SSC0747
Engenharia de Segurança

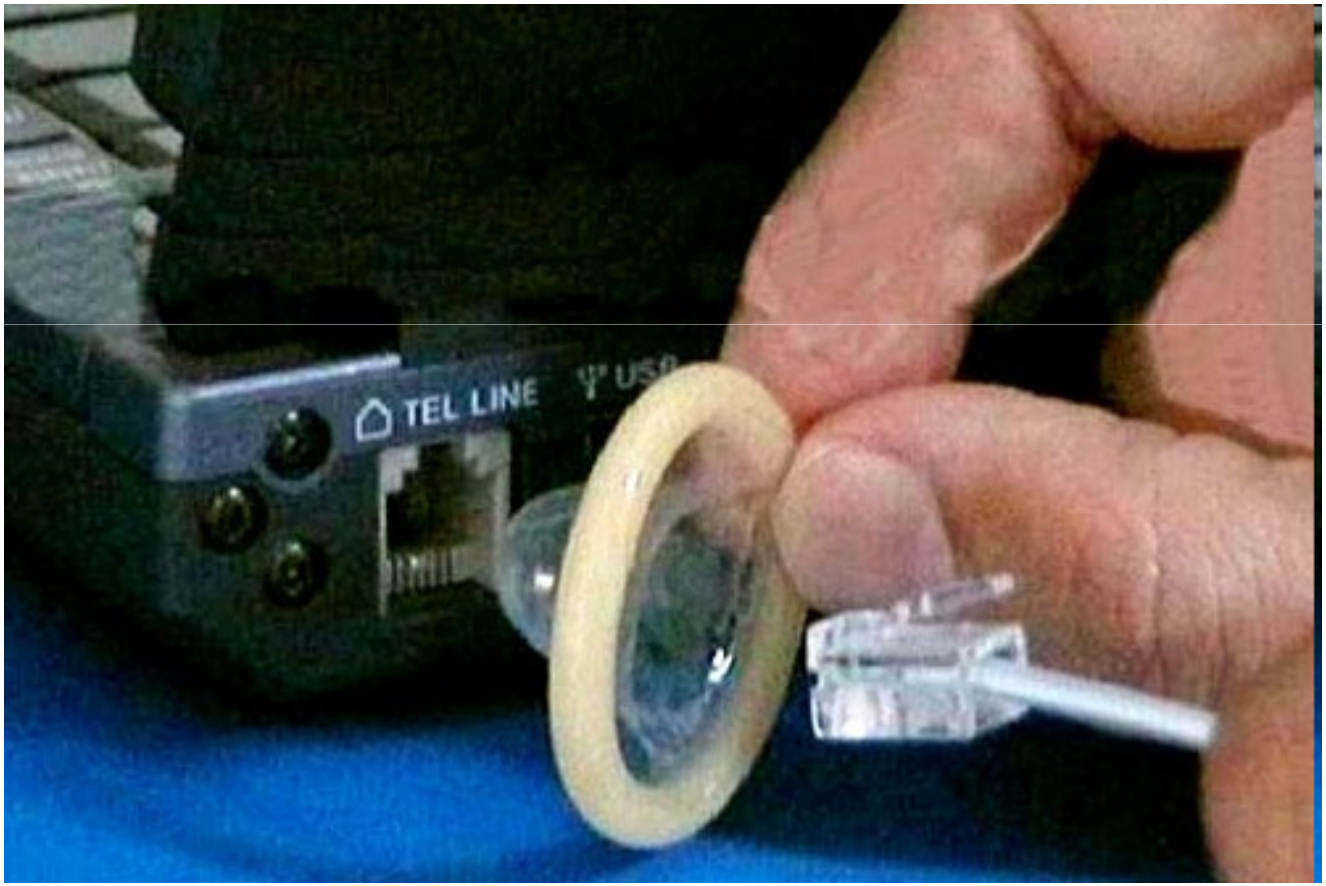
Edson Moreira
edson@icmc.usp.br

Diego Funçao
Diego.funcao@gmail.com

Fevereiro/2010

Engenharia de Segurança !

"Protegendo os Sistemas nos Pontos Certos"



Fonte http://noticias.uol.com.br/monkeynews/ultnot/2009/02/11/ult2529u454.jhtm

Objetivos

Apresentar os conceitos básicos em segurança computacional com ênfase nas tecnologias e em aspectos básicos de criptografia, controle de acesso e intrusão em redes de computadores.

Programa

Introdução; Cifras simétricas: DES, AES, avaliação; Criptografia de Chave Pública e Funções de Hash, RSA, Gerenciamento de Chaves; Algoritmos de Hash; Segurança em Redes: Sistemas de Autenticação; email; Segurança em IP; Segurança na Web; Sistemas de Detecção de Intrusão: Softwares de ataque; Configuração de Firewalls; Padrões nacionais e internacionais.

