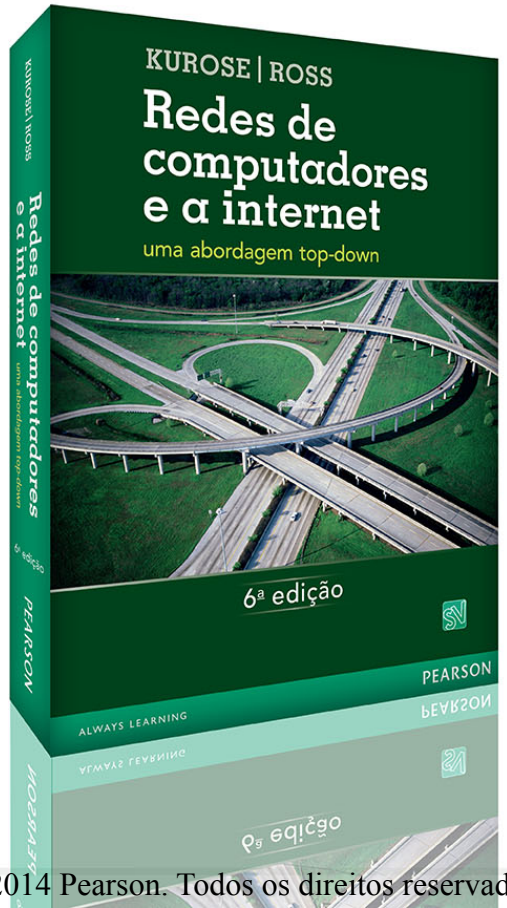
Segurança em redes de computadores

Parte 1



Introdução

- Alice e Bob são duas pessoas que desejam se comunicar “com segurança”.
  - Dois roteadores que querem trocar tabelas de roteamento com segurança.
  - Um cliente e um servidor que querem estabelecer uma conexão de transporte segura.
  - Duas aplicações de e-mail que querem trocar e-mails com segurança.

O que é segurança de rede?

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- O que significa comunicar com segurança?
  - Alice quer que somente Bob entenda a mensagem que ela envia.
    - Comunicação ocorre em um meio inseguro. Um intruso (Trudy) pode interceptar, ler e executar processos computacionais com qualquer dado transmitido de Alice para Bob.
  - Bob quer ter certeza de que a mensagem que recebe de Alice foi de fato enviada por ela. Alice quer ter certeza de que a pessoa com quem está se comunicando é de fato Bob.
  - Alice e Bob querem ter certeza de que o conteúdo de suas mensagens não foi alterado em trânsito.

O que é segurança de rede?

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

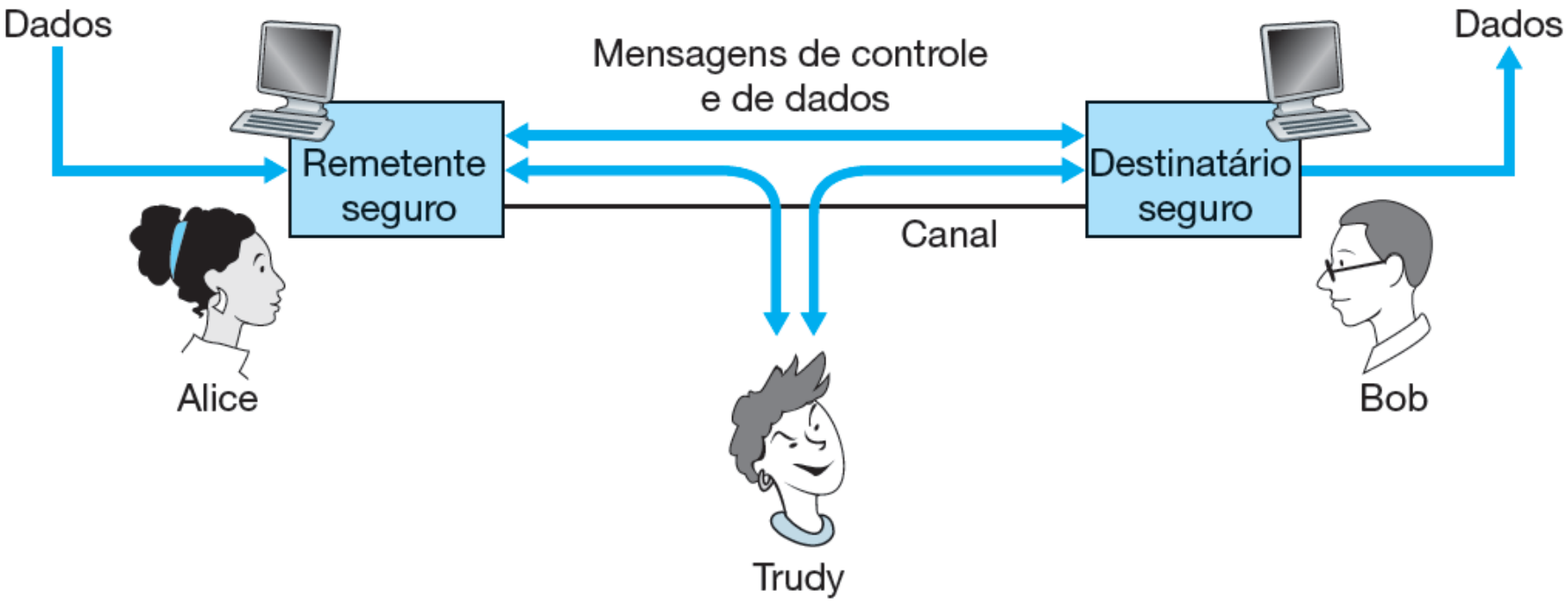
- Propriedades desejáveis da **comunicação segura:**
  - *Confidencialidade:* Somente o remetente e o destinatário pretendido devem poder entender o conteúdo da mensagem transmitida.
    - Mensagem deve ser **cifrada** (“disfarçar” os dados de alguma maneira).
    - Impedir que uma mensagem interceptada seja **decifrada** (entendida) por um interceptador.
  - *Integridade:* Remetente e destinatário querem assegurar que o conteúdo de sua comunicação não seja alterado, por acidente ou por má intenção, durante a transmissão.

