Autenticação

Objetivo: Bob quer que Alice “prove” sua identidade para ele

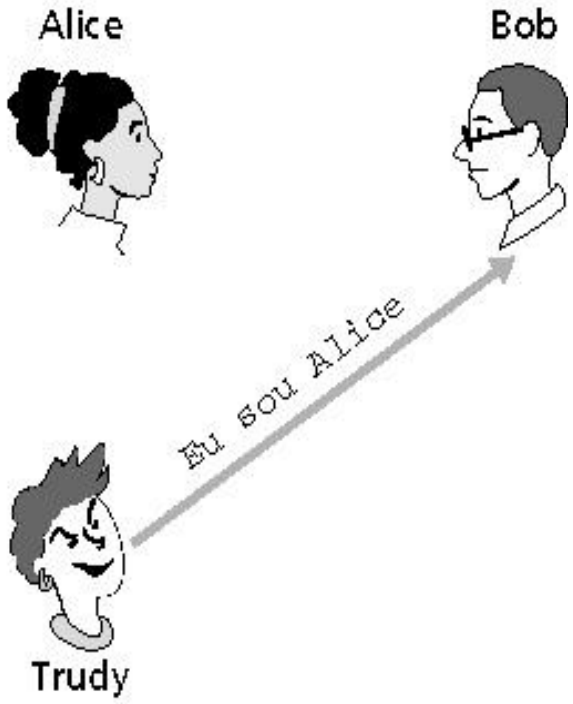
Protocolo ap1.0: Alice diz “Eu sou Alice”.

Cenário de falha??

Autenticação (cont.)

Objetivo: Bob quer que Alice "prove" sua identidade para ele

Protocolo ap1.0: Alice diz "Eu sou Alice".



Numa rede,
Bob não pode "ver" Alice,
então Trudy simplesmente
declara
que ela é Alice

Autenticação: outra tentativa

Protocolo ap2.0: Alice diz “Eu sou Alice” e envia seu endereço IP junto como prova.

Cenário de falha??

Autenticação: outra tentativa (cont.)

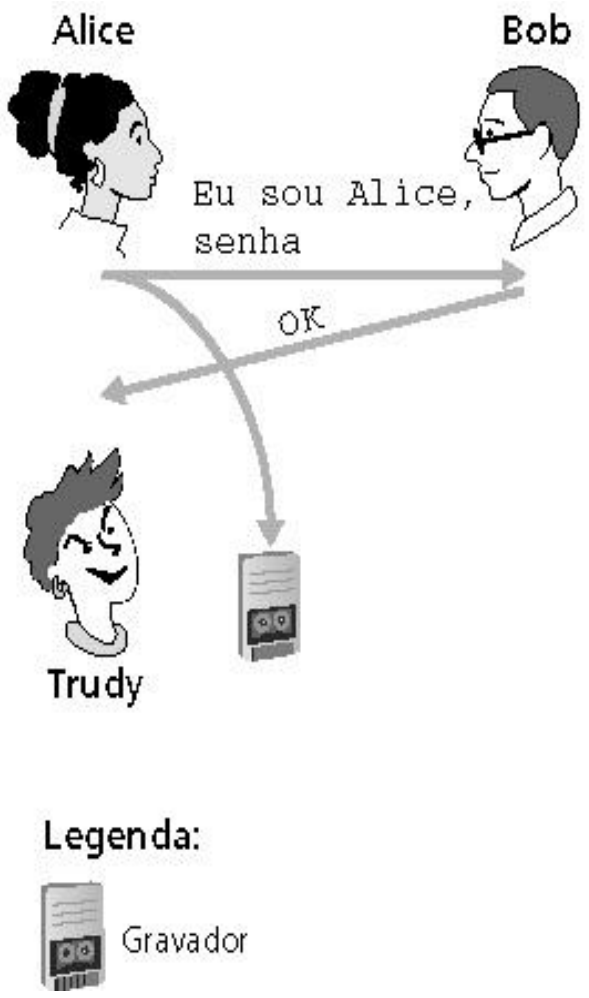
Protocolo ap2.0: Alice diz “Eu sou Alice” num pacote IP contendo seu endereço IP de origem.

Trudy pode criar um pacote “trapaceando” (*spoofing*) o endereço de Alice

Autenticação: outra tentativa (cont.)