Texto básico: Tanenbaum e Kurose, cap. 8 (e suas referências)

Criptografia

- **Criptografia** (Do Grego *kryptós*, "escondido", e *gráphein*, "escrita") é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade.
- Nos dias atuais, onde grande parte dos dados é digital, sendo representados por bits, o processo de criptografia é basicamente feito por algoritmos que fazem o embaralhamento dos bits desses dados a partir de uma determinada chave ou par de chaves, dependendo do sistema criptográfico escolhido

Fonte: wikipedia

Avaliação

Provinhas todas as aulas (3.0 pontos) – grupos de 4 alunos

Projeto final (2.0 pontos) – grupos de 5 alunos

- um sistema de autenticação para redes wireless
- um sistema de transação segura para internet
- sistema de medição de vulnerabilidade de acesso
- módulos de proteção de fluxo de dados
- sistema de gerenciamento de chaves digitais
- etc

Provona (5.0 pontos) – 16/06

Segurança da Informação

- **Segurança da Informação** é a proteção de um conjunto de dados objetivando a manutenção do valor que possuem. Normalmente se define como básicas da segurança da informação os atributos de autenticidade, confidencialidade, integridade e disponibilidade.

Padrões

- Atualmente o conceito de Segurança da Informação está padronizado pela norma ISO/IEC 17799:2005, influenciada pelo padrão inglês BS 7799. A série de normas ISO/IEC 27000 foram reservadas para tratar de padrões de Segurança da Informação, incluindo a complementação ao trabalho original do padrão inglês. A ISO/IEC 27002:2005 continua sendo considerada formalmente como 17799:2005 para fins históricos.

Fonte: wikipedia

Segurança de Computadores

- **Segurança de computadores** é o esforço em implementar métodos e tecnologias para garantir que um computador ou rede de computadores será usado apenas, e devidamente, por pessoas autorizadas.

Fonte: wikipedia

- O conceito de segurança na área de informática surgiu ao longo do desenvolvimento dessa tecnologia e obteve maior atenção por parte dos administradores de sistemas quando as redes e principalmente a Internet foram desenvolvidas, já que era possível compartilhar quaisquer tipos de dados e informações para qualquer lugar do mundo, assim usuários domésticos e empresariais necessitavam de proteção contra os ataques de hackers e vírus. Com essa necessidade surgiram diversas empresas que desenvolvem as mais variadas soluções, desde o foro da criptografia a sistemas especializados.

Fonte: wikipedia

- O conceito de *Segurança Informática* ou *Segurança de Computadores* está intimamente relacionado com o de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si.

Fonte: wikipedia

Segurança em Redes

- **Network security** consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together.

Fonte: wikipedia

Engenharia de Segurança

- **Engenharia de Segurança** é um campo especializado de engenharia que trata com o desenvolvimento de planos e projetos detalhados para funcionalidades de segurança. Deve ser semelhante a outras atividades de engenharia em que sua principal motivação é o suporte à implementação de de soluções de engenharia que satisfazem requisitos funcionais e de usuários, mas com a dimensão adicional de prevenir mau-uso ou compportamentos maliciosos. Estas restrições e condições normalmente são definidas em Políticas de Segurança.

Na USP
Código de Ética da USP

Capítulo V - Registros de Dados e Informática

- Art. 33 - A coleta, a inserção e a conservação, em fichário ou registro, informatizado ou não, de dados pessoais relativos a opiniões políticas, filosóficas ou religiosas, origem, conduta sexual e filiação sindical ou partidária devem estar sob a égide da voluntariedade, da privacidade e da confidencialidade, podendo ser utilizados para os fins propostos para sua coleta.
  - §1º - É proibido usar os dados a que se refere o capítulo para discriminar ou estigmatizar o indivíduo, cuja dignidade humana deve ser sempre respeitada.
  - §2º - No caso de dados para fins de pesquisa, deve ser obedecido o disposto na Resolução 196/96 do Conselho Nacional de Saúde, atinente à ética na pesquisa envolvendo seres humanos.

Código de Ética da USP

- Art. 34 - Os membros da Universidade têm direito de acesso aos registros que lhes digam respeito.
- Art. 35 - O acesso e a utilização de informações relativas à vida acadêmica ou funcional de outrem, por qualquer membro da Universidade, dependem de:
  - I-expressa autorização do titular do direito;
  - II-ato administrativo motivado, em razão de objetivos acadêmicos ou funcionais, devidamente justificados
- Art. 36 - Os recursos computacionais da Universidade destinam-se exclusivamente ao desenvolvimento de suas atividades de ensino, pesquisa e extensão.

Código de Ética da USP

- Art. 37 - Arquivos computacionais são de uso privativo e confidencial de seu autor ou proprietário, sendo igualmente confidencial todo o tráfego na rede. Parágrafo único - Os administradores dos sistemas computacionais poderão ter acesso aos arquivos em casos de necessidade de manutenção ou falha de segurança.
- Art. 38 - No que concerne ao uso dos sistemas de computação compartilhados, é vedado aos membros da Universidade:
  - I-utilizar a identificação de outro usuário;
  - II-enviar mensagens sem identificação do remetente;
  - III-degradar o desempenho do sistema ou interferir no trabalho dos demais usuários;
  - IV-fazer uso de falhas de configuração, falhas de segurança ou conhecimento de senhas especiais para alterar o sistema computacional;
  - V-fazer uso de meio eletrônico para enviar mensagens ou sediar páginas ofensivas, preconceituosas ou caluniosas.

Política de Segurança da USP

Dispõe sobre os administradores e usuários dos sistemas computacionais da USP.