O que é segurança de rede?

- Propriedades desejáveis da **comunicação segura:**
  - *Autenticação:* Remetente e destinatário precisam confirmar a identidade da outra parte envolvida na comunicação
    - Confirmar que a outra parte realmente é quem alega ser.

O que é segurança de rede?

- Remetente, destinatário e intruso (Alice, Bob e Trudy)



O que é segurança de rede?

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- Quais informações um intruso pode ter acesso e que ações podem ser executadas por ele?
  - *Monitorar* – ouvir e gravar as mensagens de controle e de dados no canal.
  - *Modificar, inserir ou eliminar* mensagens ou conteúdo de mensagens.
- Possibilita montar uma grande variedade de ataques à segurança:
  - Roubar senhas e dados.
  - Fazer-se passar por outra entidade.
  - Sequestrar uma sessão em curso.

Princípios de criptografia

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- Técnicas criptográficas permitem que um remetente disfarce os dados de modo que um intruso não consiga obter nenhuma informação dos dados interceptados.

- O destinatário deve estar habilitado a recuperar os dados originais a partir dos dados disfarçados.

  - Criptografia fornece naturalmente confidencialidade.

  - Utilizada também para prover integridade e autenticação.

Princípios de criptografia

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- Suponha que Alice queira enviar uma mensagem a Bob.
- A mensagem de Alice em sua forma original é conhecida como **texto aberto** (m) ou **texto claro**.
- Alice criptografa sua mensagem em texto aberto usando um **algoritmo de criptografia.**
  - Padronizados e disponíveis para qualquer um.
- Alice fornece uma **chave** (K_A) como entrada para o algoritmo de criptografia.
- O algoritmo de criptografia gera uma mensagem criptografada, conhecida como **texto cifrado** ($K_A(m)$), que parece ininteligível para qualquer intruso.

Princípios de criptografia

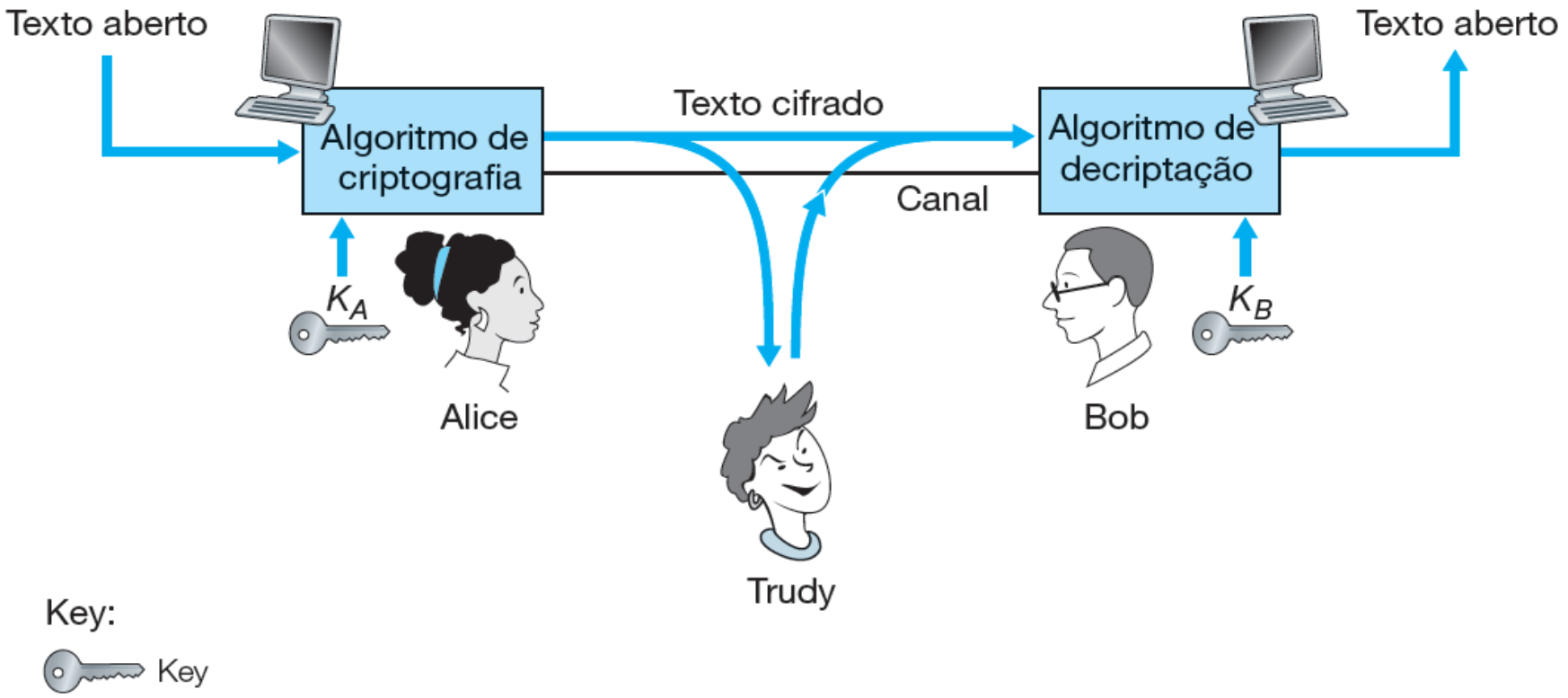
KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- De maneira semelhante, Bob fornecerá uma chave (K_B) ao **algoritmo de decriptação**.
  - Pega o texto cifrado e a chave de Bob como entrada e produz o texto aberto original como saída.
    - $K_B(K_A(m)) => m$
- Em **sistemas de chaves simétricas**, as chaves de Alice e Bob são idênticas e secretas.
- Em **sistemas de chaves públicas**, é usado um par de chaves.
  - Uma das chaves é conhecida por Bob e Alice (mundo inteiro).
  - A outra chave é conhecida apenas por Bob ou por Alice (mas não ambos).