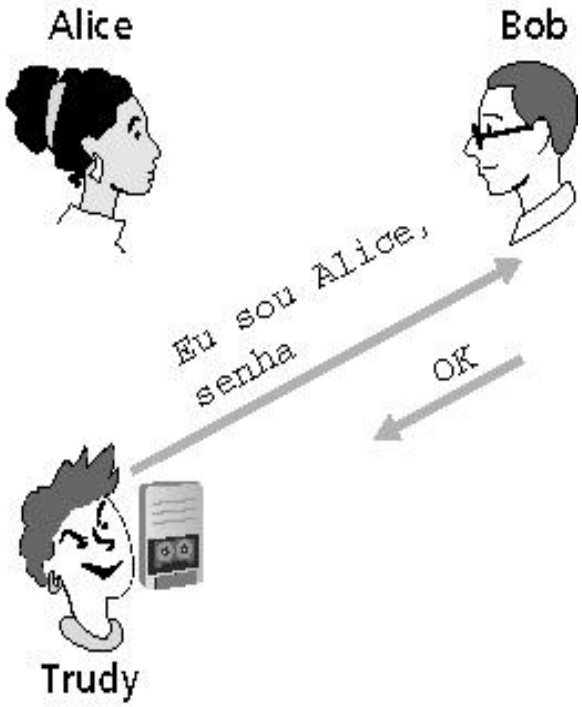
Protocolo ap3.0: Alice diz "Eu sou Alice" e envia sua senha secreta como prova.

Cenário de falha??



Autenticação: outra tentativa (cont.)

Protocolo ap3.0: Alice diz “Eu sou Alice” e envia sua senha secreta como prova.



ataque de playback:
Trudy grava o pacote de Alice e depois o envia de volta para Bob.

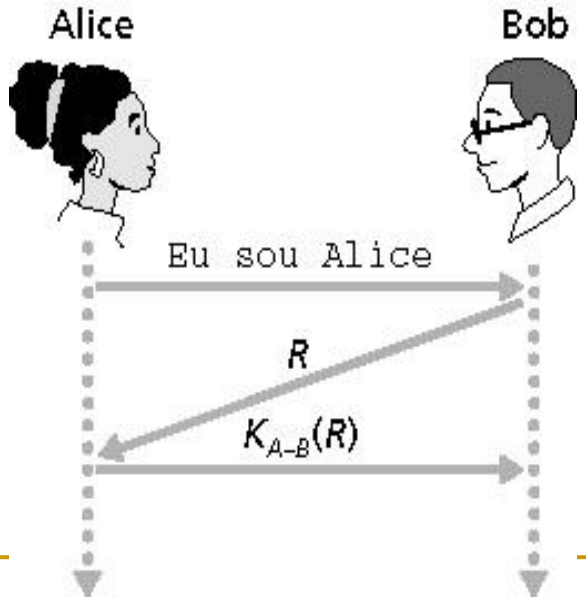
Autenticação: mais uma tentativa (cont.)

Protocolo ap3.1: Alice diz "Eu sou Alice" e envia sua senha secreta *criptografada* para prová-lo.

Meta: evitar ataque de reprodução (playback).

Nonce: número (R) usado apenas uma vez na vida.

ap4.0: para provar que Alice "está ao vivo", Bob envia a Alice um nonce, R. Alice deve devolver R, criptografado com a chave secreta comum.



Falhas, problemas?