A Reitora da Universidade de São Paulo, usando de suas atribuições legais, tendo em vista o deliberado pelo Conselho Supervisor da Coordenadoria de Tecnologia da Informação, e considerando:

- a necessidade de manter a segurança dos dados armazenados em sistemas computacionais da USP, garantindo a sua integridade e só permitindo acesso a quem tenha direito a ele;
- a necessidade de identificar claramente os usuários dos sistemas computacionais da USP, particularmente os autores de atos que violem as regras estabelecidas para o uso desses sistemas e o Código de Ética da USP, em seus artigos 36 a 38, baixa a seguinte

- **PORTARIA:**

- **Artigo 1º** - Os administradores dos sistemas computacionais da USP devem zelar pela segurança dos sistemas e dos dados sob os seus cuidados.
- Parágrafo único - Entende-se por "administradores de sistemas computacionais" quaisquer pessoas dos quadros docente, discente e funcional que tenham conhecimento autorizado do código de acesso e senha do super usuário, root ou função equivalente dos computadores em que estejam instalados esses sistemas computacionais, sejam eles de uso geral, de uso restrito a uma Unidade, Departamento ou grupo de pessoas, ou ainda de uso individual.
- **Artigo 2º** - Em particular, os administradores de sistemas computacionais devem observar as seguintes normas:
- …..

Continua em.... http://leginf.uspnet.usp.br/port/pgr3662.htm

Política de Segurança na USPnet

http://www.security.usp.br/normas_pseg00.html

Este documento foi elaborado pela Comissão de Segurança da USPnet, criada com as seguintes atribuições:

- Assessorar a Comissão Central de Informática, o DI, os Centros de Informática da capital e do Interior no tratamento de questões de segurança;
- Elaborar uma Política de Segurança que dê sustentação às atividades de proteção da informação eletrônica da Universidade;
- Propor Planos de Segurança e de Contingência para os sistemas computacionais da Universidade, sempre que possível de acordo com a norma NB 17799;
- Acompanhar a implantação e execução dos planos propostos.

O documento aborda a segurança da Rede Computacional da Universidade de São Paulo - USPnet em seus diversos aspectos, apresentando recomendações e ações que devem ser seguidas de forma a preservar o patrimônio e a informação, no que se refere aos setores computacionais e de comunicação, e a reputação da Universidade de São Paulo.

- PSeg01 - Norma de Segurança da USPnet. Criado em 04/11/2002. Última revisão em 16/09/2004
- PSeg02 - Norma para Utilização de Recursos Computacionais. Criado em 04/11/2002. Última revisão em 16/09/2004
- PSeg03 - Norma para Uso de Correio Eletrônico. Criado em 08/11/2002. Última revisão em 16/09/2004
- PSeg04 - Norma para Computadores Pessoais.Criado em 11/11/2002. Última revisão em 16/09/2004
- PSeg05 - Norma para Uso das Salas de Usuários e Pró-Aluno Oferecidas pela Universidade. Criado em 08/11/2002. Última revisão em 16/09/2004
- PSeg06 - Norma de Uso de Serviços de Acesso Discado. Criado em 08/11/2002. Última revisão em 16/09/2004 Criado em 04/11/2002
- PSeg07 - Norma de Uso de Serviços SSH. Criado em 08/11/2002. Última revisão em 08/04/2003
- PSeg08 - Norma de Uso de Serviços Telnet. Criado em 08/11/2002. Última revisão em 08/04/2003
- PSeg09 - Norma de Uso de Serviços FTP. Criado em 08/11/2002. Última revisão em 08/04/2003
- ....

NORMAS PARA UTILIZAÇÃO DE COMPUTADORES E REDES DO ICMC

- A obtenção de uma conta eletrônica em qualquer computador do ICMC implica na aceitação e no respeito às regras de uso contidas neste documento. Como os computadores estão ligados em rede, a má utilização de algum deles, podeacarretar problemas sérios a todos usuários.
- 1. A conta eletrônica é pessoal, confidencial e intransferível. Sua senha não deve ser fornecida a ninguém e deve ser de difícil decodificação.
- 2. A utilização dos equipamentos computacionais do ICMC, através de um código de acesso, é permitida somente para atividades acadêmicas, de pesquisa e de extensão. Esses recursos necessitam de autorização especial para utilização em qualquer outra finalidade e não devem ser extensivamente usados para fins privativos.
- 3. A tentativa de acesso, ou o acesso a computadores não autorizados; a tentativa de quebra, ou a quebra de sigilo de senhas alheias; o acesso e modificação de arquivos pertencentes a outros usuários sem a sua autorização; são considerados delitos graves, puníveis com o cancelamento da conta eletrônica infratora em todos os computadores do ICMC e com a restrição de acesso físico aos laboratórios do ICMC, podendo até resultar emação legal.
- 4. O conteúdo das páginas pessoais no site do ICMC deve ser exclusivamente acadêmico. Qualquer assunto que não seja de caráter acadêmico poderá resultar em ação de responsabilidade administrativa, civil e/ou criminal.

- 5. Não é permitido desenvolver, manter, usar ou divulgar meios que possibilitem a violação de computadores da rede. O desrespeito a esta regra também será punido com a exclusão da conta eletrônica envolvida e impedimento de obtenção de novas contas eletrônicas pelo usuário em questão.
- 6. Toda documentação ou informação obtidas através da rede, que tenham propriedade registrada, não podem ser copiadas, modificadas, disseminadas ou usadas, no todo ou em parte, sem permissão expressa do detentor dos direitos autorais.

