CAP 8. SEGURANÇA EM REDES DE COMPUTADORES

INE5422 REDES DE COMPUTADORES II

PROF. ROBERTO WILLRICH (INE/UFSC)
ROBERTO.WILLRICH@UFSC.BR

HTTPS://MOODLE.UFSC.BR

Segurança em redes de computadores

O que é segurança?

Princípios da criptografia

Autenticação

Integridade

Distribuição de chaves e certificação

Controle de acesso: firewalls

Segurança em muitas camadas

O que é segurança de rede?

Propriedades desejáveis de uma comunicação segura

- **Confidencialidade**: apenas o transmissor e o receptor pretendido deveriam "entender" o conteúdo da mensagem (usando criptografia)
- **Autenticação**: transmissor e receptor querem confirmar a identidade um do outro
- **Integridade de mensagens**: transmissor e receptor querem assegurar que as mensagens não foram alteradas, (em trânsito, ou depois) sem detecção
- **Acesso e disponibilidade**: serviços devem ser acessíveis e disponíveis para os usuários
  - Impedir que ataques (tipo denial of service – DoS) impeçam o acesso ao serviço

Segurança em redes de computadores

O que é segurança?

Princípios da criptografia

Autenticação

Integridade

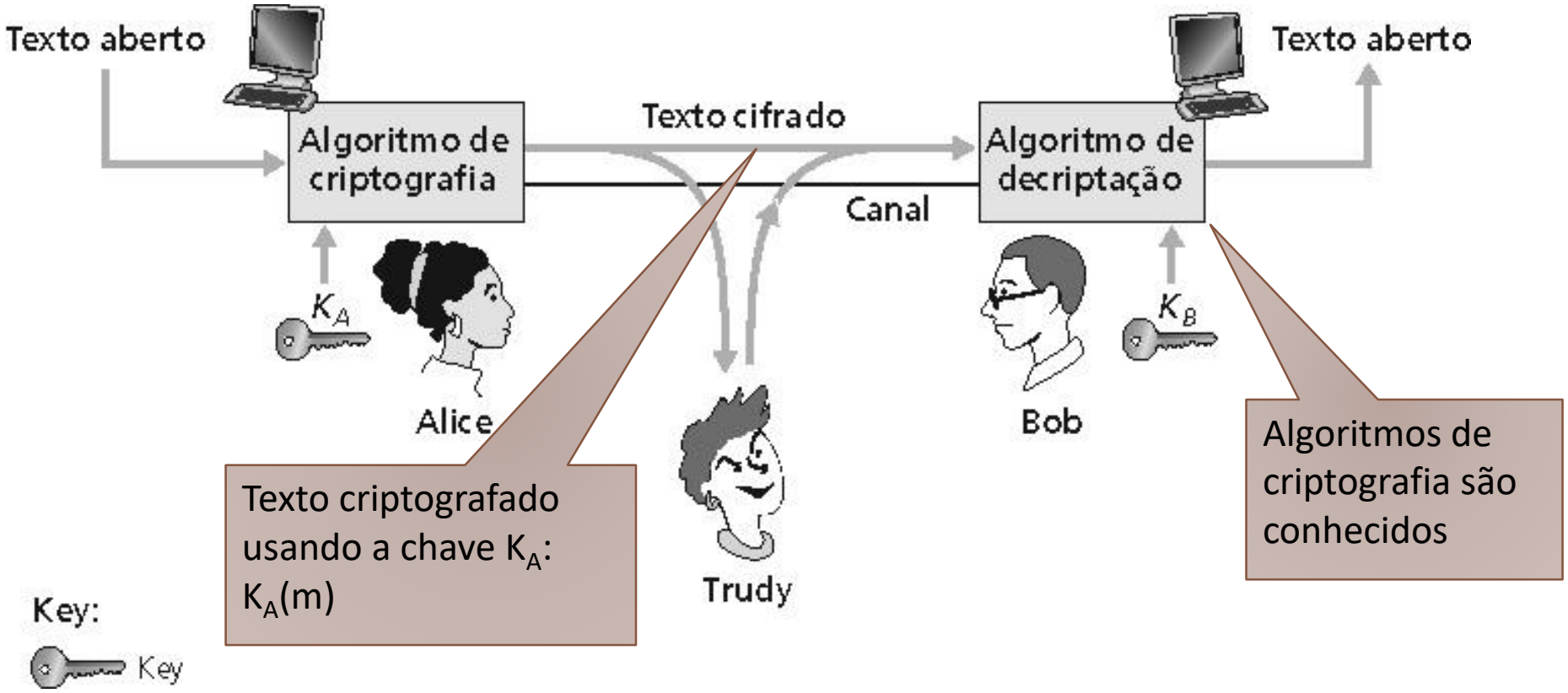
Distribuição de chaves e certificação

Controle de acesso: firewalls

Segurança em muitas camadas

Princípios da criptografia

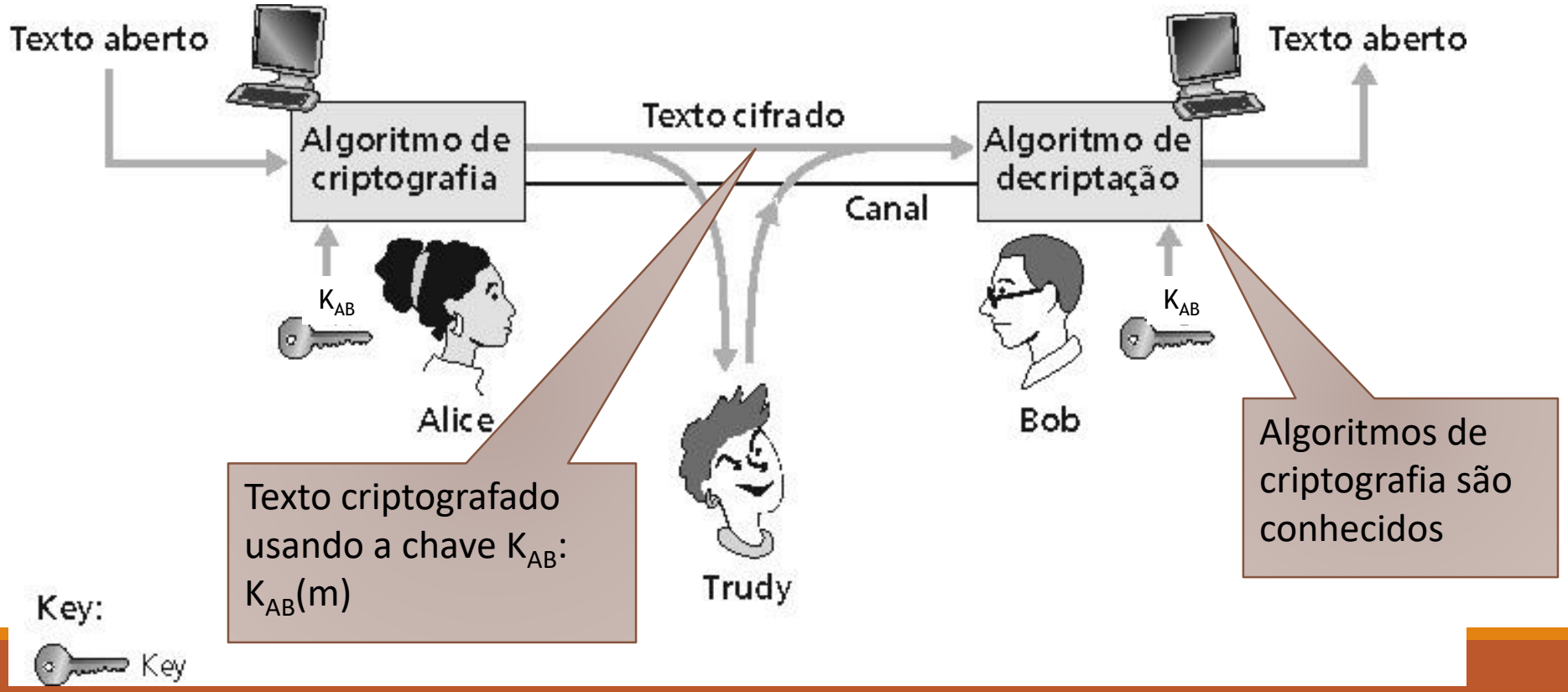
Uso de algoritmos de criptografia/decriptação que se baseia no uso de chaves (K)



Princípios da criptografia

Criptografia de chave simétrica:

- Bob e Alice compartilham a mesma chave (simétrica) conhecida: K_{AB} ($K_A = K_B$)
- Ex.: sabe que a chave corresponde ao padrão de substituição num código substituição monoalfabético