Criptografia de chaves simétricas

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- Componentes criptográficos



Criptografia de chaves simétricas

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- **Cifra de César**
  - Algoritmo de chaves simétricas muito antigo, muito simples, atribuído a Júlio César.
  - Tomar cada letra da mensagem do texto aberto e substitui-la pela k-ésima letra sucessiva do alfabeto.
  - Exemplo: k= 3
    - ‘a’ -> ‘d’; ‘b’ -> ‘e’
    - Mensagem “*bob, i love you. alice*” se torna “*ere, l oryh brx. dolfh*” em texto cifrado.

Criptografia de chaves simétricas

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- **DES** (*Data Encryption Standard*)
  - Desenvolvido em 1977
  - Codifica texto aberto em porções de 64 bits usando uma chave de 56 bits.
  - Considerado inseguro.
    - No desafio DES Challange III de 1999 conseguiram decodificar uma mensagem em pouco mais de 22 horas.

Criptografia de chaves simétricas

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- **DES triplo (3DES)**
  - Proposto como padrão criptográfico para o PPP.

  1. O 3DES executa primeiro o algoritmo de criptografia DES sobre os dados utilizando uma primeira chave de 56 bits.

  2. Em seguida, executa o algoritmo de decriptação DES sobre a saída da primeira rodada de criptografia usando uma segunda chave.

  3. Finalmente, executa o algoritmo de criptografia DES sobre a saída da segunda rodada usando uma terceira chave.

Criptografia de chaves simétricas

- **AES** (*Advanced Encryption Standard*)
  - Sucessor do DES.
  - Processa dados em blocos de 128 bits.
  - Pode funcionar com chaves de 128, 192 e 256 bits.
  - Estima-se que uma máquina que conseguisse quebrar o DES de 56 bits em 1 segundo levaria aproximadamente 149 trilhões de anos para quebrar uma chave AES de 128 bits.

Criptografia de chave pública

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- A criptografia de chaves simétricas exige que as duas partes comunicantes compartilhem um segredo em comum (chave simétrica).
    - As duas partes têm de concordar, de alguma maneira, com a chave compartilhada.
        - É preciso comunicação segura!
- Criptografia de chave pública permite que duas partes se comuniquem por criptografia sem compartilhar uma chave comum secreta conhecida com antecedência.
- Propriedades úteis tanto para a confidencialidade quanto para autenticação e assinaturas digitais.

Criptografia de chave pública

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- Suponha que Alice queira enviar uma mensagem (*m*) para Bob.
- Bob (destinatário) tem duas chaves:
  - **Chave pública (K_B^+):** está à disposição do mundo todo (inclusive Trudy, a intrusa).
  - **Chave privada (K_B^-):** apenas Bob conhece.

Criptografia de chave pública

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

1. Alice busca a chave pública de Bob (K_B^+).

2. Alice criptografa *m* usando a chave pública de Bob e um algoritmo criptográfico conhecido (calcula $K_B^+(m)$).

3. Bob recebe a mensagem criptografada de Alice ($K_B^+(m)$) e usa sua chave privada (K_B^-) e um algoritmo de decriptação para decifrar a mensagem de Alice (calcula $K_B^-(K_B^+(m)) \Rightarrow m$).