Continua em ... http://www.icmc.usp.br/~sti/forms/conta_verso.pdf

Ao nível do usuário...

Estou ciente das “Normas para Utilização de Computadores e Redes do ICMC”, das “Normas de uso dos laboratórios de Informática do ICMC-USP”, do “Código de Ética da USP”, e comprometo-me a respeitá-las assumindo as conseqüências administrativas, cíveis e penais decorrentes do desvio de finalidade e do desrespeito às normas de uso de contas. Comprometo-me, ainda, a aceitar eventuais alterações e regulamentações futuras, assim como comunicar meu desligamento da Universidade, a qualquer título, para a regularização da conta. Estou ciente também que os laboratórios do ICMC são monitorados por um circuito interno de câmeras.

Por ser verdade, firmo a presente.

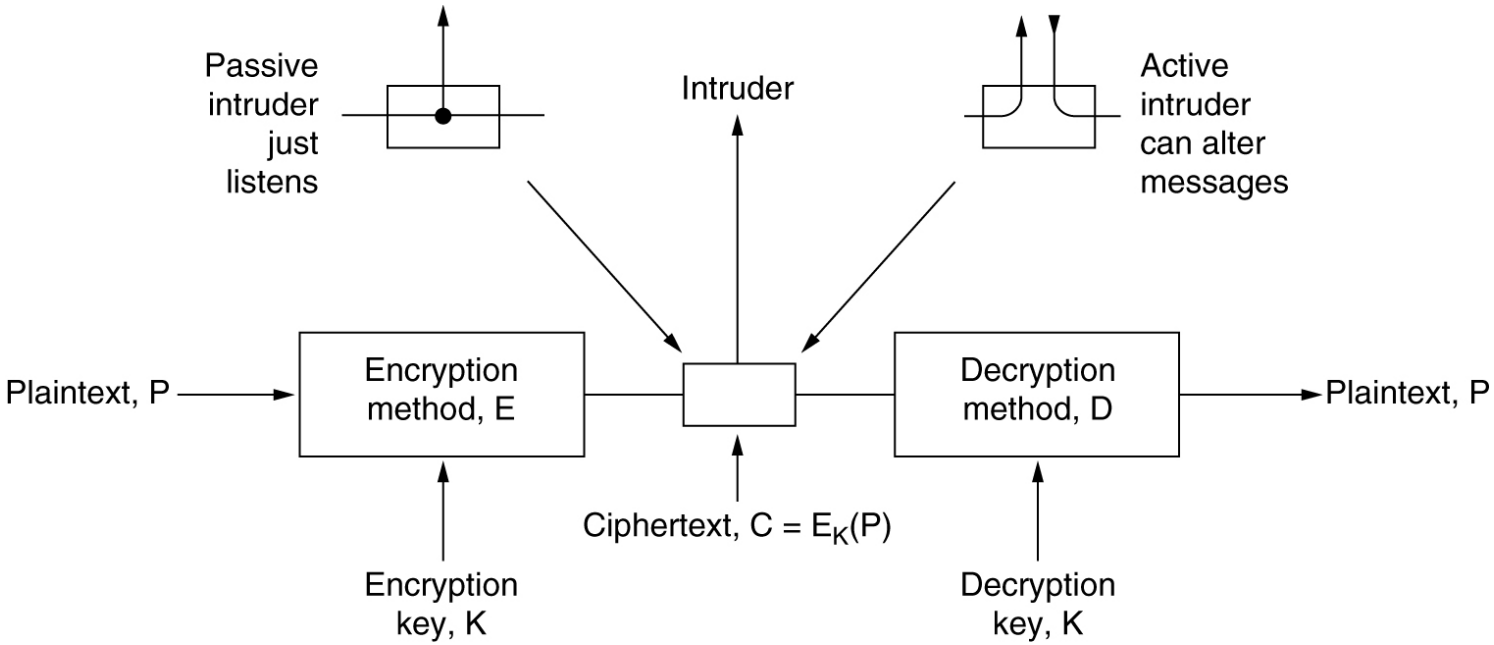
Cap. 8 - Segurança em redes de computadores

Objetivos do capítulo:

- Compreender princípios de segurança de redes:
  - Criptografia e seus *muitos* usos além da "confidencialidade"
  - Autenticação
  - Integridade de mensagem
  - Distribuição de chave

- Segurança na pilha Internet:
  - Firewalls
  - Segurança nas camadas de aplicação, transporte, rede e enlace