Criptografia de chave pública

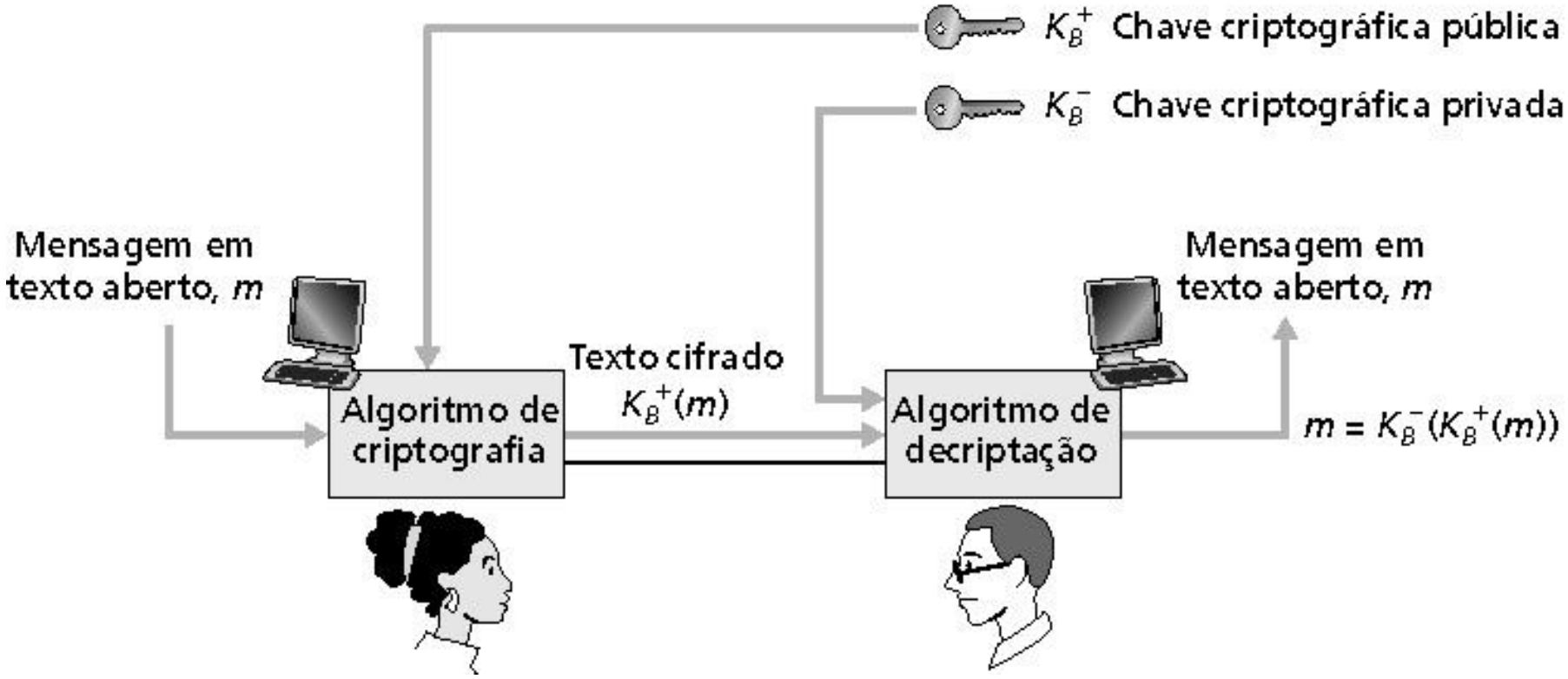
Chave simétrica

- Exige que o transmissor e o receptor compartilhem a chave secreta
- P.: Como combinar a chave inicialmente (especialmente no caso em que eles nunca se encontram)?

Chave pública

- Abordagem radicalmente diferente [Diffie-Hellman76, RSA78]
- Transmissor e receptor não compartilham uma chave secreta
- A chave de criptografia é *pública* (conhecida por *todos*)
- Chave de decriptografia é privada (conhecida somente pelo receptor)

Criptografia de chave pública (cont.)



Segurança em redes de computadores

O que é segurança?

Princípios da criptografia

Autenticação

Integridade

Distribuição de chaves e certificação

Controle de acesso: firewalls

Segurança em muitas camadas

Autenticação

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

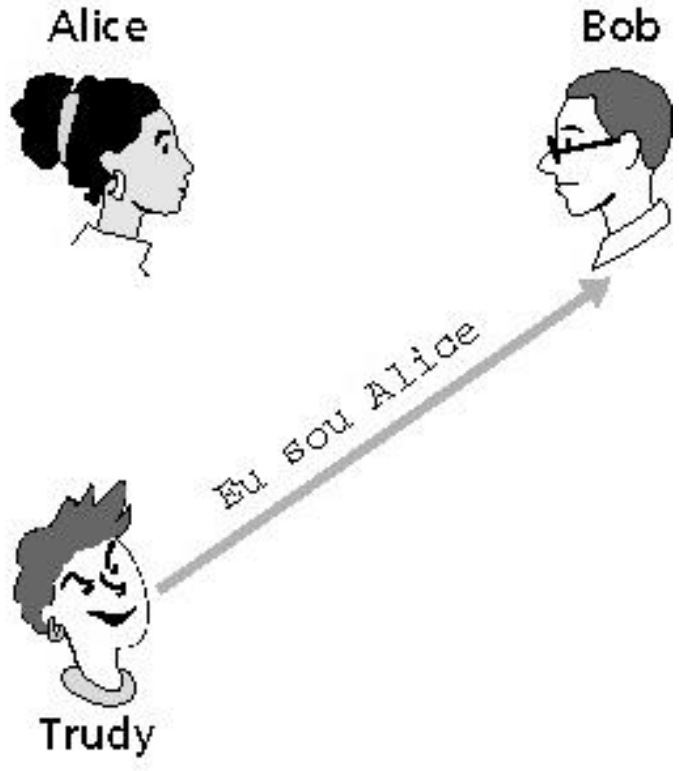
Protocolo ap1.0: Alice diz “Eu sou Alice”.

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.)

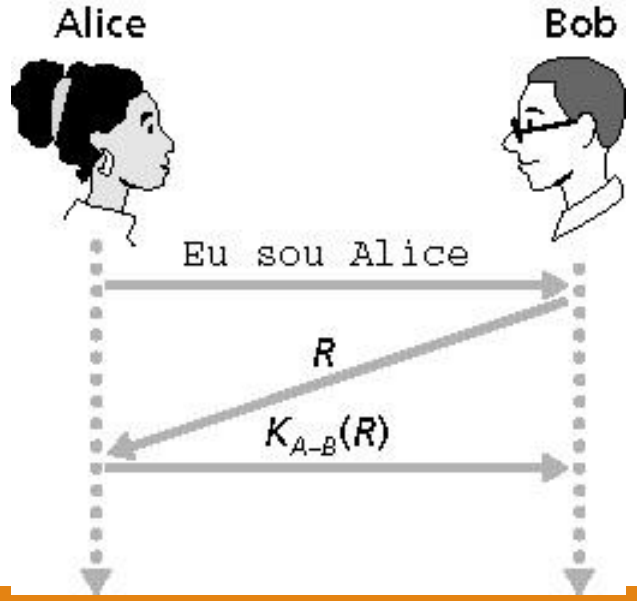
Protocolo ap3.1: Alice diz "Eu sou Alice" e envia sua senha secreta *criptografada* para prová-lo.

Não evita ataque de reprodução (playback).

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.

Meta: evitar ataque de reprodução (playback).