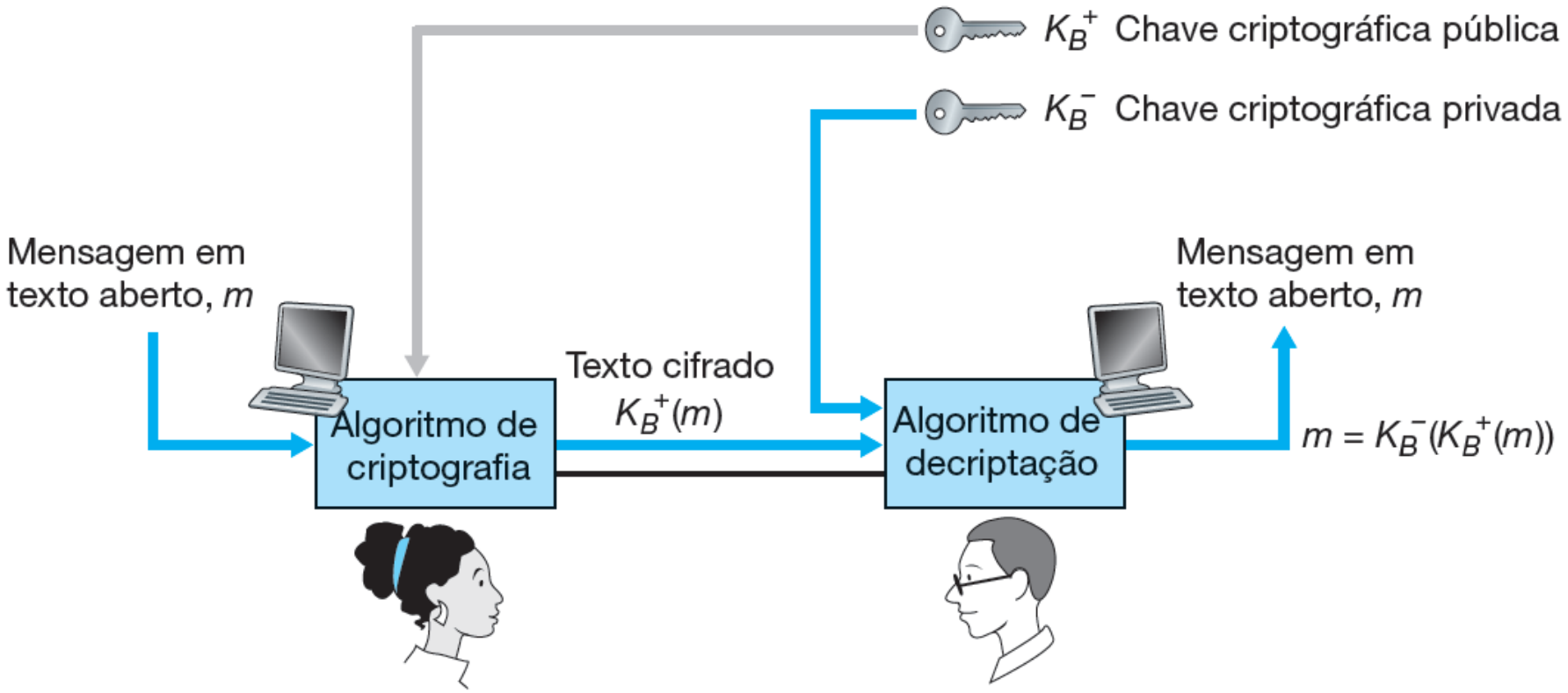
   - É possível permutar a chave pública e a chave privada:

     - $K_B^-(K_B^+(m)) = K_B^+(K_B^-(m)) = m$

Criptografia de chave pública

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- Criptografia de chaves públicas



RSA

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- O algoritmo **RSA** (Ron Rivest, Adi Shamir e Leonard Adleman) tounou-se um sinônimo de criptografia de chave pública
- Há dois componentes inter-relacionados no RSA.
  - A escolha da chave pública e da chave privada.
  - O algoritmo de criptografia/decriptação.

RSA

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- Escolha das chaves pública e privada:

  1. Escolher dois números primos grandes, *p* e *q*.

  2. Computar *n = pq* e *z = (p - 1)(q - 1)*.

  3. Escolher um número *e* (*encryption*) menor que *n* que não tenha fatores comuns com *z* (*e* e *z* são números primos entre si).

  4. Achar um número *d* (*decryption*), tal que *ed – 1* seja divisível exatamente por *z*.

  5. A chave pública que Bob põe à disposição de todos (K_B^+) é o par de números (*n, e*); sua chave privada (K_B^-) é o par de números (*n, d*).

RSA

- A criptografia e decriptação:
  - Alice quer enviar a Bob um padrão de bits, ou número m, tal que $m < n$. Assim, o valor cifrado (c) da mensagem em texto aberto (m) que Alice envia é:
    - $c = m^e \bmod n$
- Para decifrar a mensagem em texto cifrado recebida, Bob processa:
  - $m = c^d \bmod n$

RSA

- Exemplo: $e = 5$, $n = 35$

Plaintext Letter	m: numeric representation	m^e	Ciphertext $c = m^e \bmod n$
l	12	248832	17
o	15	759375	15
v	22	5153632	22
e	5	3125	10

Criptografia RSA

RSA

- Exemplo: $d = 29$, $n = 35$

Ciphertext c	c^d	$m = c^d \bmod n$	Plaintext Letter
17	481968572106750915091509141 1825223071697	12	l
15	12783403940394885893911123275756835 9375	15	o
22	85164331908653770195619449972 1106030592	22	v
10	10000000000000000000000000000000	5	e

Decriptação RSA

RSA e Chaves de Sessão

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- A exponenciação exigida pelo RSA é um processo que consome tempo considerável.