Modelo

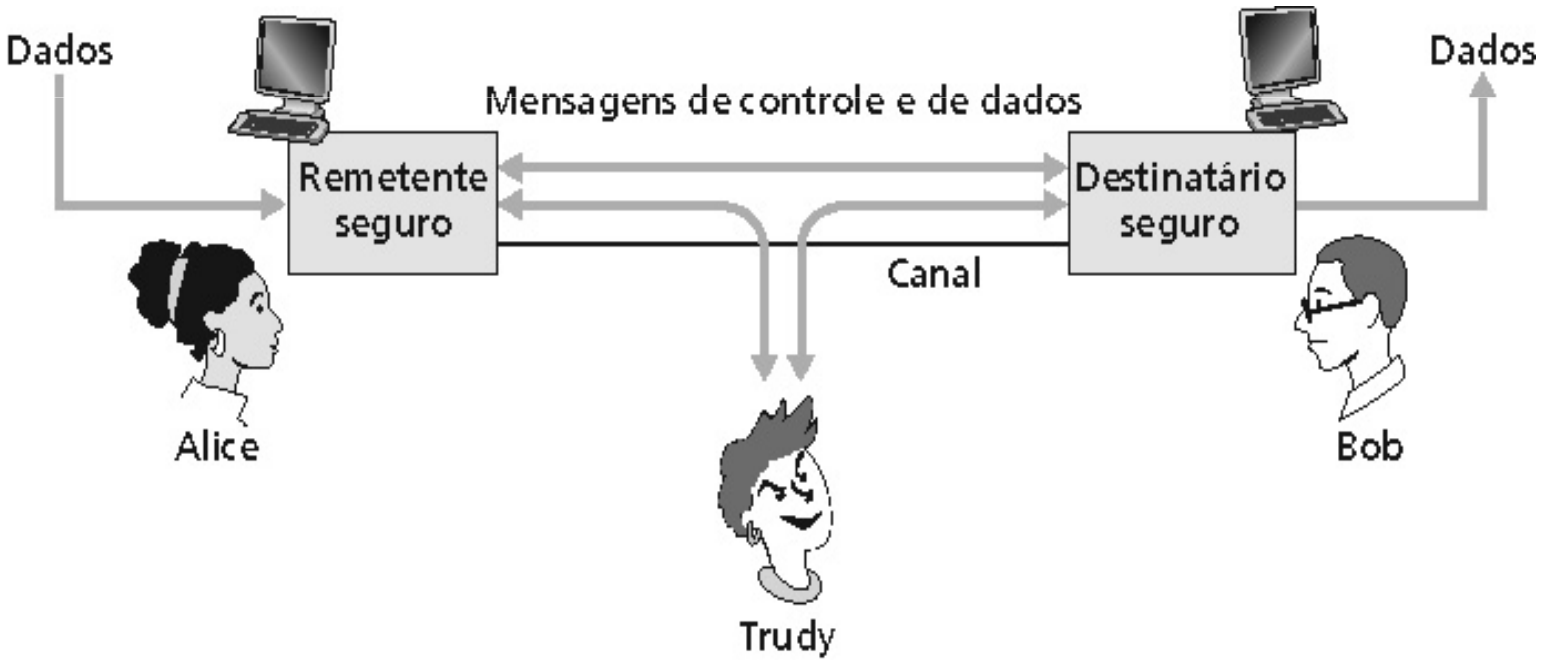

Passive intruder just listens
Intruder
Active intruder can alter messages
Plaintext, P
Encryption method, E
Decryption method, D
Plaintext, P
Encryption key, K
Ciphertext, C = E_K(P)
Decryption key, K

Provinha 1 – 24.02.2010

- Explique os 4 principais parâmetros de segurança. Para cada um deles, explique como pode interferir no desempenho de aplicações em rede
- A Política de Segurança da USP trata como os parâmetros devem ser implementados?

Vamos Tratar de Comunicação Segura !

- Bob e Alice (amantes!) querem se comunicar “seguramente”
- Bem conhecidos no mundo da segurança de redes
- Trudy, a “intrusa” pode interceptar, apagar, modificar mensagens



Segurança em redes de computadores

- 8.1 O que é segurança?
- 8.2 Princípios da criptografia
- 8.3 Autenticação
- 8.4 Integridade
- 8.5 Distribuição de chaves e certificação
- 8.6 Controle de acesso: firewalls
- 8.7 Ataques e medidas de defesa
- 8.8 Segurança em muitas camadas

O que é segurança de rede?

Confidencialidade: apenas o transmissor e o receptor pretendido deveriam "entender" o conteúdo da mensagem

- Transmissor criptografa mensagem
- Receptor decodifica a mensagem

Autenticidade: transmissor e receptor querem confirmar a identidade um do outro

Integridade e não repudiação 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

Quem poderiam ser Bob e Alice?

- Browser/servidor Web para transações eletrônicas (ex.: compras on-line)
- Cliente/servidor de banco on-line
- Servidores DNS
- Roteadores trocando atualizações de tabela de roteamento

Existem pessoas más por aí!

P.: O que uma “pessoa má” pode fazer?

R.: Muito!