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



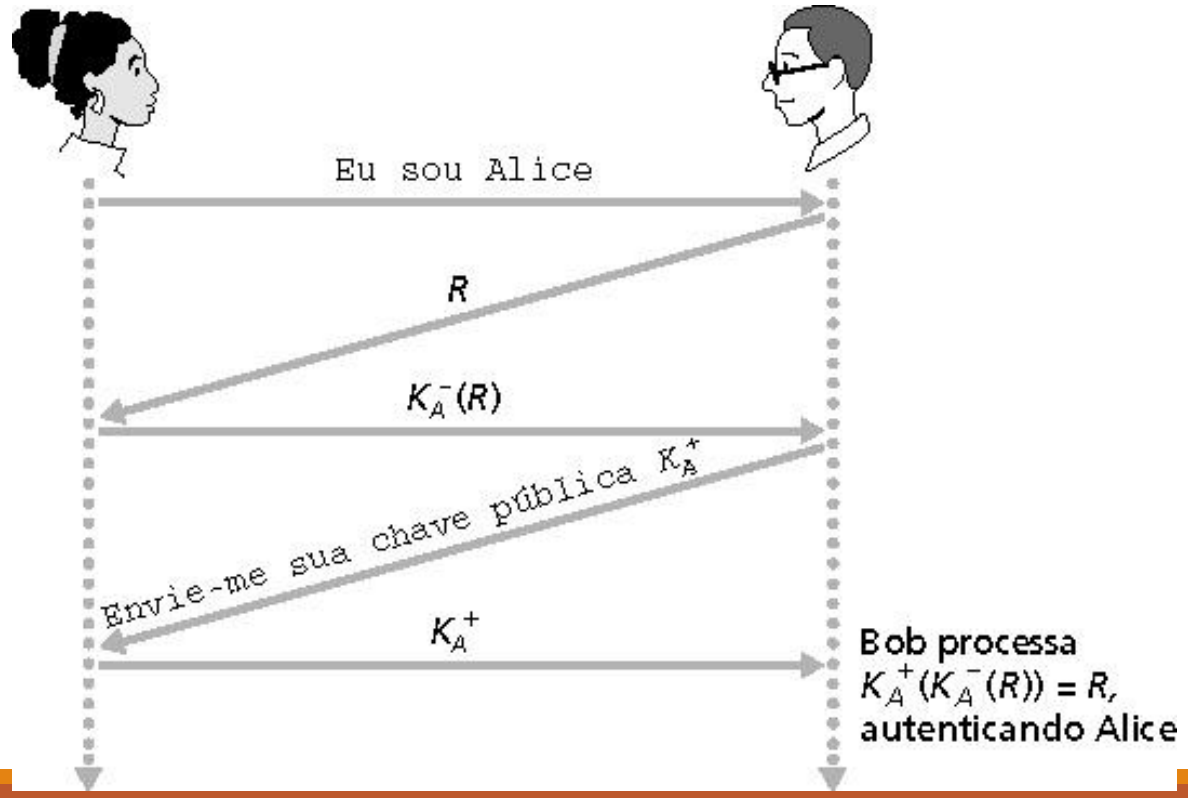
Alice está ao vivo, e apenas Alice conhece a chave para criptografar o nonce, então ela deve ser Alice!

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

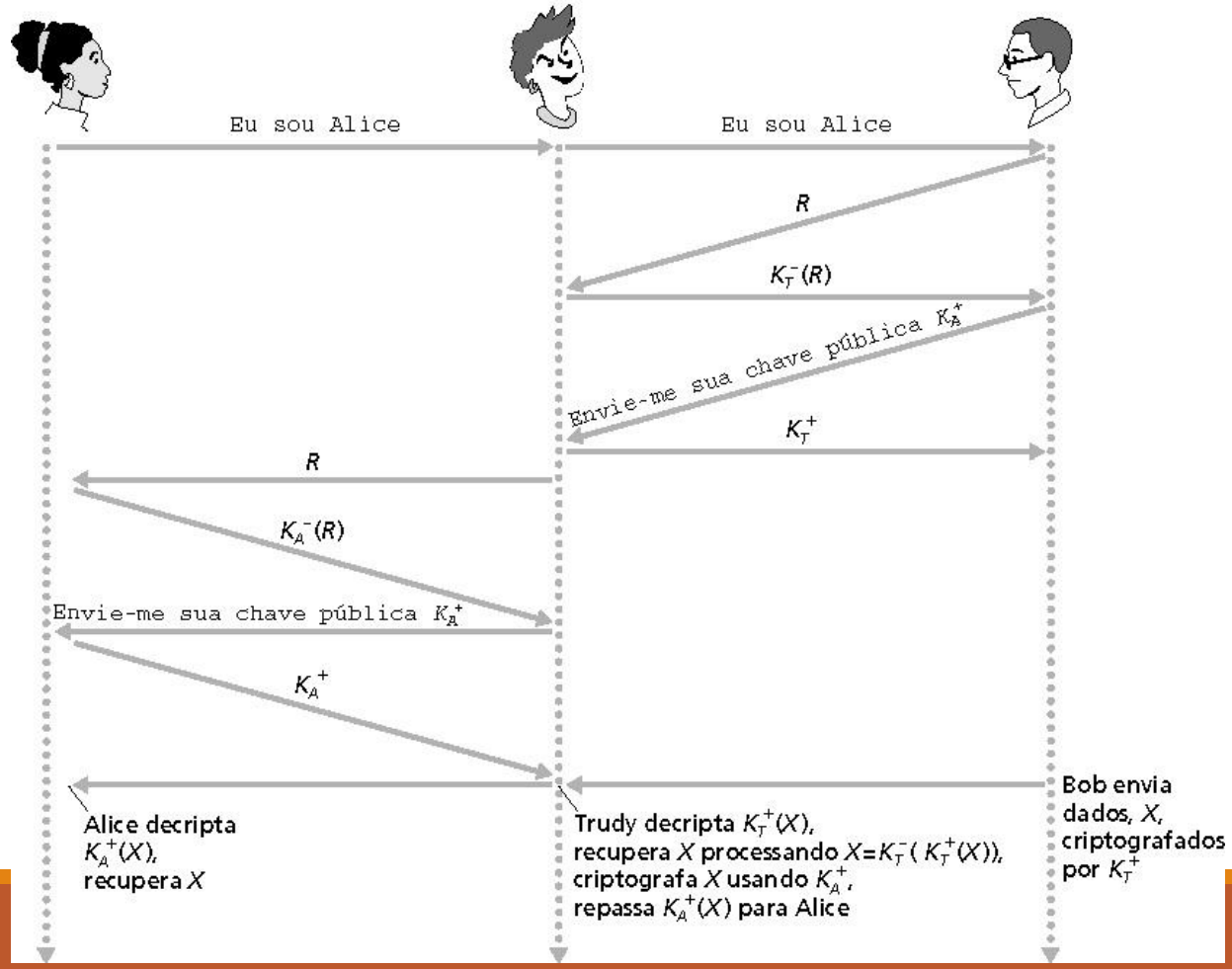
$$K_A^+ \ (K_A^-(R)) = R$$

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.

Segurança em redes de computadores

O que é segurança?

Princípios da criptografia

Autenticação

Integridade

Distribuição de chaves e certificação

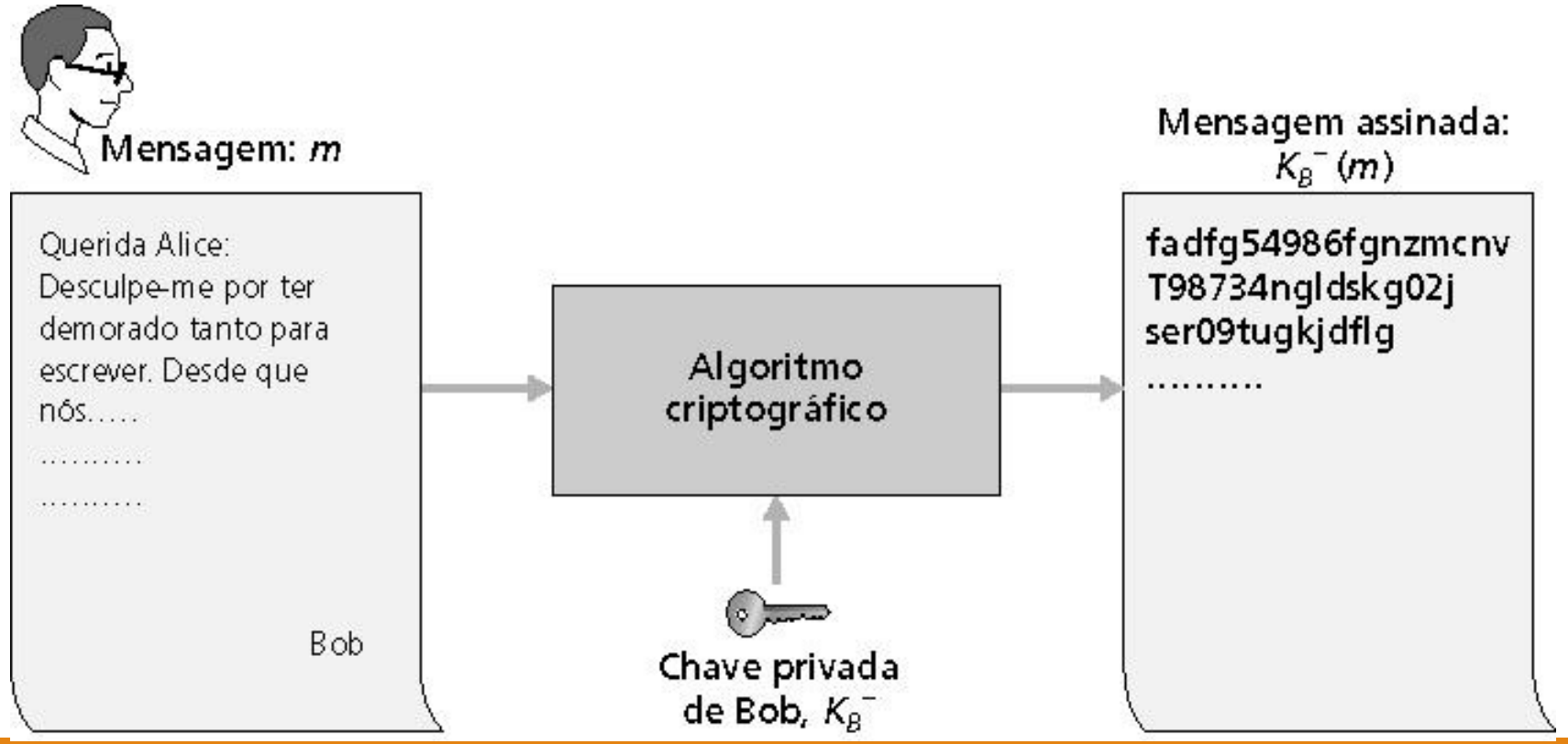
Controle de acesso: firewalls

Segurança em muitas camadas

Integridade: Assinaturas digitais

Assinatura digital simples para mensagem m:

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



Assinaturas digitais (mais)

Suponha que Alice receba a mensagem m e a assinatura digital $K_B^-(m)$

- Alice verifica que m foi assinada por Bob aplicando a chave pública de Bob K_B^+ para $K_B^+(m)$ e então verifica que $K_B^+(K_B^-(m)) = m$
- Se $K_B^+(K_B^-(m)) = m$, quem quer que tenha assinado m deve possuir a chave privada de Bob

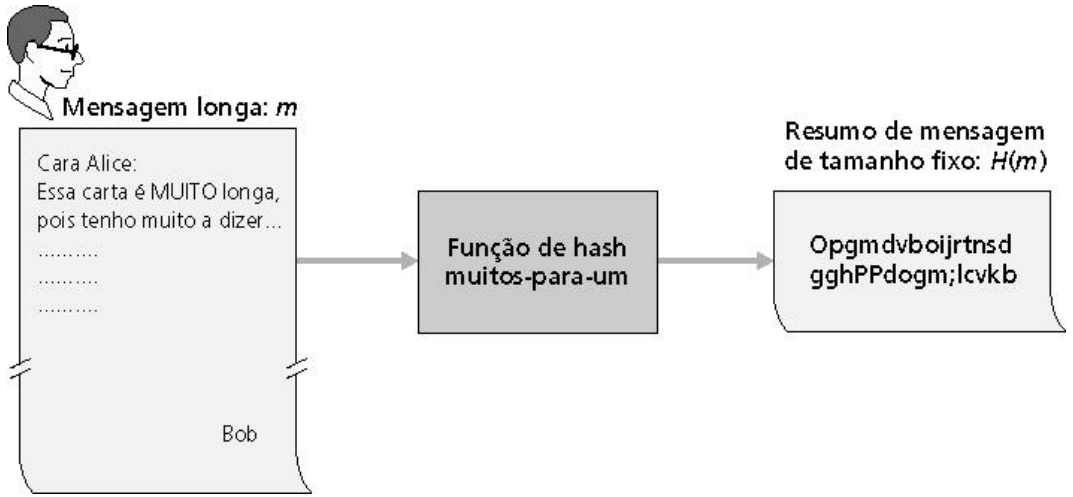
Não-repúdio:

- Alice pode levar m e a assinatura $K_B^-(m)$ a um tribunal para provar que Bob assinou m.

Resumos de mensagens

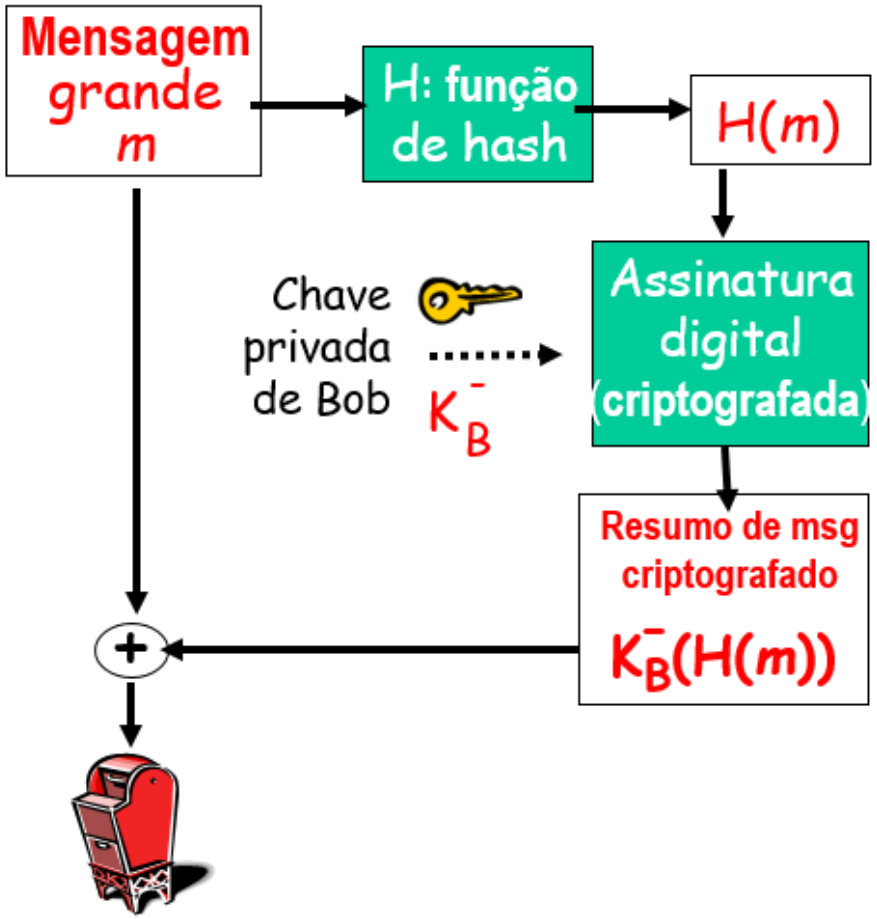
Computacionalmente caro criptografar mensagens longas com chave privada

- Meta: assinaturas digitais de tamanho fixo, facilmente computáveis, “impressão digital”
- Aplicar função hash H a m para obter um resumo de tamanho fixo, H(m)
- Propriedades das funções de hash:
  - Muitas-para-1
  - Produz um resumo da mensagem de tamanho fixo (impressão digital)
  - Dado um resumo da mensagem x, é computacionalmente impraticável encontrar m tal que H(x) = H(m)

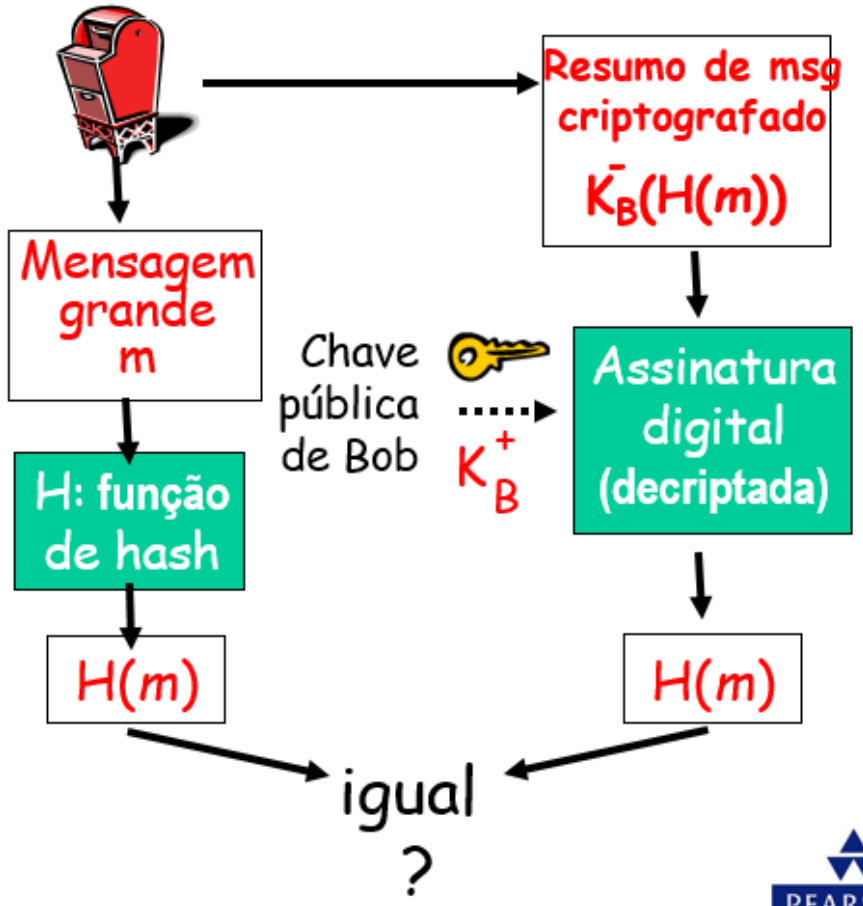


Assinatura digital = resumo assinado de mensagem

Bob envia mensagem digitalmente assinada:



Alice verifica a assinatura e a integridade da mensagem digitalmente assinada:



Algoritmos de funções de hash

MD5 (RFC 1321)

- Calcula resumo de 128 bits da mensagem num processo de 4 etapas
- Constatado que ele sofre de extensas vulnerabilidades.

