Segurança

- Application Layer
- transport Layer

tem para cada tecnologia

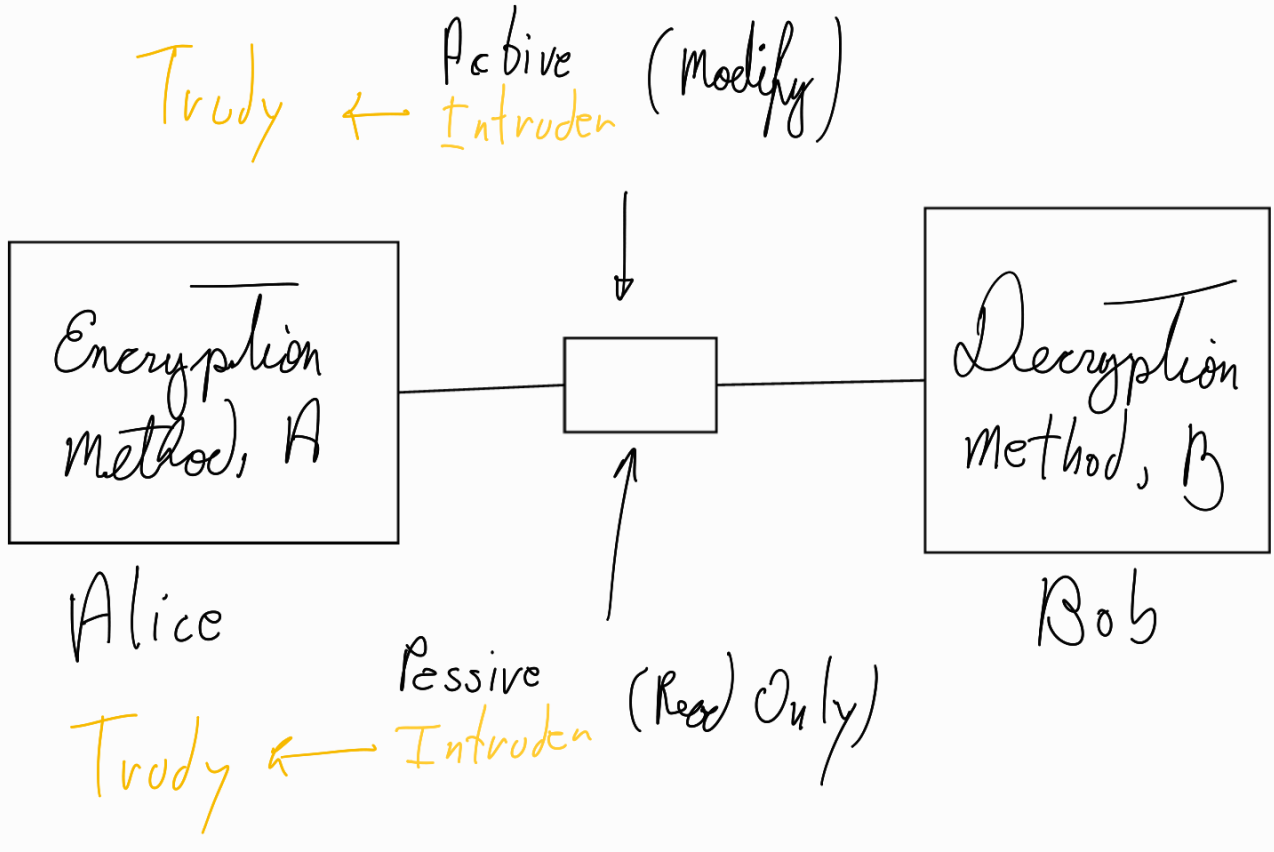
Cibersegurança
↳ threat inteligence reports

- Ataque Principal : Phishing (enganar o usuário)

- Back doors : Software com malware

ex:

- DDOS: Ataque em massa
- Engenharia Social
- Direct Memory Access : Acessa Memória