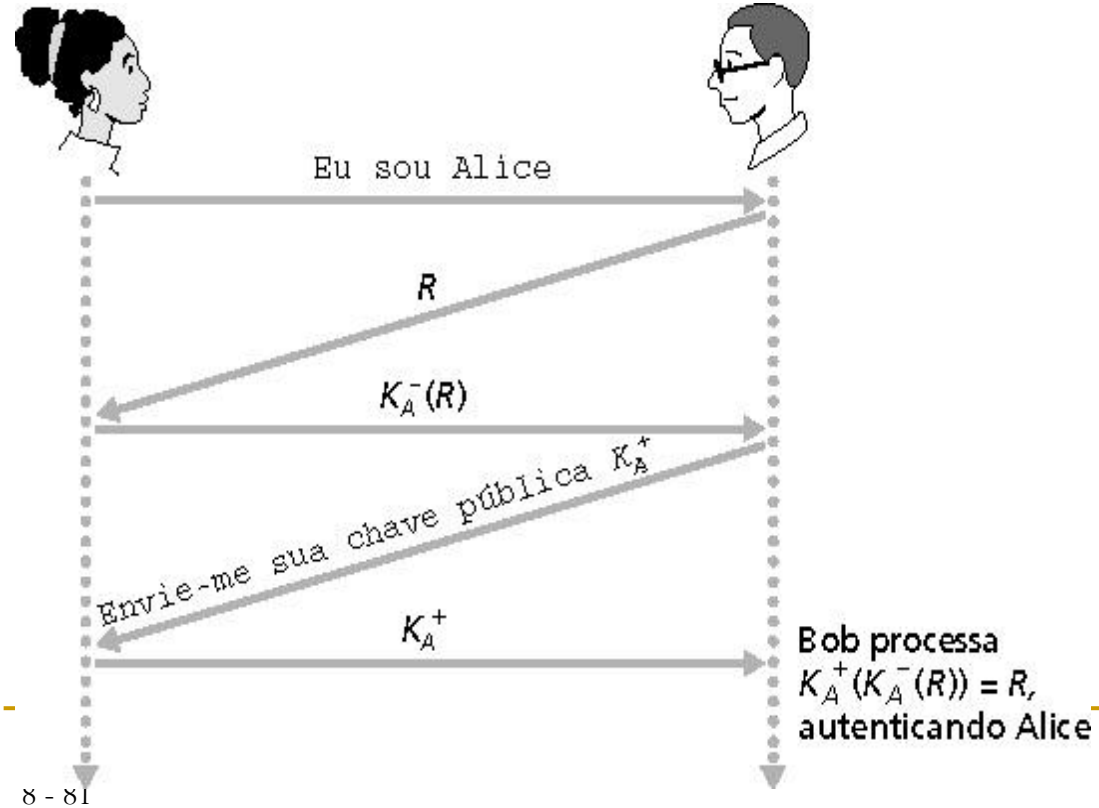
Alice está ao vivo, e apenas Alice conhece a chave para criptografar o nonce, então ela deve ser Alice!

Autenticação: ap5.0

ap4.0 exige chave secreta compartilhada.

- É possível autenticar usando técnicas de chave pública?

ap5.0: usar nonce, criptografia de chave pública.