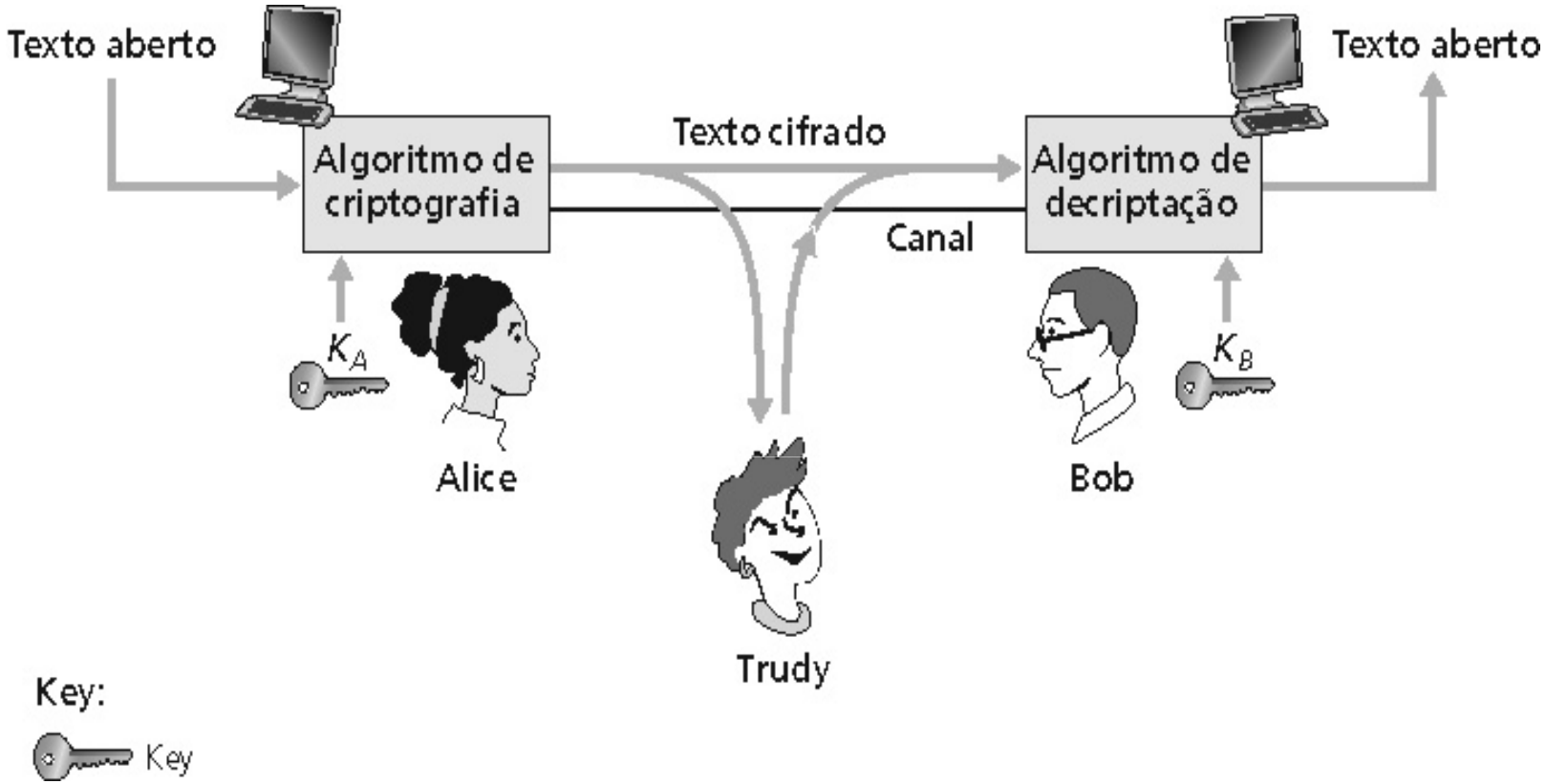
- *Interceptação* de mensagens
- *Inserção* ativa de mensagens na conexão
- *Personificação:* falsificar (spoof) endereço de origem no pacote (ou qualquer campo no pacote)
- *Hijacking:* assume a conexão removendo o transmissor ou receptor e se inserindo no lugar
- *Negação de serviço:* impede que um serviço seja usado pelos outros (ex.: por sobrecarga de recursos)

Veremos mais sobre isso depois...

Segurança em redes de computadores

- 8.1 O que é segurança?
- 8.2 Princípios da criptografia (confidencialidade, privacidade)
  - Somente o remetente e o destinatário devem entender o conteúdo da mensagem transmitida
- 8.3 Autenticação
- 8.4 Integridade
- 8.5 Distribuição de chaves e certificação
- 8.6 Controle de acesso: firewalls
- 8.7 Ataques e medidas de defesa
- 8.8 Segurança em muitas camadas

A linguagem da criptografia



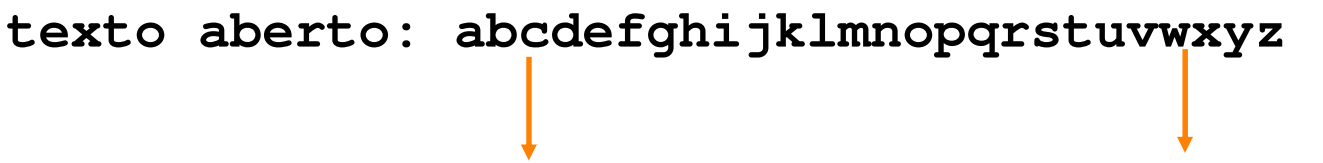
Chave simétrica de criptografia: as chaves do transmissor e do receptor são idênticas

Chave pública de criptografia: criptografa com chave pública, decriptografa com chave secreta (privada)

Criptografia de chave simétrica

Código de substituição: substituindo uma coisa por outra

- Código monoalfabético: substituir uma letra por outra



Ex.:

```
texto aberto: bob. i love you. alice
texto cifrado: nkn. s gktc wky. mgsbc
```

Criptografia de chave simétrica (cont.)