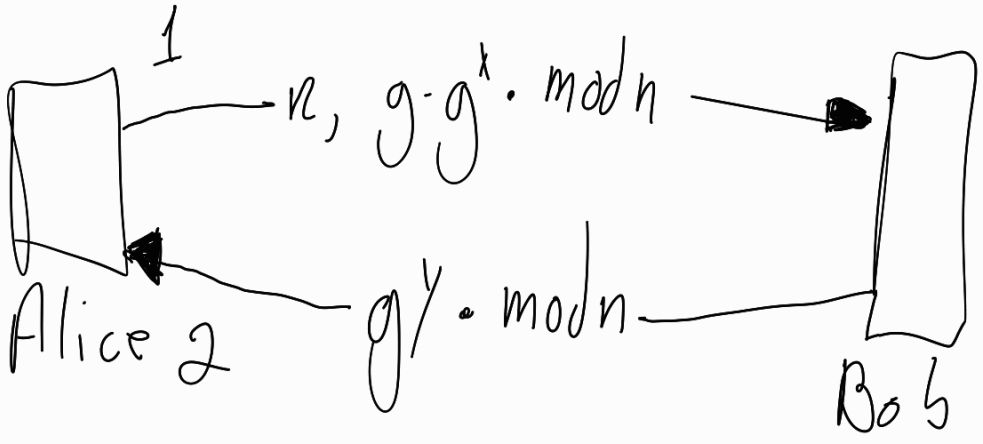
Metodos de Segurança

- Chave Secretes e não algoritmos

  Proteção Matemática

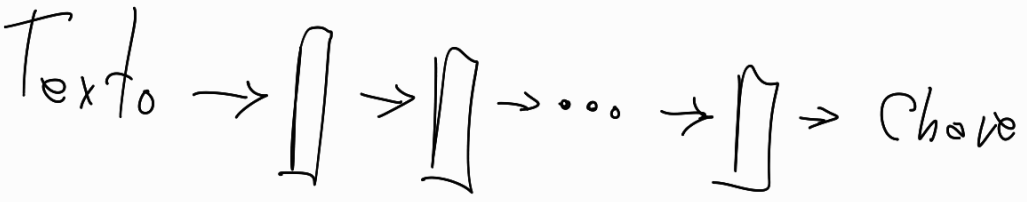
- Segurança fim a fim
- Menos Interface com Sistema