SHA-1

- Padrão dos Estados Unidos [NIST, FIPS PUB 180-1]
- Resumo de mensagem de 160 bits

Segurança em redes de computadores

O que é segurança?

Princípios da criptografia

Autenticação

Integridade

Distribuição de chaves e certificação

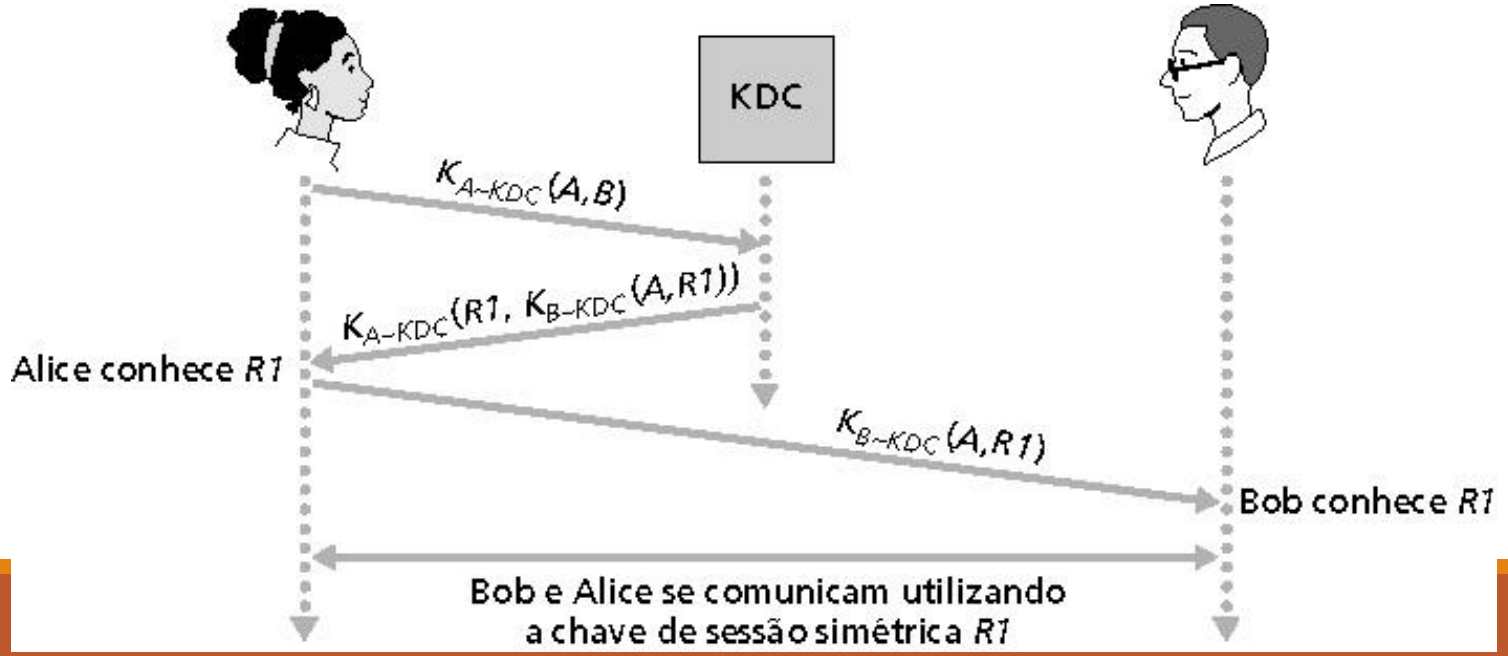
Controle de acesso: firewalls

Segurança em muitas camadas

Distribuição de chaves e certificação

Centro de distribuição de chave (KDC)

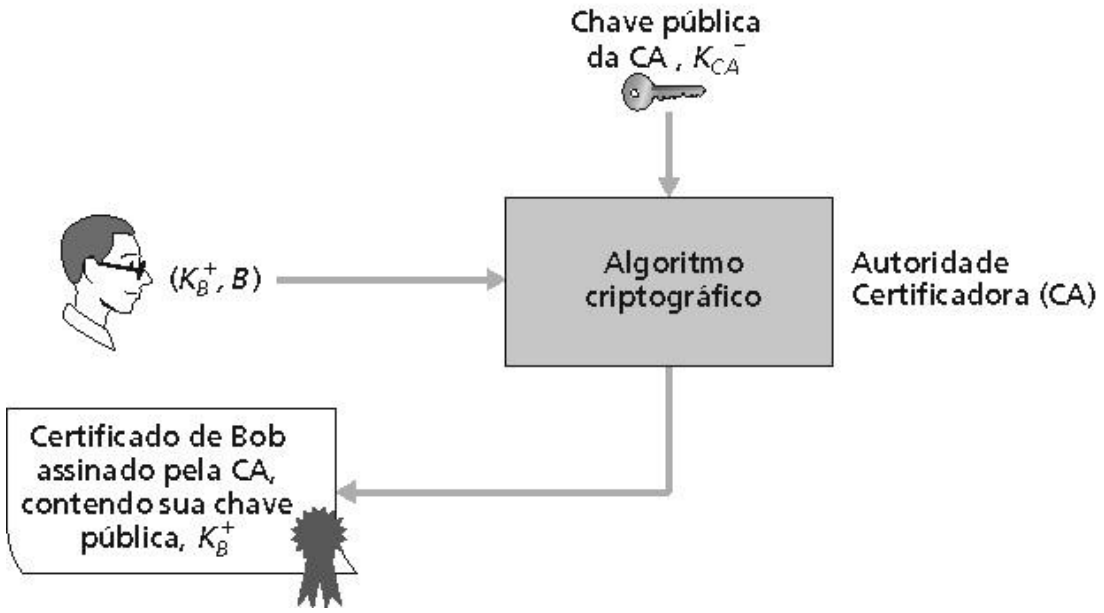
- Alice e Bob necessitam de uma chave simétrica comum
- KDC: servidor compartilha diferentes chaves secretas com cada usuário registrado (muitos usuários)
- Alice e Bob conhecem as próprias chaves simétricas, KA-KDC KB-KDC , para comunicação com o KDC



Distribuição de chaves e certificação

Autoridades certificadoras (CAs)

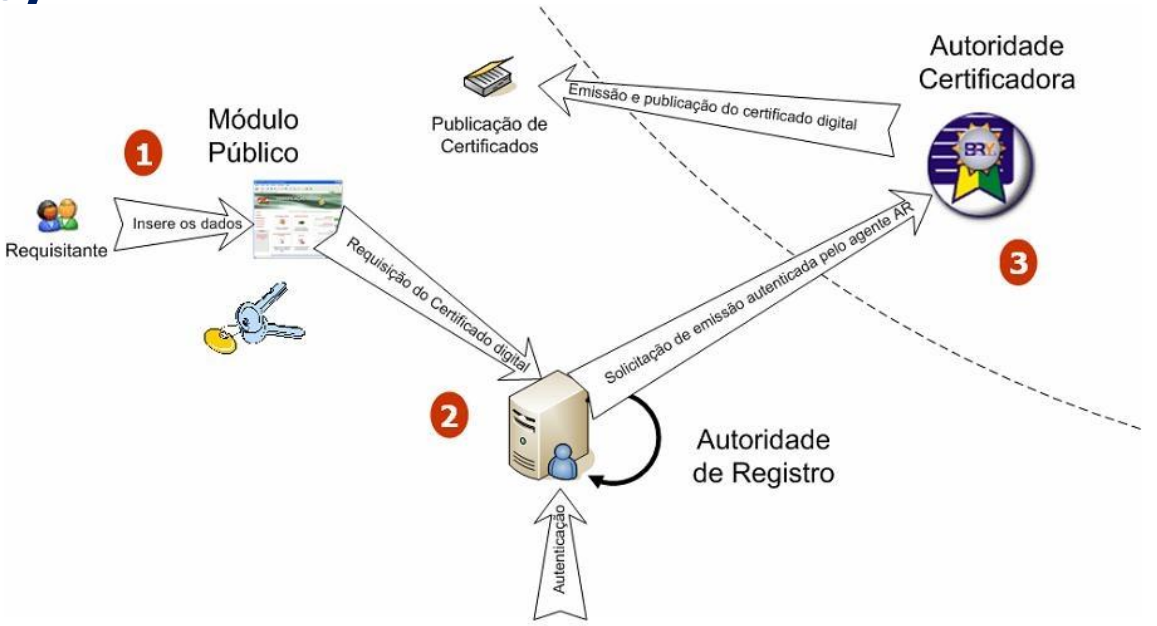
- CA associa uma chave pública a uma entidade em particular, E
- E (pessoa, roteador) registra sua chave pública com CA
  - E fornece “prova de identidade” ao CA
  - CA cria um certificado associando E à sua chave pública
  - Certificado contendo a chave pública de E digitalmente assinada pela CA. CA diz “esta é a chave pública de E”



Distribuição de chaves e certificação

ICP (Infraestrutura de Chaves Públicas)

- Órgão ou iniciativa pública ou privada que tem como objetivo manter uma estrutura de emissão de chaves públicas
- consiste de serviços, protocolos e aplicações utilizados para o gerenciamento de chaves públicas e certificados
- utiliza de certificados para determinar a autenticidade da chave



Segurança em redes de computadores

O que é segurança?