- Na prática, RSA é usando em combinação com um algoritmo de chave simétrica (DES ou AES).

- Alice quer enviar a Bob uma grande quantidade de dados.

    1. Alice escolhe uma chave DES (**chave de sessão** – K_S) que será utilizada para codificar os dados em si.
    2. Alice criptografa a chave de sessão usando a chave pública RSA de Bob ($c = (K_S)^e \ mod \ n$)
    3. Bob recebe a chave de sessão codificada RSA (c), e a decifra para obter a chave de sessão K_S que Alice usará para transferir dados cifrados em DES.

Integridade

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- Como indicar o dono ou o criador de um documento?
- Como deixar claro que alguém concorda com o conteúdo do documento?
- Exemplo: ao receber uma mensagem de Alice, Bob precisa verificar se:
  1. A mensagem foi, realmente, enviada por Alice.
  2. A mensagem não foi alterada em seu caminho para Bob.

Assinaturas digitais

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- A assinatura digital é uma técnica criptográfica que cumpre essas finalidades no mundo digital.
- Uma assinatura digital deve ser:
  - *Verificável*: provar que um documento assinado por um indivíduo foi na verdade assinado por ele.
  - *Não falsificável*: somente aquele indivíduo pode ter assinado o documento.
  - *Incontestável*: o signatário não pode mais tarde negar que assinou o documento.

Assinaturas digitais

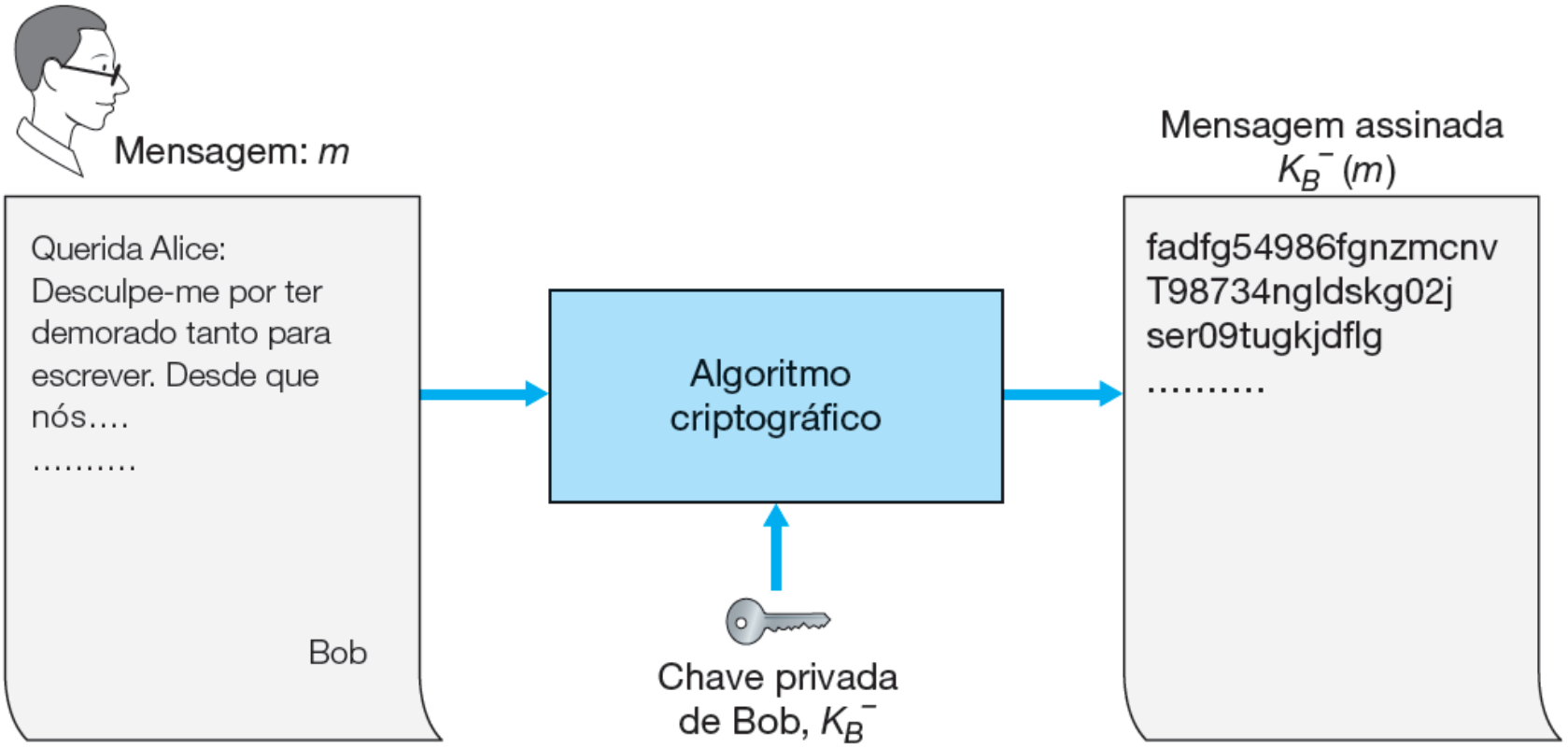
KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- Suponha que Bob queira assinar digitalmente um documento *m*.
- Para assinar esse documento, Bob simplesmente usa sua chave criptográfica privada K_B^- para processar $K_B^-(m)$.
- Bob tem o documento *m*, e sua assinatura digital do documento é $K_B^-(m)$.