Troca de Chaves: Diffie-Hellman



Chaves Simétricas

Ex. de Método de embaralhamento: DES



Métodos de Chaves Simétricas

DES → weak

RC4 → have caution

RC5 → good

AES (Rijndael) → best

Serpent → strg

Triple DES → good old

TwoFish → strong

Chaves Assimétricas

$K_{A,B}$: Secred Key shared by A and B

K_A^+ : Public Key of A

$K_{\bar{A}}$: Private Key of A

$K(\cdot)$: algorithm that uses the key K

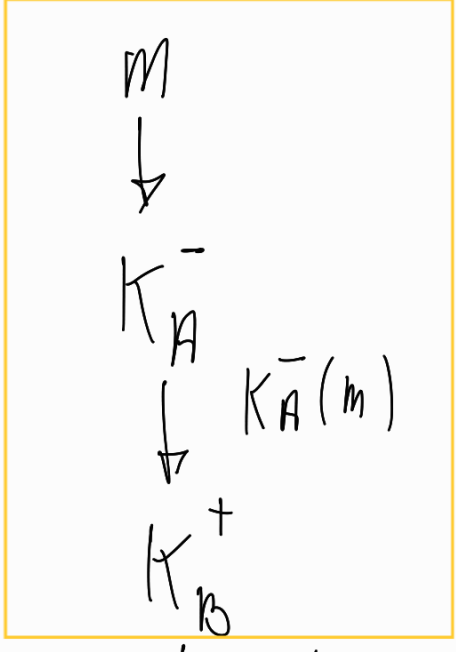
$K(d)$: data d encrypted with key K

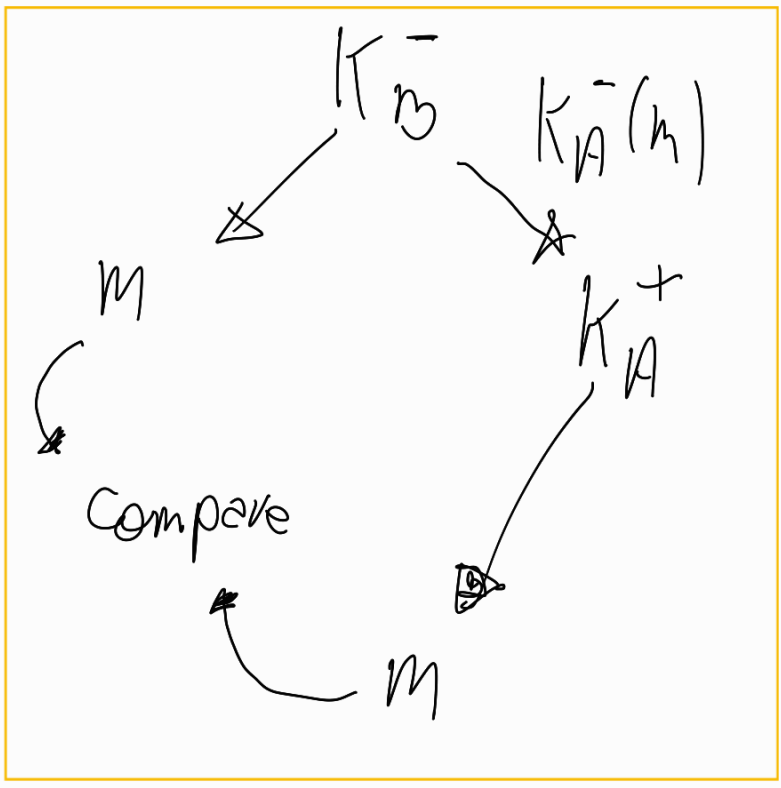
Decryption

$$K_A^+(d) \xrightarrow[K_A^-]{} d$$

$$K_A^-(d) \xrightarrow[K_A^+]{} d$$

Assinaturas com Public e Private Key