Princípios da criptografia

Autenticação

Integridade

Distribuição de chaves e certificação

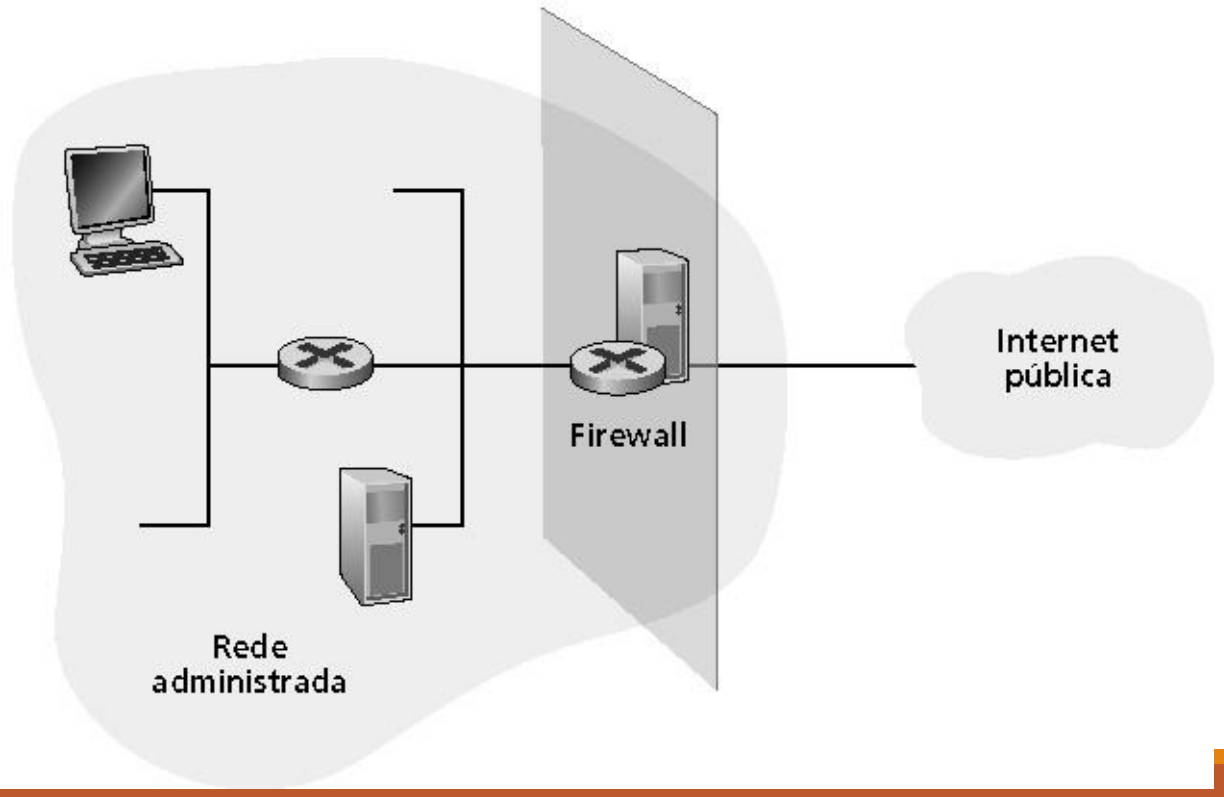
Controle de acesso: firewalls

Segurança em muitas camadas

Controle de acesso: firewalls

Firewall

- Isola a rede interna da organização da área pública da Internet, permitindo que alguns pacotes passem e outros não.



Firewalls: por quê?

Previne ataques de negação de serviço:

- Inundação de SYN: atacado estabelece muitas conexões TCP falsas, esgota os recursos para as conexões “reais”

Previne modificações e acessos ilegais aos dados internos

- Ex.: o atacante substitui a página da CIA por alguma outra coisa

Permite apenas acesso autorizado à rede interna (conjunto de usuários e hospedeiros autenticados)

Dois tipos de firewalls:

- Nível de aplicação
- Filtro de pacotes

Filtro de pacotes

Rede interna conectada à Internet via roteador firewall

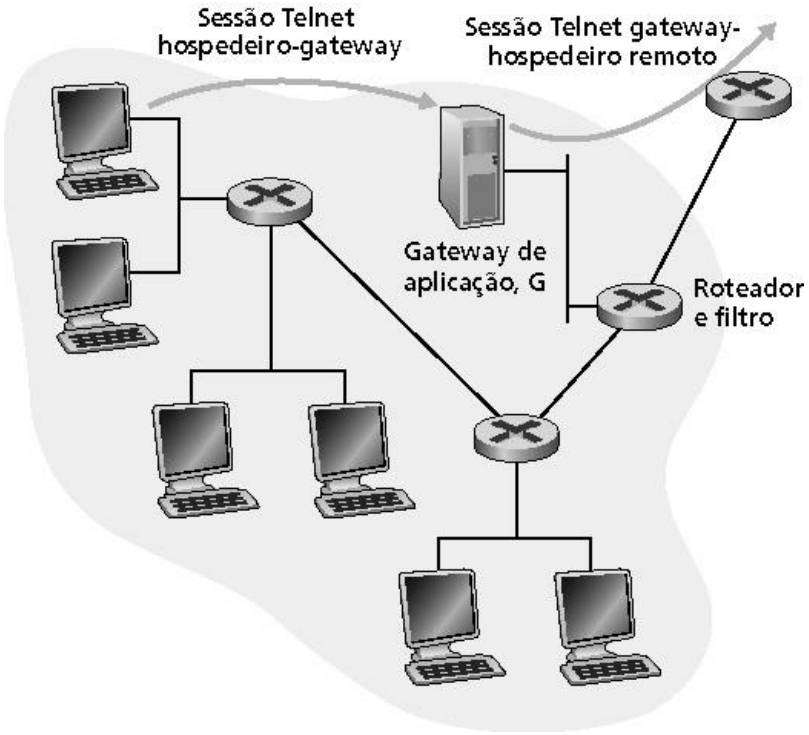
Roteador filtra pacotes; decisão de enviar ou descartar pacotes baseia-se em:

- Endereço IP de origem, endereço IP de destino
- Número de portas TCP/UDP de origem e de destino
- Tipo de mensagem ICMP
- Bits TCP SYN e ACK

Gateways de aplicação

Filtra pacotes em função de dados de aplicação, assim como de campos do IP/TCP/UDP

- Exemplo: permite selecionar usuários internos que podem usar o Telnet
  1) Exige que todos os usuários Telnet se comuniquem através do gateway
  2) Para os usuários autorizados, o gateway estabelece conexões Telnet com o hospedeiro de destino. O gateway repassa os dados entre as duas conexões
  3) O filtro do roteador bloqueia todas as sessões Telnet que não se originam no gateway



Sistemas de detecção de intrusões (IDS)

Solução complementar ao firewall

Software capazes de detectar atividades suspeitas

- Utiliza-se de padrões conhecidos de comportamento de intrusos
- Podem analisar o tráfego interno, externo e entre eles

Exemplo de sistema IDS

- http://www.snort.org/

Segurança em redes de computadores

O que é segurança?