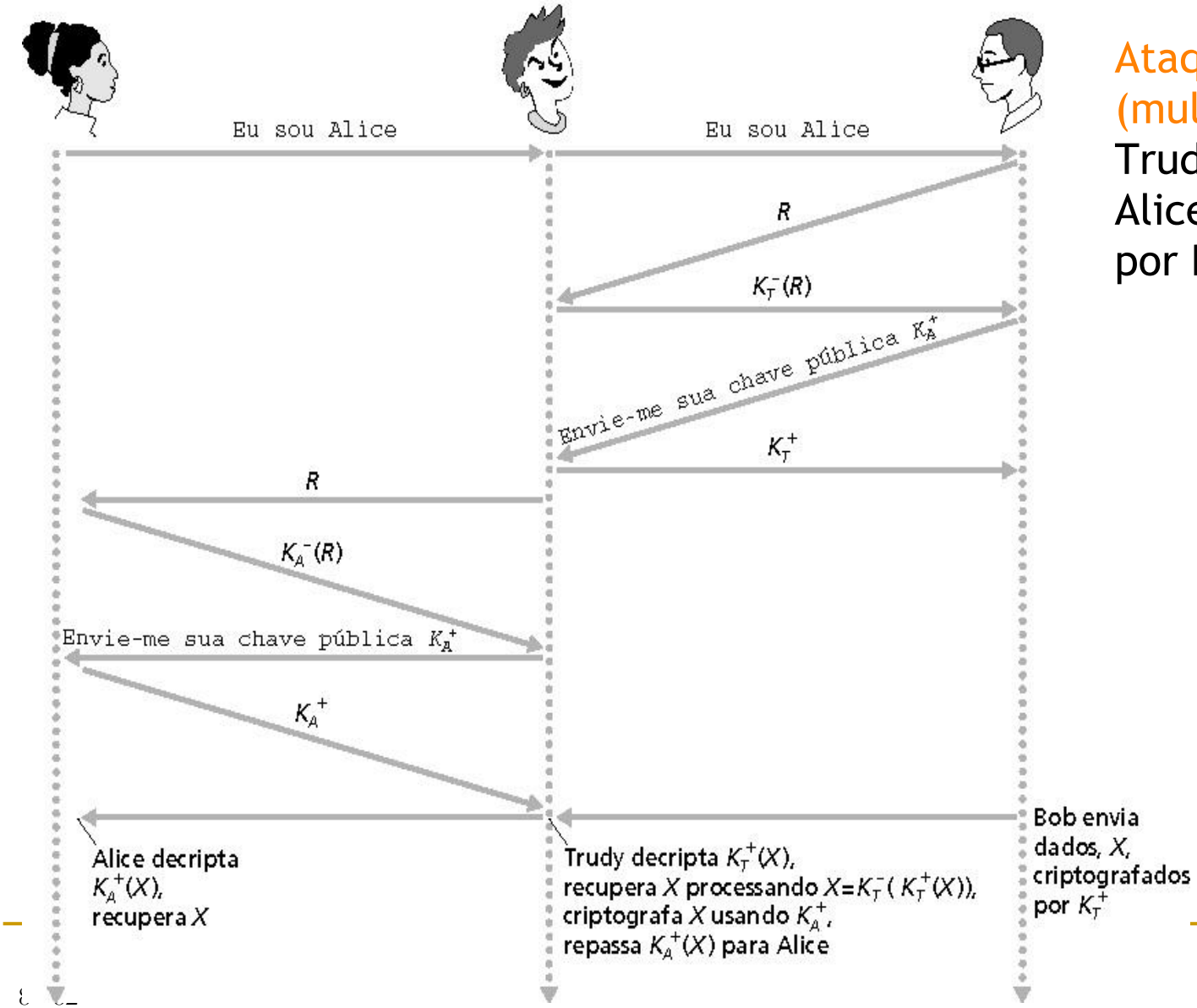
Bob calcula

$$K_A^+(K_A^-(R)) = R$$

e sabe que apenas Alice poderia ter a chave privada, que criptografou R desta maneira

$$K_A^+(K_A^-(R)) = R$$

ap5.0: falha de segurança



Ataque do homem (mulher) no meio:
Trudy se passa por Alice (para Bob) e por Bob (para Alice)

ap5.0: falha de segurança

Ataque do homem no meio: Trudy se passa por Alice (para Bob) e por Bob (para Alice)

Difícil de detectar:

- O problema é que Trudy recebe todas as mensagens também!
- Bob recebe tudo o que Alice envia e vice-versa. (Ex.: então Bob/Alice podem se encontrar uma semana depois e recordar a conversação.)

Sumário

- Fundamentos
- Criptografia Simétrica
- Criptografia Assimétrica
- Integridade
- Autenticação
- Assinatura Digital e Certificação Digital
- Distribuição de Chaves
- Serviços de Rede