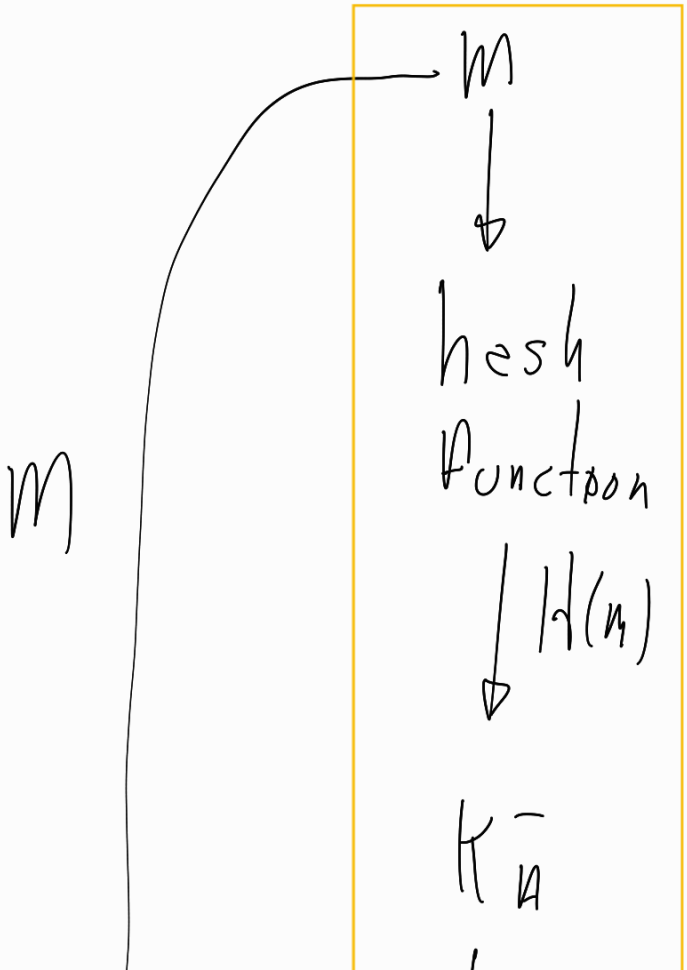




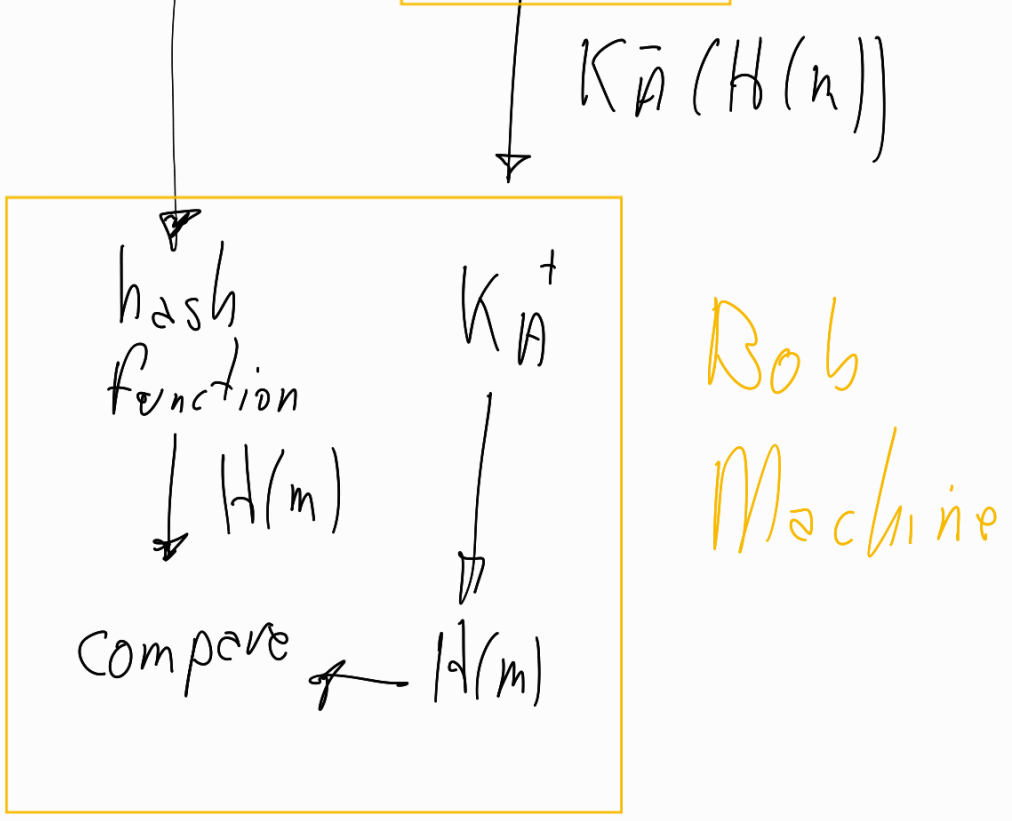
Bob Machine

Assinatura com Hash

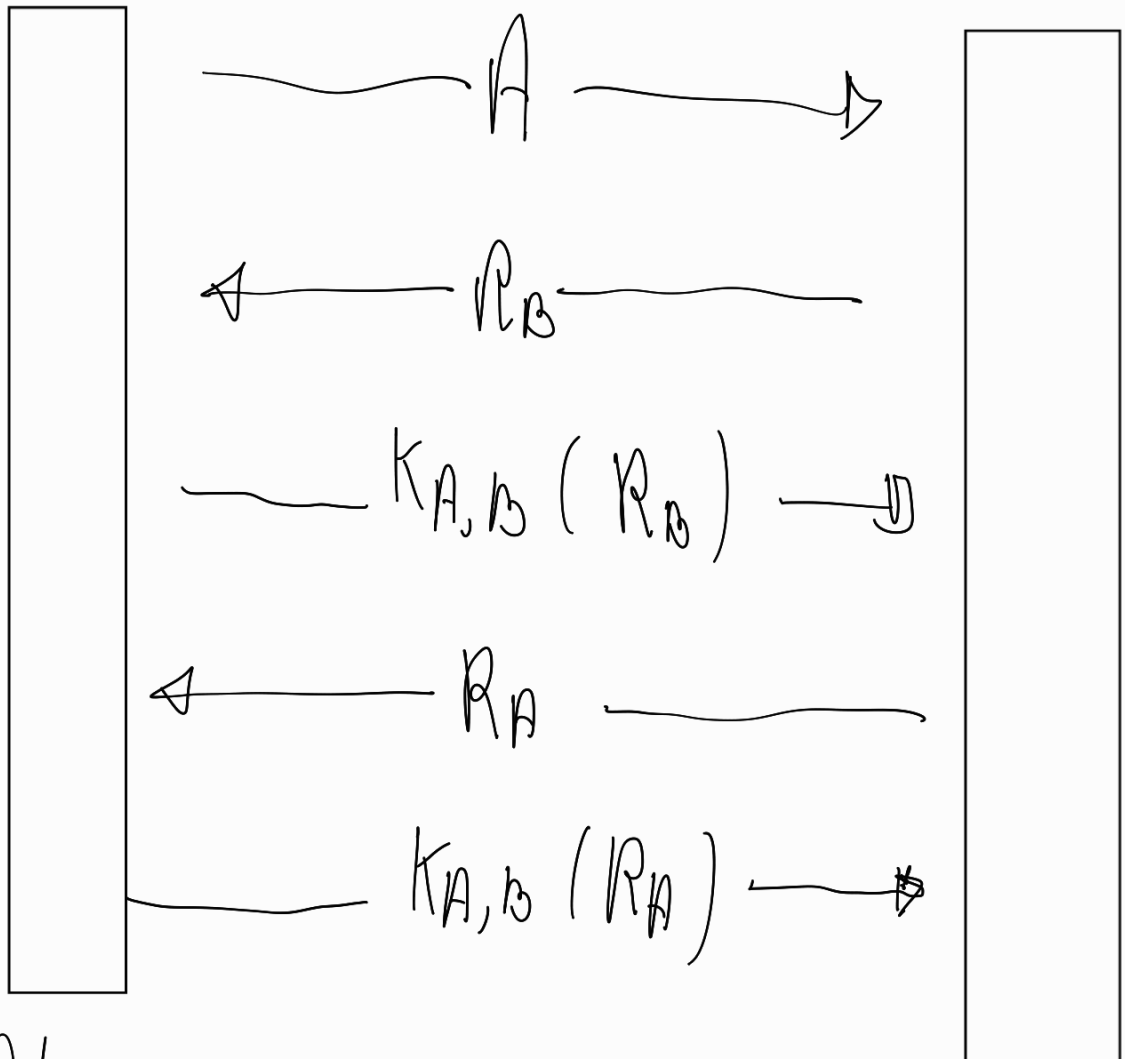
Não é criptográfic



Alice Machine



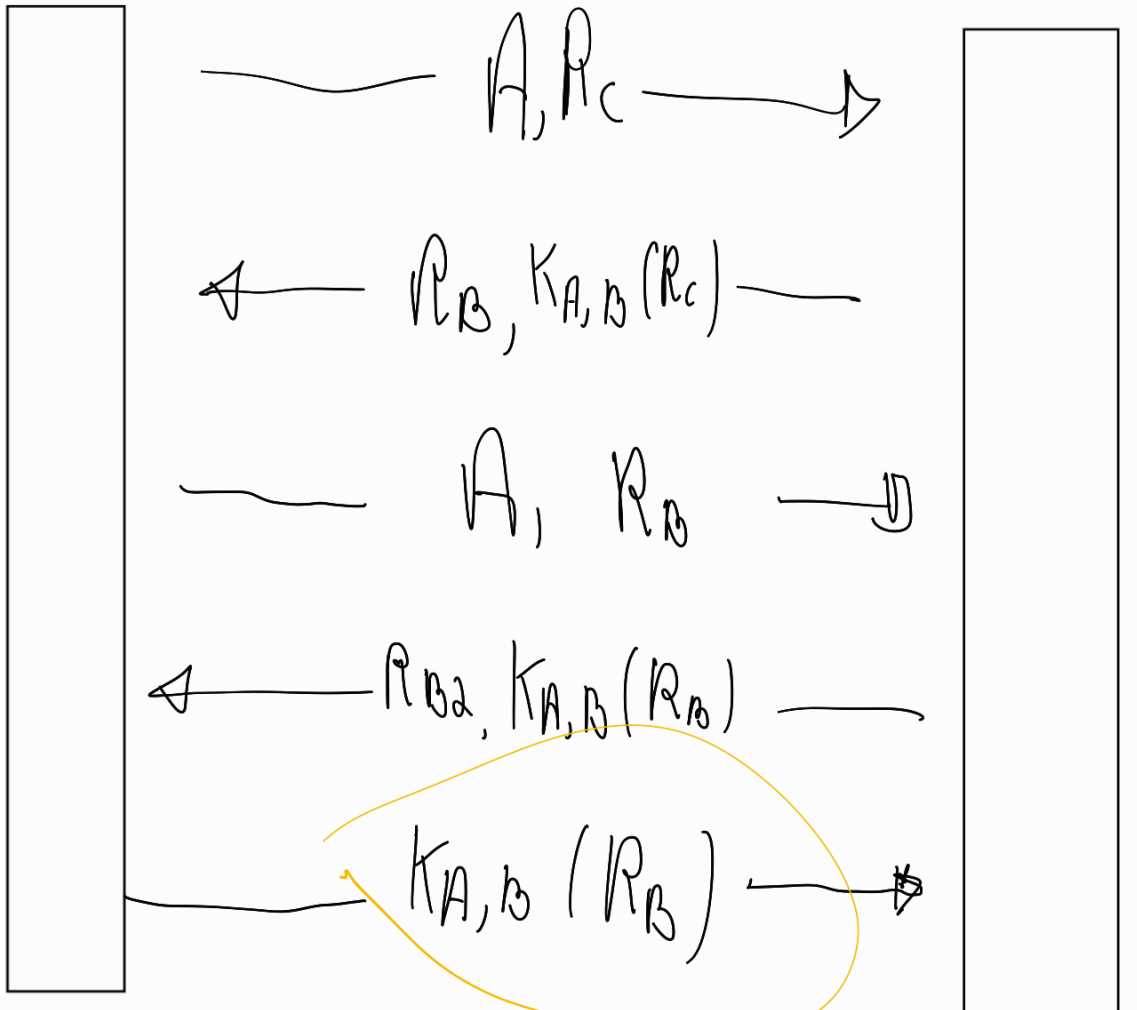
Assinatura com Chave Simétrica



Alice

Bob

Ataque de Reflexão (na assinatura acima)