Princípios da criptografia

Autenticação

Integridade

Distribuição de chaves e certificação

Controle de acesso: firewalls

Segurança em muitas camadas

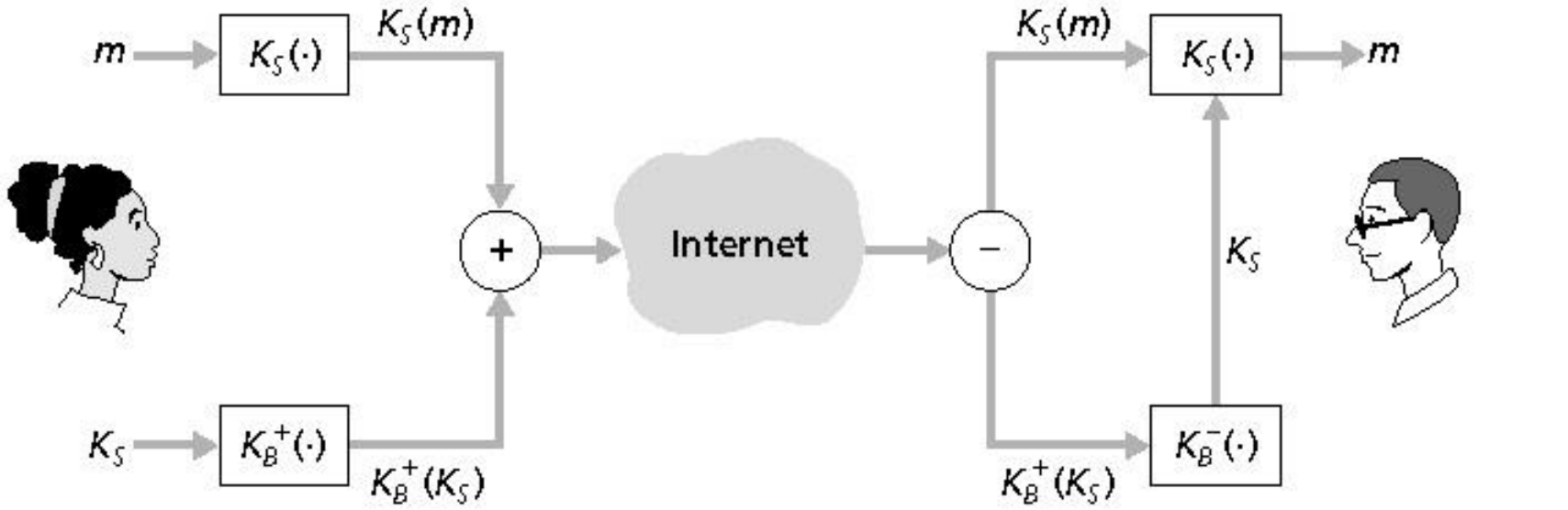
Segurança em redes de computadores

Segurança em muitas camadas

- e-mail seguro
- sockets seguros

E-mail seguro

- Alice quer enviar e-mail confidencial, *m*, para Bob.



Alice envia uma mensagem de e-mail, *m*

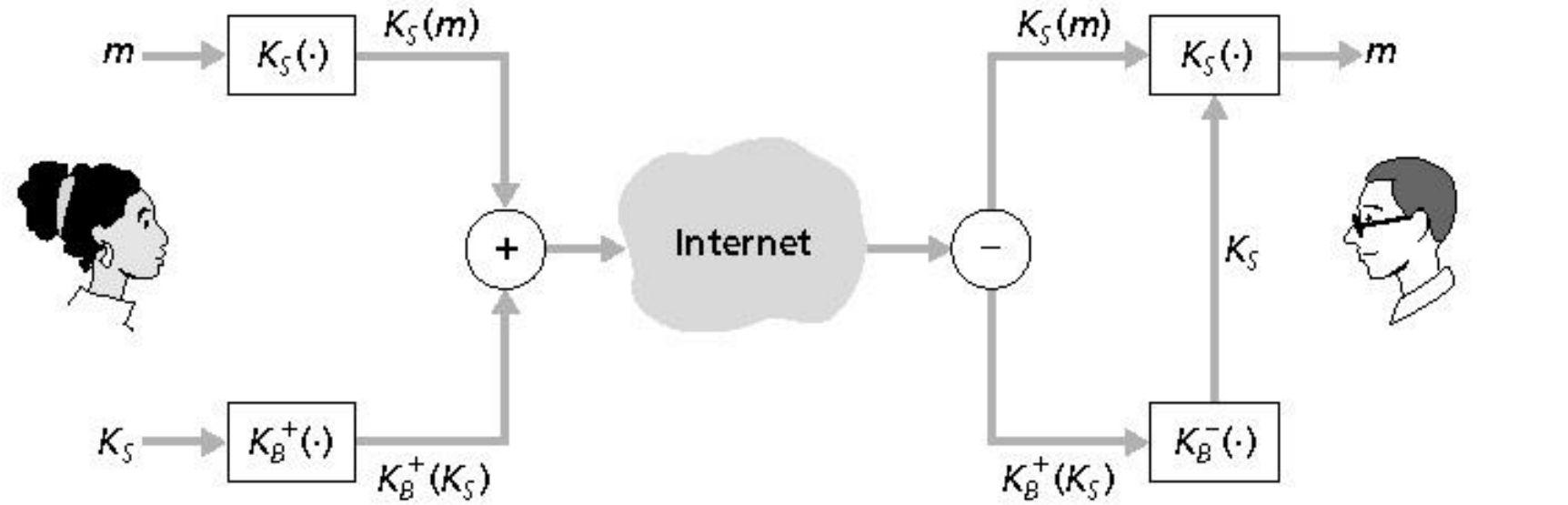
Bob recebe uma mensagem de e-mail, *m*

Alice:

- Gera uma chave privada *simétrica*, K_S
- Codifica mensagem com K_S (por eficiência)
- Também codifica K_S com a chave pública de Bob
- Envia tanto $K_S(m)$ como $K_B(K_S)$ para Bob

E-mail seguro (cont.)

- Alice quer enviar e-mail confidencial, *m*, para Bob.



Alice envia uma mensagem de e-mail, *m*

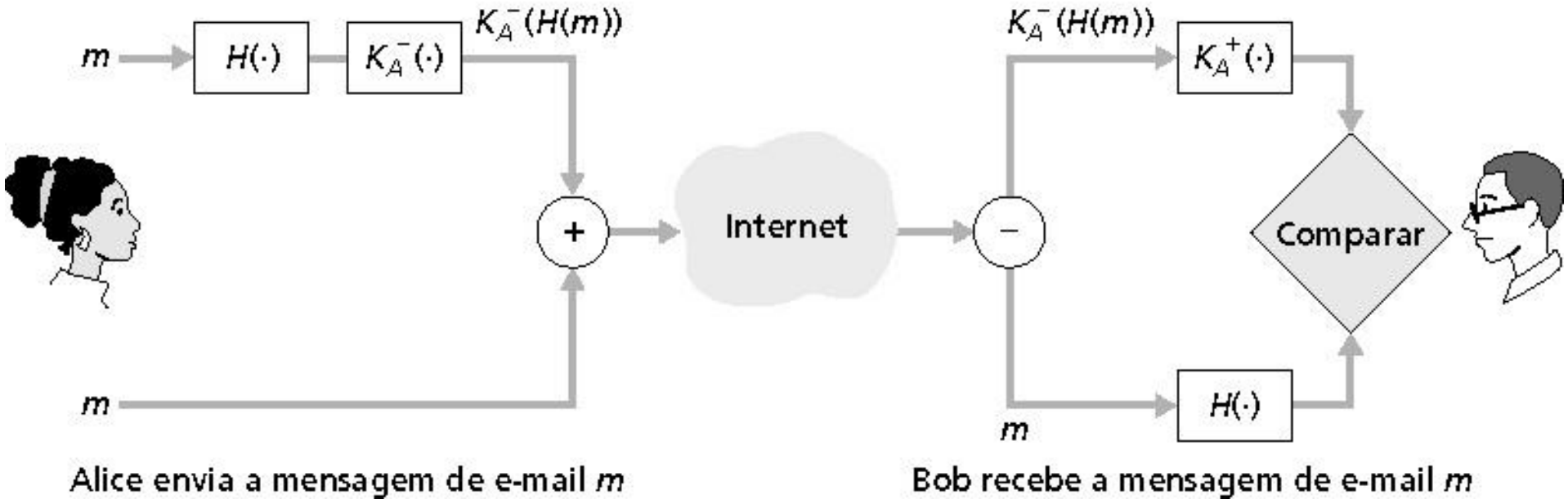
Bob recebe uma mensagem de e-mail, *m*

Bob:

- Usa sua chave privada para decodificar e recuperar K_S
- Usa K_S para decodificar $K_S(m)$ e recuperar *m*

E-mail seguro (cont.)