Assinaturas digitais

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- Criando uma assinatura digital para um documento



Assinaturas digitais

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- A assinatura digital $K_B^-(m)$ atende às exigências de ser verificável, não falsificável e não repudiável?

- Como Alice prova que Bob de fato assinou o documento e que ele era a única pessoa que poderia tê-lo assinado?

  - Alice pega a chave pública de Bob, K_B^+, e a aplica à assinatura digital $K_B^-(m)$ associada ao documento m.

    - $K_B^+(K_B^-(m))$, o que produz m.

    - Reprodução exata do documento original.

Assinaturas digitais

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- Somente Bob pode ter assinado o documento pelas seguintes razões:
  - Quem assinou o documento deve ter usado a chave criptográfica privada K_B^-, para processar a assinatura $K_B^-(m)$, de modo que $K_B^+(K_B^-(m)) = m$.
  - A única pessoa que poderia conhecer a chave privada K_B^- é Bob.

Resumos de mensagens

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- Dada a sobrecarga de criptografia e decriptação, a assinatura de dados por criptografia/decriptação da mensagem completa pode ser exagerada.

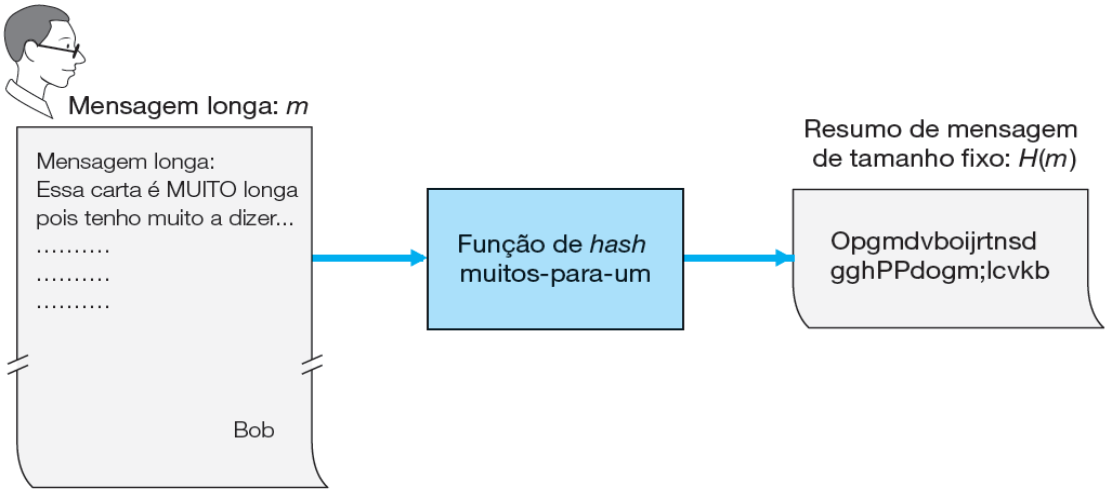
- Um **resumo de mensagem** recebe uma mensagem *m*, de comprimento arbitrário e calcula uma "impressão digital" dos dados, com comprimento fixo, conhecida como resumo de mensagem *H*(*m*).

- Se *m* for modificado para *m'*, então *H(m)* processada para os dados originais não combinará com *H(m')* processada sobre os dados modificados.