Criptografia de chave simétrica: Bob e Alice compartilham a mesma chave (simétrica) conhecida: K

•Ex.: sabe que a chave corresponde ao padrão de substituição num código substituição monoalfabético

• P.: Como Bob e Alice combinam o tamanho da chave?

DES: criptografia com chave simétrica

DES: Data encryption standard

- Padrão de criptografia dos Estados Unidos [NIST 1993]
- Chave simétrica de 56 bits, 64 bits de texto aberto na entrada
- Quão seguro é o padrão DES?
  - DES Challenge: uma frase criptografada com chave de 56 bits (“strong cryptography makes the world a safer place”) foi decodificada pelo método da força bruta em 4 meses
- Tornando o DES mais seguro
  - Use três chaves em seqüência (3-DES) sobre cada dado
  - Use encadeamento de blocos de códigos

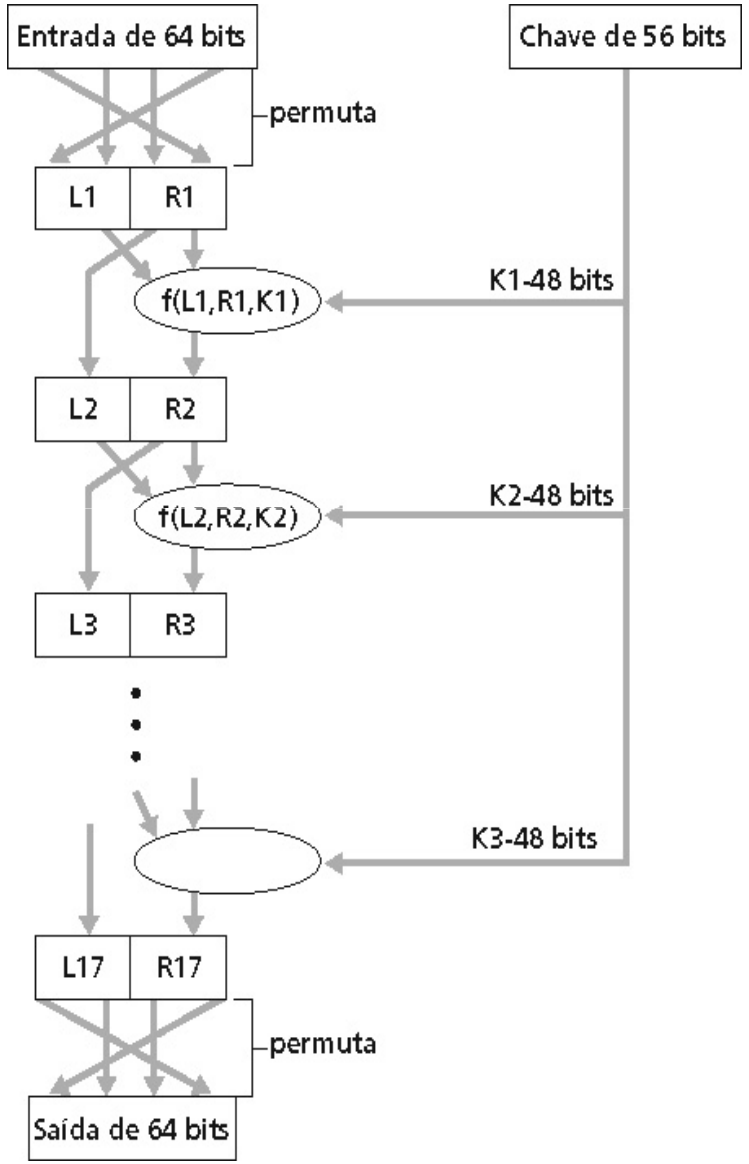
Criptografia de chave simétrica: DES

Operação do DES

Permutação inicial

16 rodadas idênticas de função de substituição, cada uma usando uma diferente chave de 48 bits

Permutação final



Padrão avançado de criptografia

- Novo (nov/2001) padrão do NIST para chaves simétricas, substituindo o DES
- Processa dados em blocos de 128 bits
- Chaves de 128, 192, ou 256 bits
- Decodificação por força bruta (tentar cada chave) leva 1 segundo no DES e 149 trilhões de anos no AES