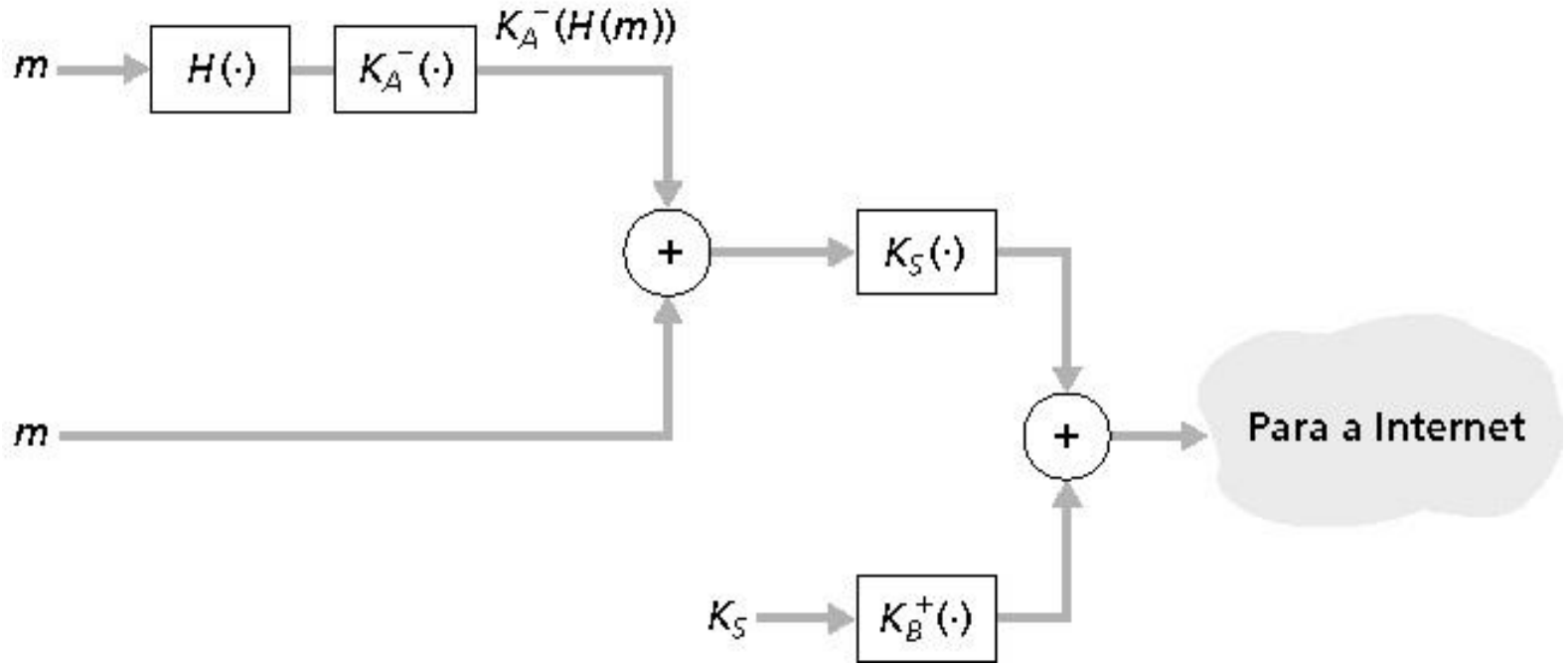
- Alice quer fornecer autenticação de emissor e integridade de mensagem.



- Alice assina digitalmente a mensagem
- Envia tanto a mensagem (aberta) quanto a assinatura digital

E-mail seguro (cont.)

- Alice quer fornecer confidencialidade, autenticação de emissor e integridade de mensagem



Alice usa três chaves: sua chave privada, a chave pública de Bob e uma nova chave simétrica

Pretty good privacy (PGP)

Uma mensagem PGP:

```
---BEGIN PGP SIGNED MESSAGE---
Hash: SHA1

Bob: My husband is out of town
 tonight.Passionately yours, Alice

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3mqJhFE
 vZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

Esquema de codificação de e-mail da Internet, padrão de fato

- Usa criptografia de chave simétrica, criptografia de chave pública, função de hash e assinatura digital
- Fornece confidencialidade, autenticação do emissor, integridade

Camada de sockets segura (SSL)

Segurança de camada de transporte para qualquer aplicação baseada no TCP usando serviços SSL

- Usado entre browsers Web e servidores para comércio eletrônico (https)

Serviços de segurança:

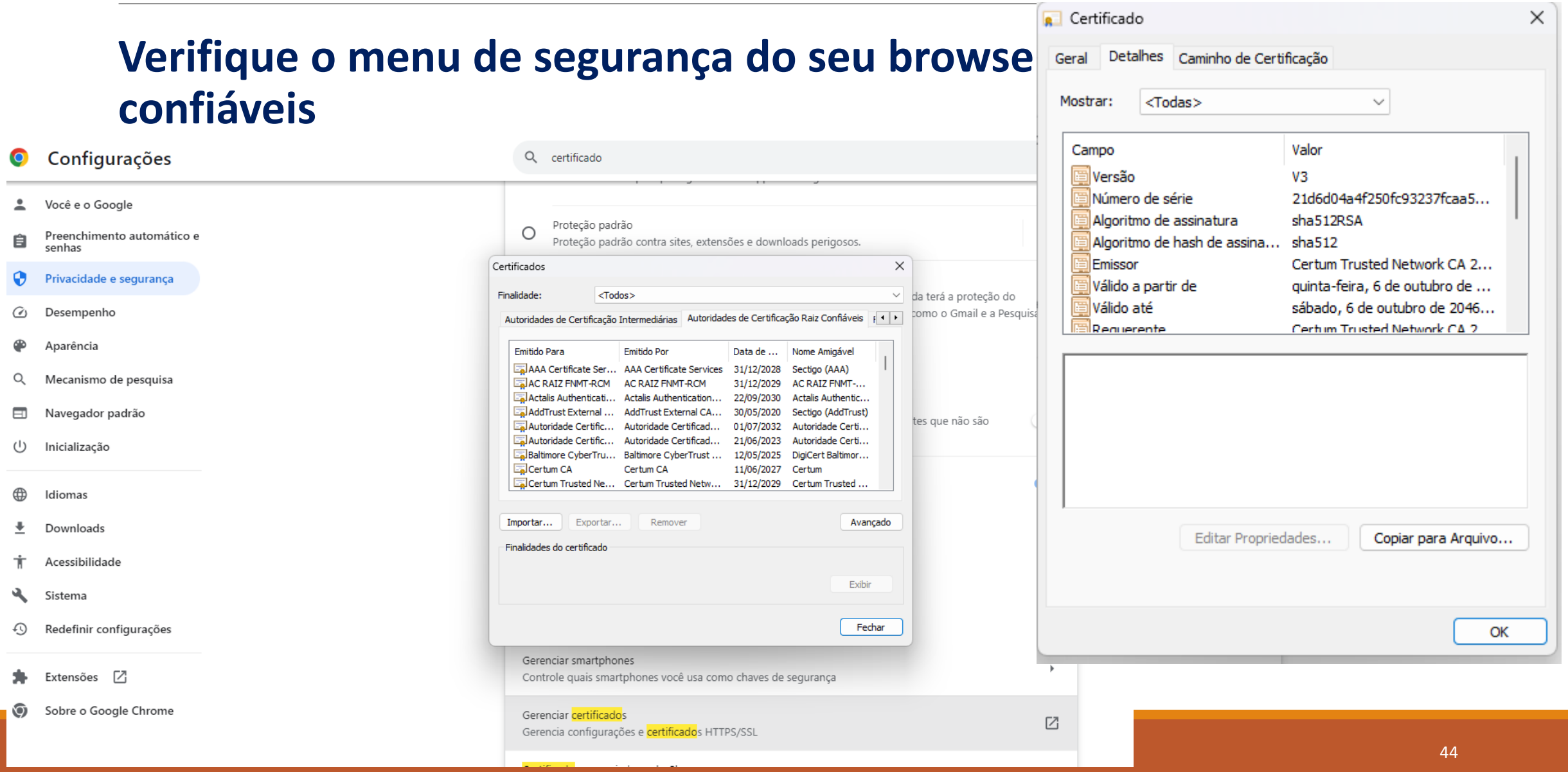
- Autenticação de servidor
- Criptografia de dados
- Autenticação de cliente (opcional)

Autenticação do Servidor:

- Browser com TLS/SSL habilitado inclui chaves públicas para CA confiáveis
- Browser pede certificado do servidor, emitido pela CA confiável
- Browser usa chave pública da CA para extrair a chave pública do servidor do certificado

Camada de sockets segura (SSL)

Verifique o menu de segurança do seu browse confiáveis



SSL (cont.)

Sessão SSL criptografada:

- Browser gera chave de sessão simétrica, criptografa essa chave com a chave pública do servidor e a envia para o servidor
- Usando a chave privada, o servidor recupera a chave de sessão
- Browser e servidor conhecem agora a chave de sessão
- Todos os dados são enviados para o socket TCP (pelo cliente e pelo servidor) criptografados com a chave de sessão

SSL pode ser usado por aplicações fora da Web; ex., IMAP

Autenticação do cliente pode ser feita com certificados do cliente