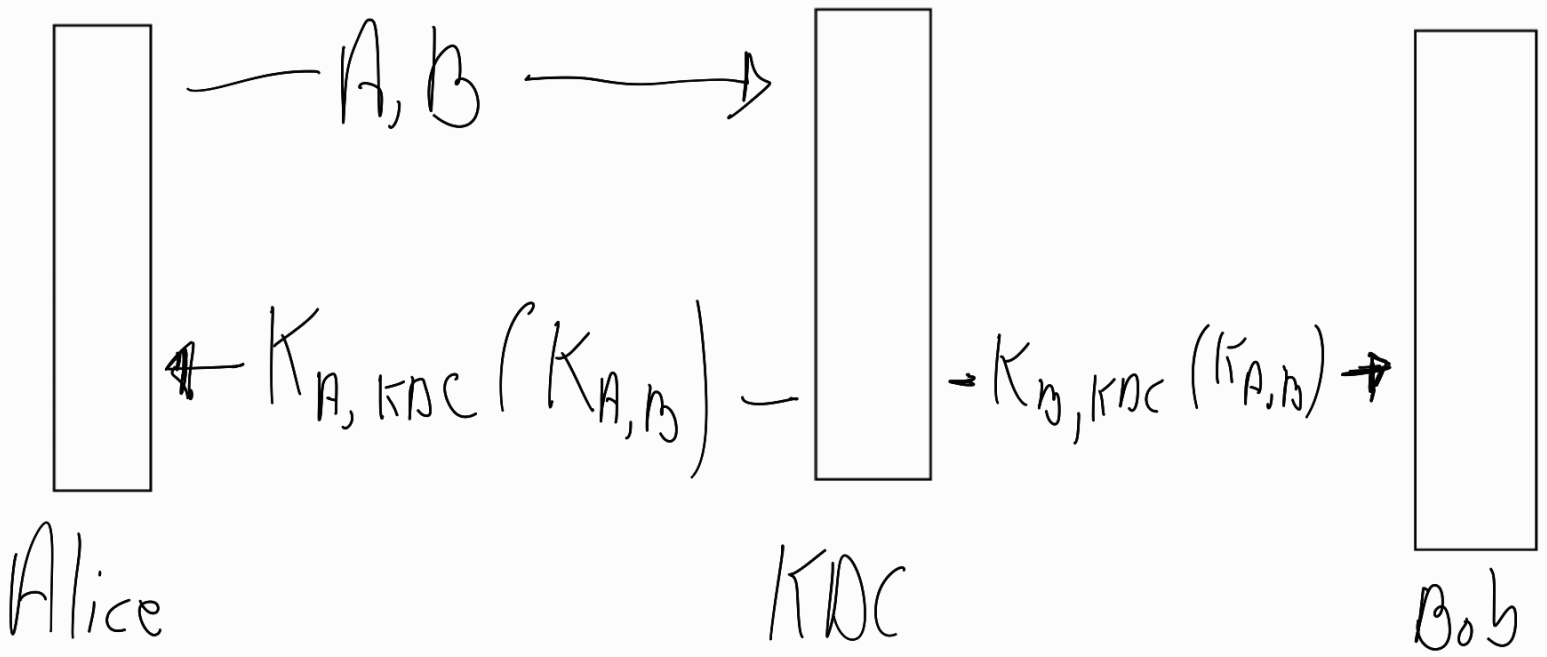
Chucky
(Fake Alice)