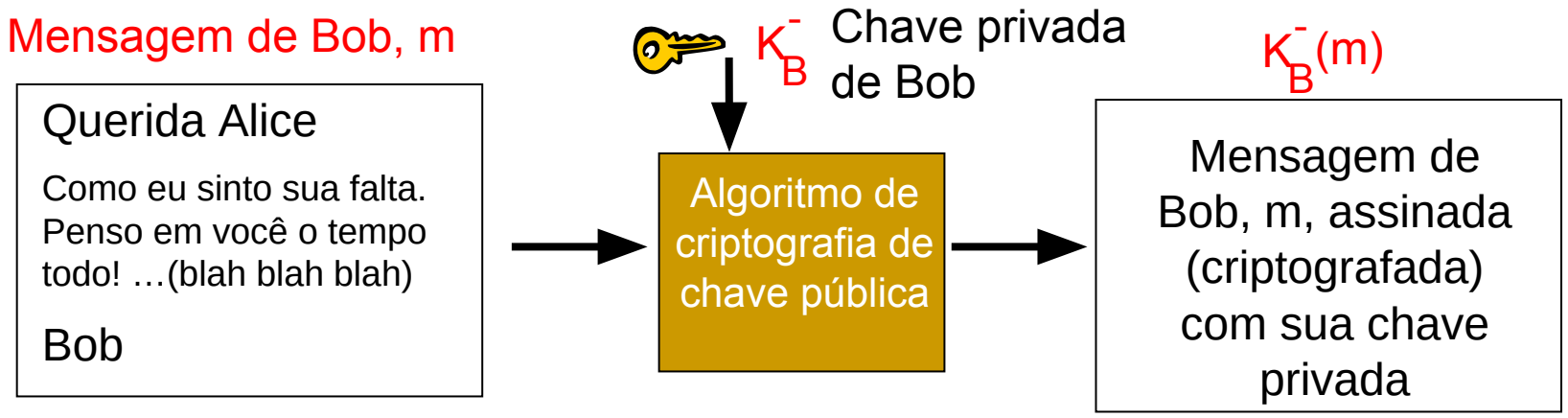
Assinaturas digitais

Técnica criptográfica semelhante a assinaturas escritas a mão.

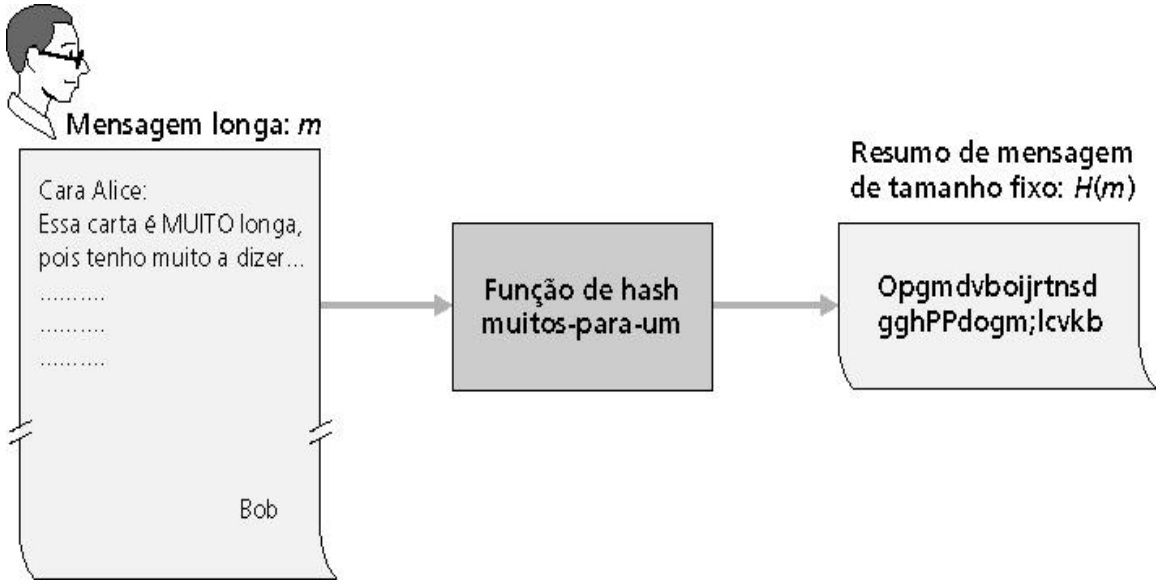
- remetente (Bob) assina documento digitalmente, estabelecendo que é o dono/criador do documento.
- objetivo semelhante a um MAC, exceto que agora usamos criptografia de chave pública.
- verificável, não falsificável: destinatário (Alice) pode provar a alguém que Bob, e ninguém mais (incluindo Alice), deverá ter assinado o documento.

assinatura digital simples para mensagem m:

- Bob assina m criptografando com sua chave privada K_B^-, criando mensagem "assinada", $K_B^-(m)$



