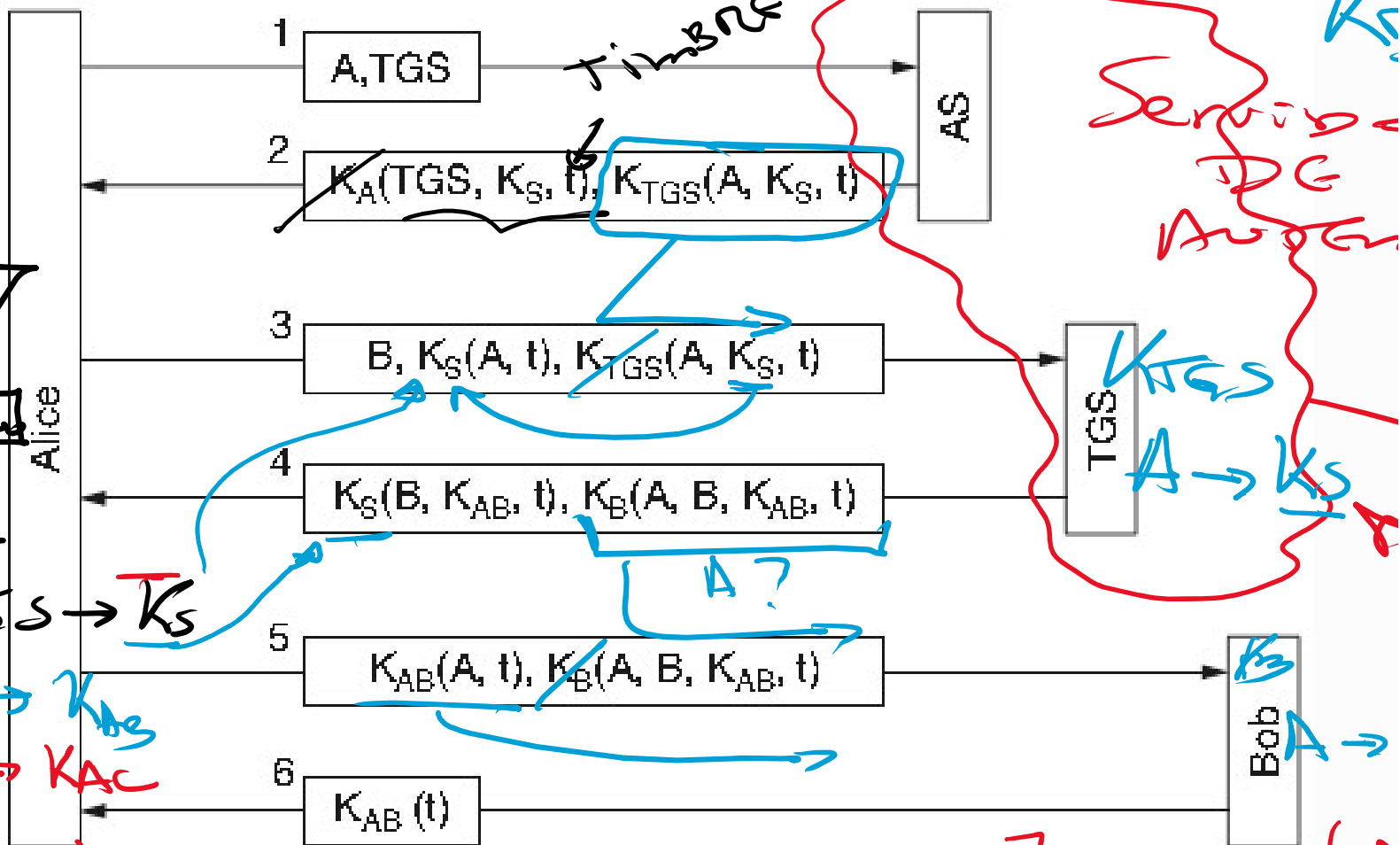
Seg. da
Comunicação

Protocolos de Autenticação

Seg. de Correio

~~Seg. da WEB~~

Questões Sociais



~~Operação do Kerberos V5~~

~~do Kerberos V5~~



PUC Minas

Criptografia de chave assimétrica

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

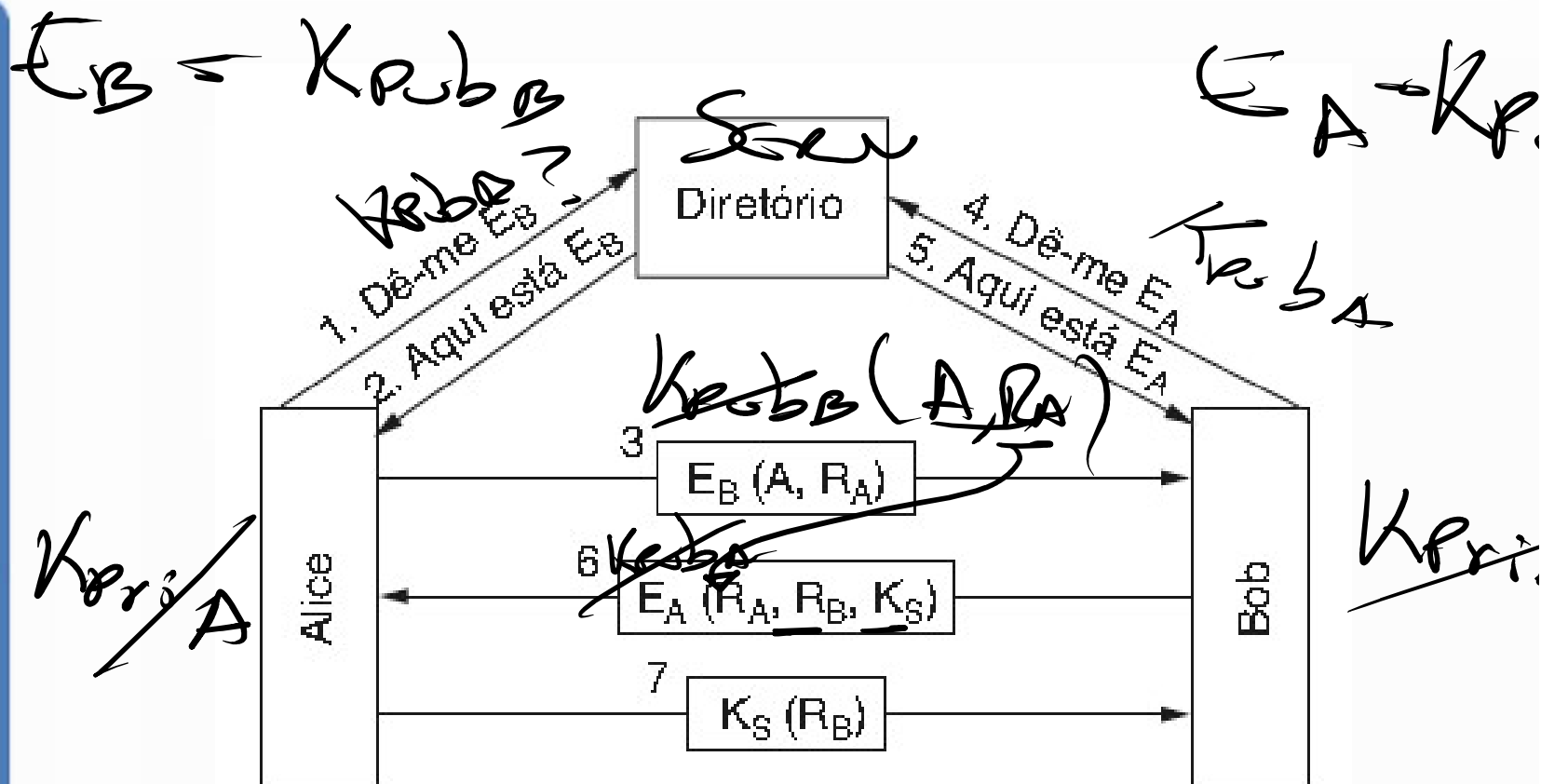
Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais



Autenticação mútua usando criptografia de chave pública.

Resumo de protocolos de Autenticação

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

• Ataques:

- Reflexão
- Homem do Meio
- Repetição para isto começo a colocar o t

$P \rightarrow K_{PRA}(S)$

• Autenticação

- Usando apenas alg simétrico
- Usando ~~Sumário de Msg~~ e chave simétrica
- Usando Centro de Distribuição de Chaves
== kerberos (KDC) $+ JOP$
- Usando Alg assimétricos
- Diffie-Hellman para trocar chaves simétricas