Bob

by this
simulates Alice Response

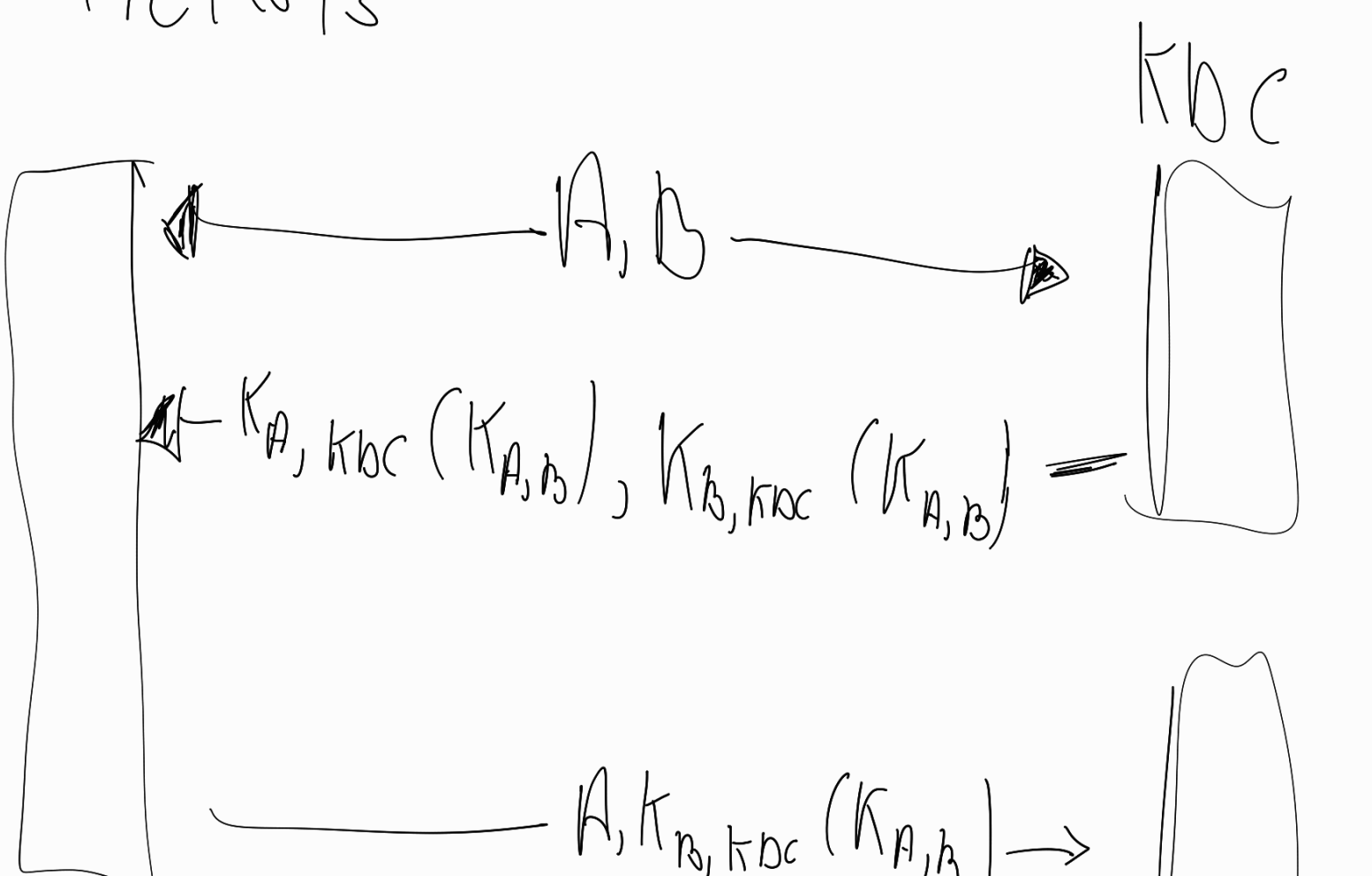
KDC

KDC



↳ center of keys

tickets



Alice

Bob

NS2 : Anti-Reflexão

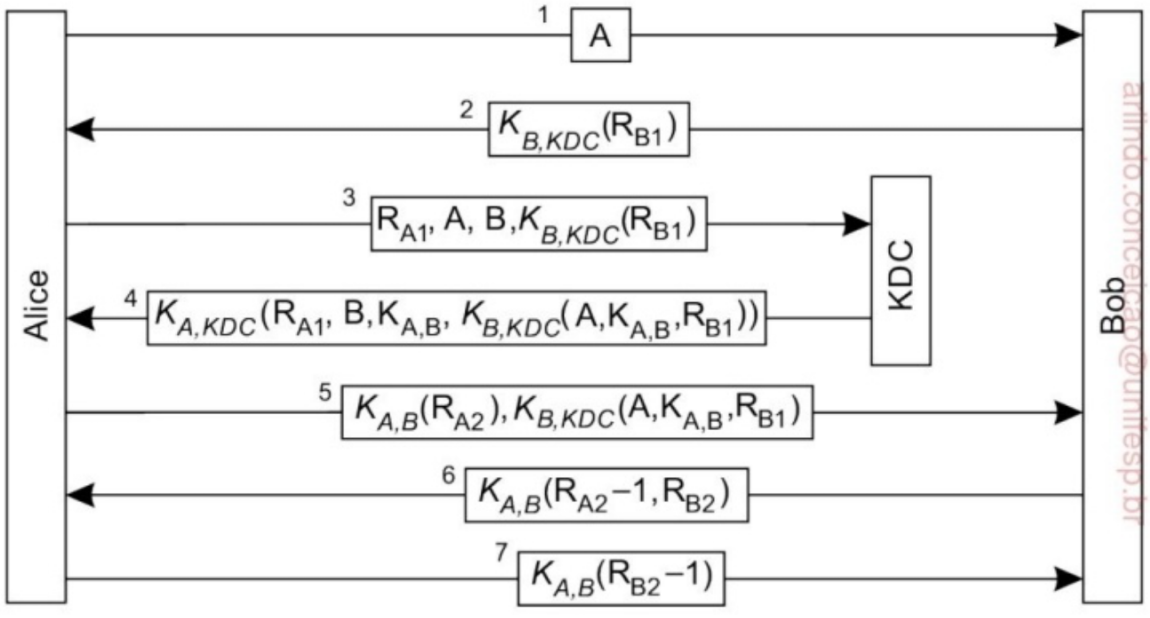
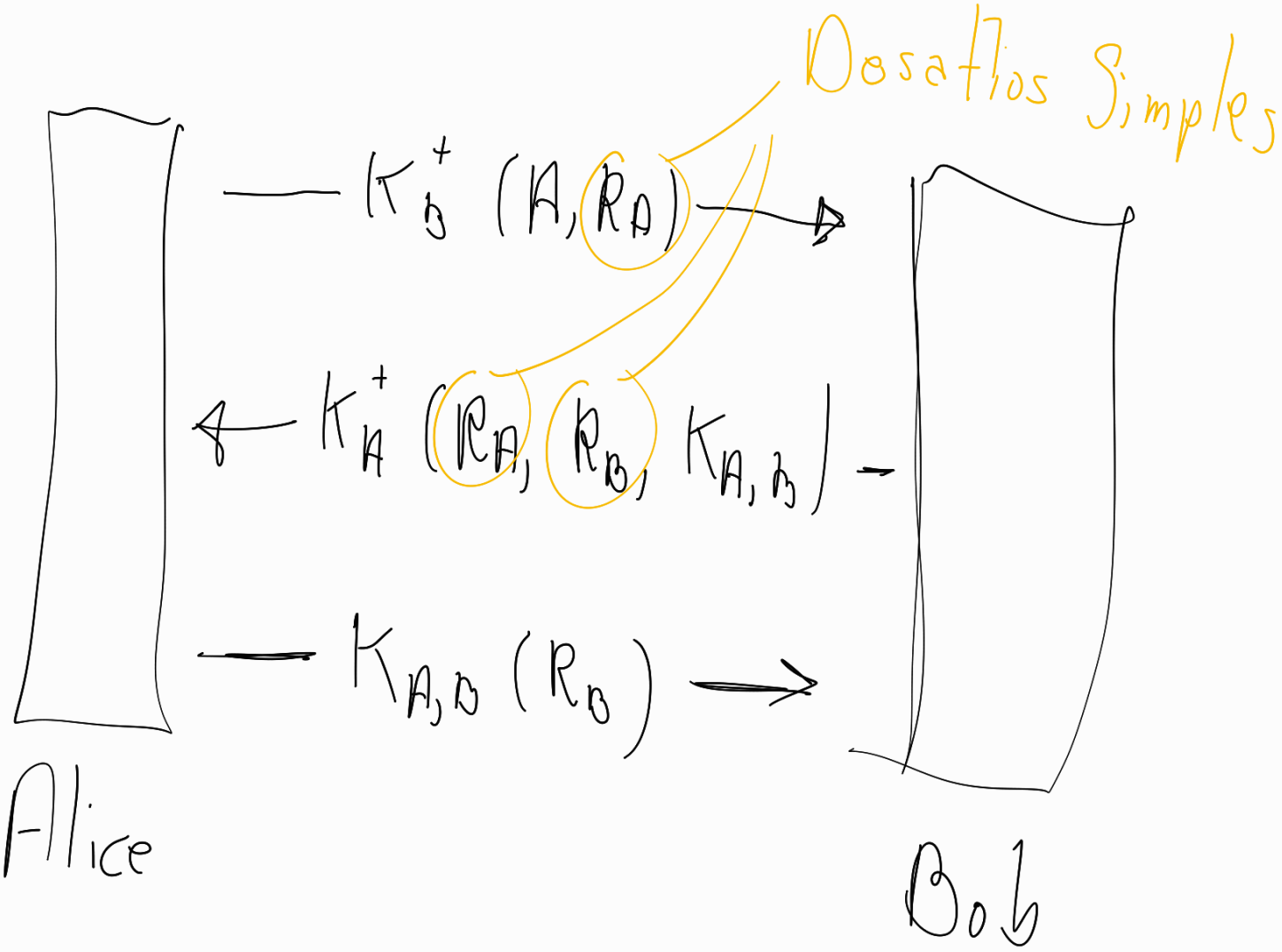


Figure 9.12: Protection against malicious reuse of a previously generated session key in the Needham-Schroeder protocol.

Autenticação Ponto a Ponto

↳ Chaves Assimetricas



Chave Assimetrica para criar chave

Então mantenho conexão com Chave Simetrica