Resumos de mensagens nas Assinaturas Digitais



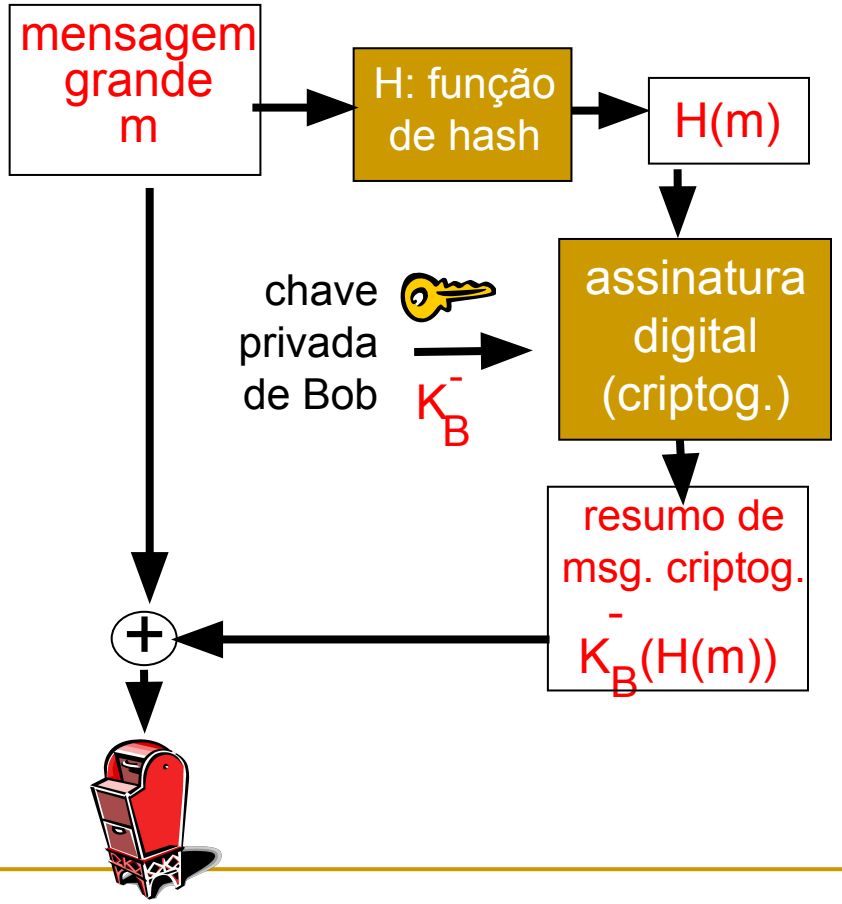
Computacionalmente caro criptografar mensagens longas com chave pública

Meta: assinaturas digitais de comprimento fixo, facilmente computáveis, "impressão digital"

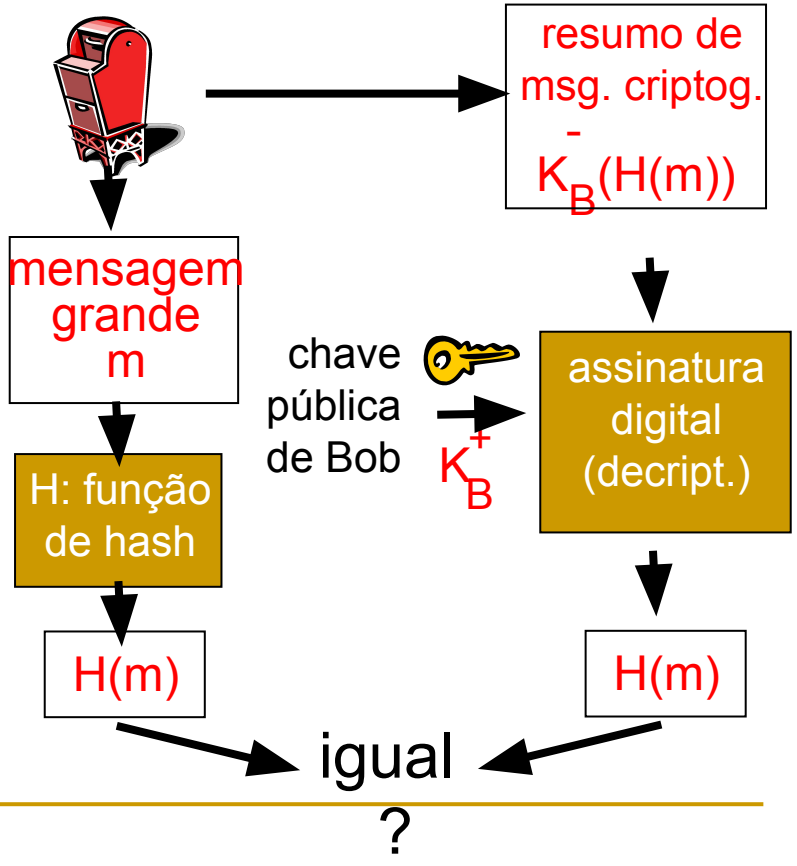
- Aplicar função hash H a *m* para obter um resumo de tamanho fixo, *H(m)*