Funções de *hash* criptográficas

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

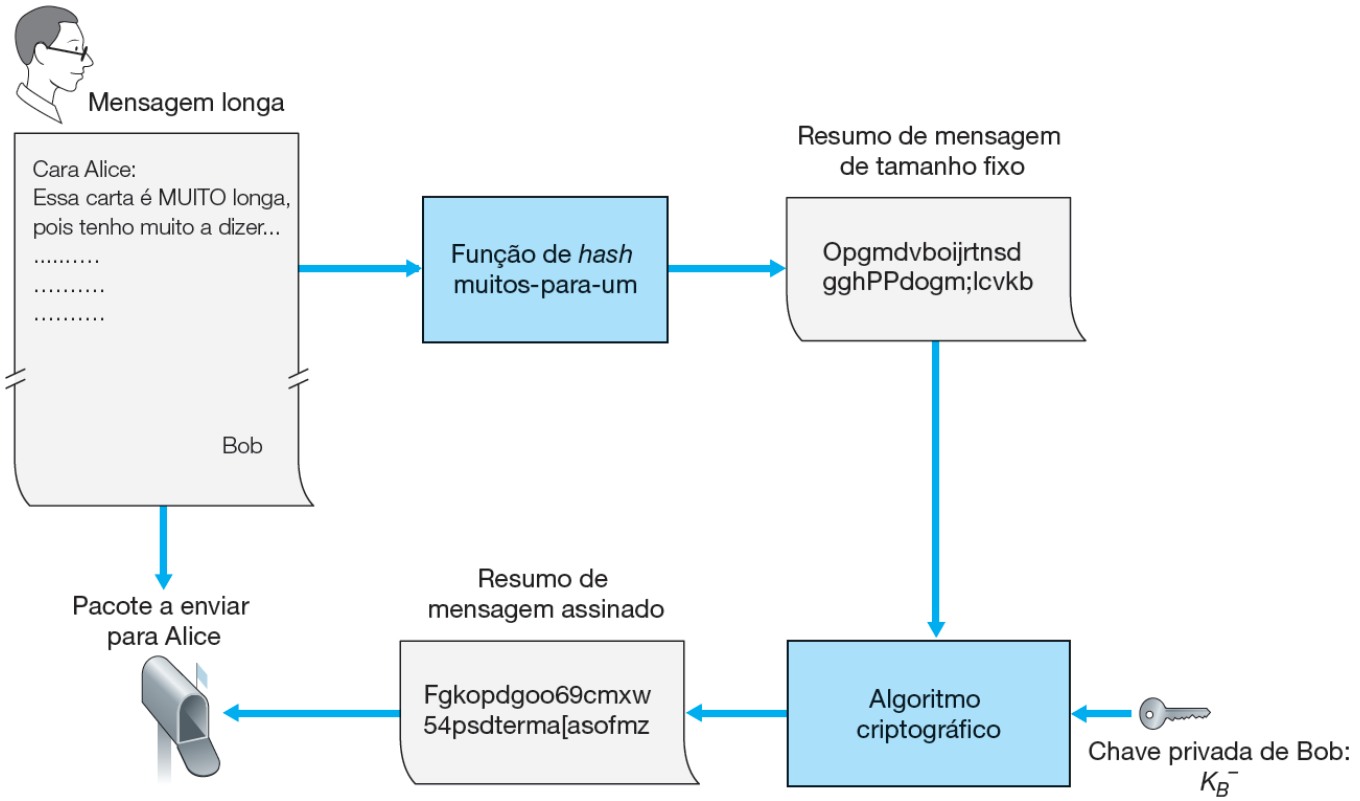
- Uma **função *hash* criptográfica** deve apresentar a seguinte propriedade:
  - Em termos de processamento, é impraticável encontrar duas mensagens diferentes x e y tais que $H(x) = H(y)$.



Assinaturas digitais

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

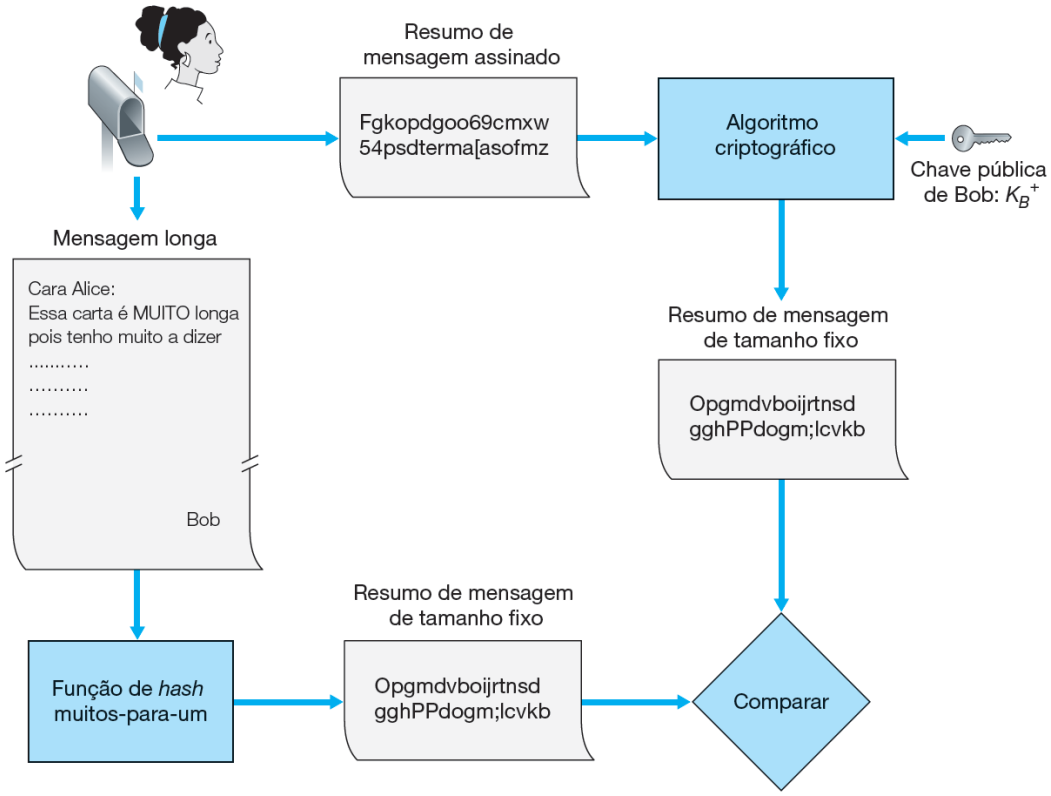
- Enviando uma mensagem assinada digitalmente