Assinatura digital = resumo de mensagem assinada

Bob envia mensagem assinada em forma digital:



Alice verifica assinatura e integridade da mensagem assinada em forma digital:



Assinaturas digitais (mais)

- Suponha que Alice receba msg *m*, assinatura digital $K_B^-(m)$
- Alice verifica m assinada por Bob aplicando chave pública de Bob K_B^+ a $K_B^-(m)$, depois verifica $K_B^+(K_B^-(m)) = m$.
- se $K_B^+(K_B^-(m)) = m$, quem assinou m deve ter usado a chave privada de Bob.

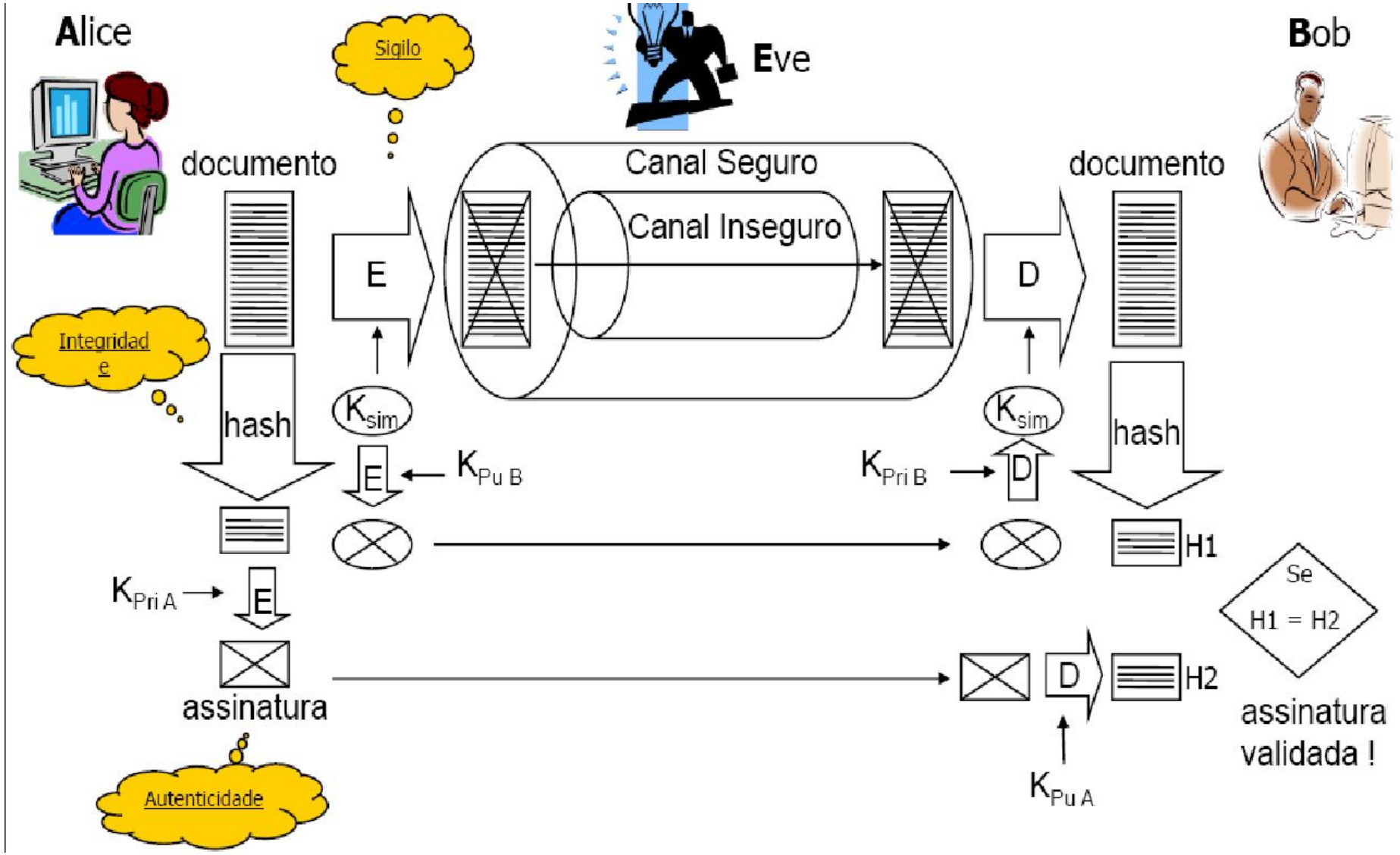
Assim, Alice verifica se:

- ü Bob assinou *m*.
- ü Ninguém mais assinou *m*.
- ü Bob assinou *m* e não *m'*.

Não repudiação:

- ü Alice pode levar *m* e assinatura $K_B^-(m)$ ao tribunal e provar que Bob assinou m.

Integração

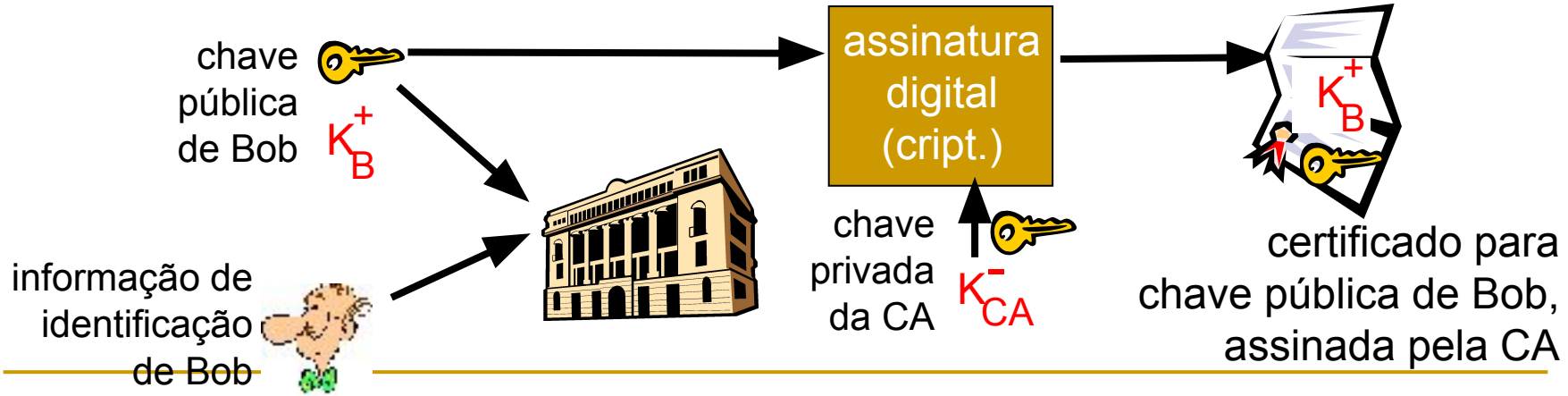

Alice
Sigilo
Eve
Bob
documento
Canal Seguro
Canal Inseguro
documento
E
D
Integridade
hash
K_{sim}
K_{sim}
hash
E
$K_{Pu\ B}$
$K_{Pri\ B}$
D
H1
$K_{Pri\ A}$
E
Se
H1 = H2
assinatura
D
H2
assinatura validada !
Autenticidade
$K_{Pu\ A}$

Certificação de chave pública

- motivação: Trudy prega peça da pizza em Bob
  - Trudy cria pedido por e-mail:
    Prezada pizzaria, Por favor, me entregue quatro pizzas de calabresa. Obrigado, Bob.
  - Trudy assina pedido com sua chave privada
  - Trudy envia pedido à pizzaria
  - Trudy envia à pizzaria sua chave pública, mas diz que é a chave pública de Bob.
  - pizzaria verifica assinatura; depois, entrega quatro pizzas para Bob.
  - Bob nem sequer gosta de calabresa.

Autoridades de certificação

- autoridade de certificação (CA): vincula chave pública à entidade particular, E.
- E (pessoa, roteador) registra sua chave pública com CA.
  - E fornece “prova de identidade” à CA.
  - CA cria certificado vinculando E à sua chave pública.
  - certificado contendo chave pública de E assinada digitalmente pela CA – CA diz “esta é a chave pública de E”



- quando Alice quer a chave pública de Bob:
  - recebe certificado de Bob (Bob ou outro).
  - aplica chave pública da CA ao certificado de Bob, recebe chave pública de Bob