Assinaturas digitais

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- Verificando uma mensagem assinada



Certificação de chaves públicas

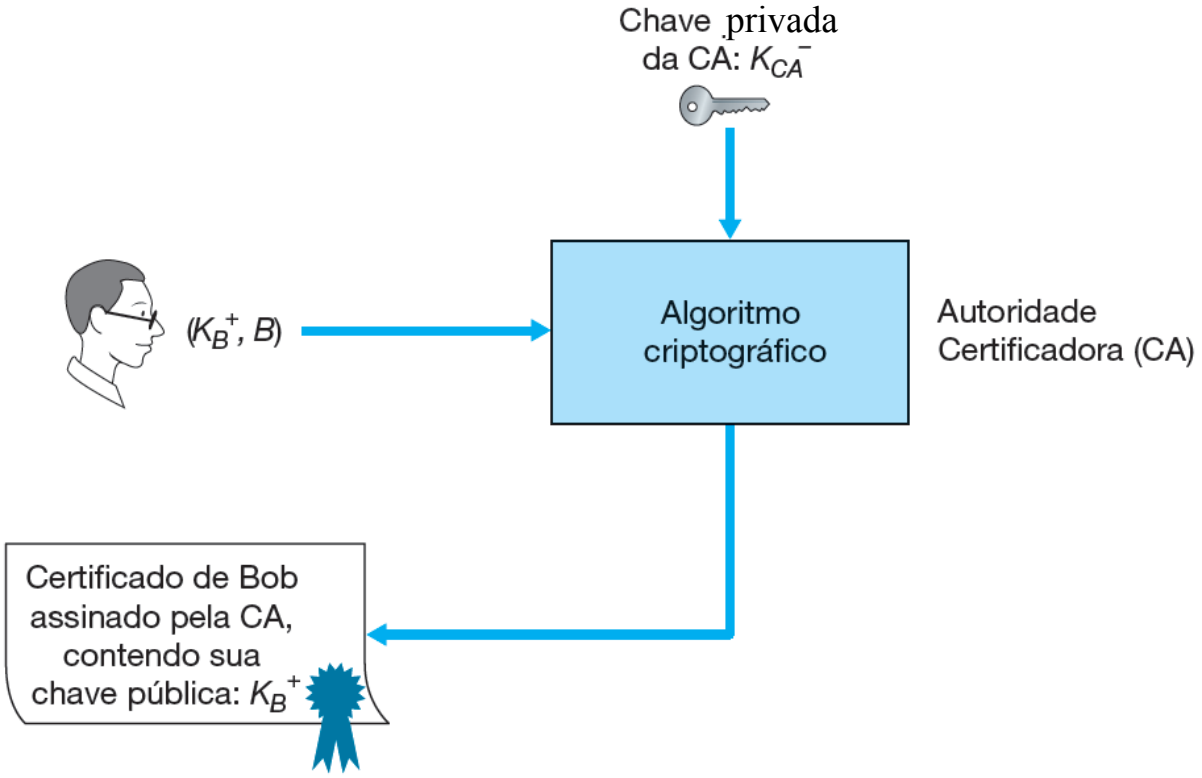
KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- Entidades (usuários, browsers, roteadores, etc) precisam ter certeza de que possuem a chave pública da entidade com a qual estão se comunicando.
  - A chave pública que supostamente é de Bob, é de fato dele?
- A vinculação de uma chave pública a uma entidade particular é feito por uma autoridade certificadora (*certification authority - CA*)
  1. Uma CA verifica se uma entidade é quem diz ser.
  2. Tão logo verifique a identidade da entidade, a CA cria um **certificado** que vincula a chave pública da entidade à identidade verificada. O certificado contém a chave pública e a informação exclusiva que identifica mundialmente o proprietário da chave pública (nome ou endereço IP).

Assinaturas digitais

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- Bob obtém sua chave pública certificada pela CA



Autenticação

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

- A autenticação é o processo de provar a identidade de uma entidade a outra entidade por uma rede de computadores.

- A autenticação precisa ser feita unicamente com base nas mensagens e dados trocados como parte de um **protocolo de autenticação**.

- O protocolo de autenticação primeiro estabelece as identidades das partes para a satisfação mútua; somente após a autenticação, as partes se lançam à tarefa que tem em mãos.

Autenticação

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição

1. Alice envia a mensagem "Eu sou Alice" para Bob.

2. Bob escolhe um **nonce** e o envia a Alice. O nonce será usado para ele se certificar de que Alice está ao vivo.

3. Alice usa sua chave privada K_A^- para criptografar o nonce e envia o valor resultante $K_A^-(R)$ a Bob.

4. Bob aplica a chave pública de Alice K_A^+ à mensagem recebida, ou seja, $K_A^+(K_A^-(R)) = R$. Bob autentica Alice.

Autenticação

KUROSE | ROSS
Redes de computadores e a internet
uma abordagem top-down
6ª edição