Criptografia de chave pública

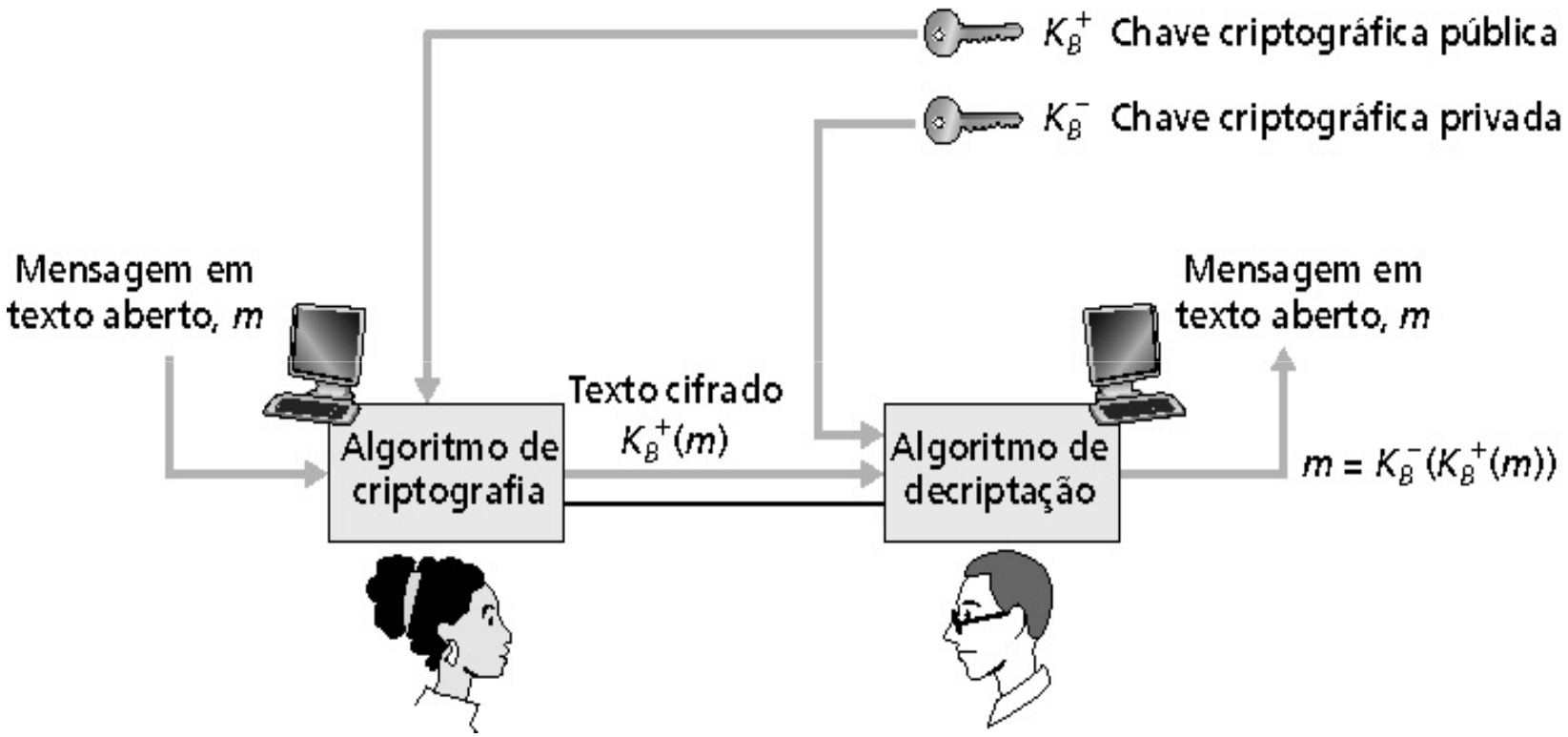
Chave simétrica

- 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.)



Algoritmos de criptografia com chave pública

Duas exigências correlatas:

1. necessita d_B ( ) e e_B ( ) tal que
   $d_B (e_B (m)) = m$

2. necessita chaves pública e privada para d_B ( ) e e_B ( )

RSA: Algoritmo de Rivest, Shamir, Adelson

RSA: Escolhendo as chaves

1. Encontre dois números primos grandes *p*, *q*.
   (ex.: 1.024 bits cada um)

2. Calcule *n* = *pq*, *z* = *(p − 1)(q − 1)*.

3. Escolha *e (com e < n)* que não tenha fatores primos em comum com z. (*e*, *z* são “primos entre si”).

4. Escolha *d* tal que *ed − 1* seja exatamente divisível por *z*.
   (em outras palavras: *ed* mod *z* = *1*).

5. Chave *pública* é *(n,e)*. Chave *privada* é *(n,d)*.

K_B^+ K_B^-

RSA: Criptografia e decriptografia

0. Dado (n,e) e (n,d) como calculados antes.

1. Para criptografar o padrão de bits, m, calcule

$c = m^e \bmod n$ (i.e., resto quando m^e é dividido por n).

2. Para decriptografar o padrão de bits recebidos, c, calcule

$m = c^d \bmod n$ (i.e., resto quando c^d é dividido por n).

Mágica acontece!

$$m = (\underbrace{m^e \bmod n}_{c})^d \bmod n$$

RSA exemplo:

Bob escolhe $p = 5$, $q = 7$. Então $n = 35$, $z = 24$.

$e = 5$ (assim e, z são primos entre si).
$d = 29$ (assim $ed - 1$ é exatamente divisível por z).

criptografia:

letra	m	m^e	$c = m^e \bmod n$
l	12	1524832	17

decriptografia:

c	c^d	$m = c^d \bmod n$	letra
17	481968572106750915091411825223072000	12	l

A propriedade a seguir será *muito* útil mais tarde:

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

usa chave pública primeiro, seguida pela chave privada

usa chave privada primeiro, seguida pela chave pública

O resultado é o mesmo!

Segurança em redes de computadores

- 8.1 O que é segurança?
- 8.2 Princípios da criptografia
- 8.3 Autenticação
  - O remetente e o destinatário precisam confirmar a identidade da outra parte
- 8.4 Integridade
- 8.5 Distribuição de chaves e certificação
- 8.6 Controle de acesso: firewalls
- 8.7 Ataques e medidas de defesa
- 8.8 Segurança em muitas camadas

Autenticação

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

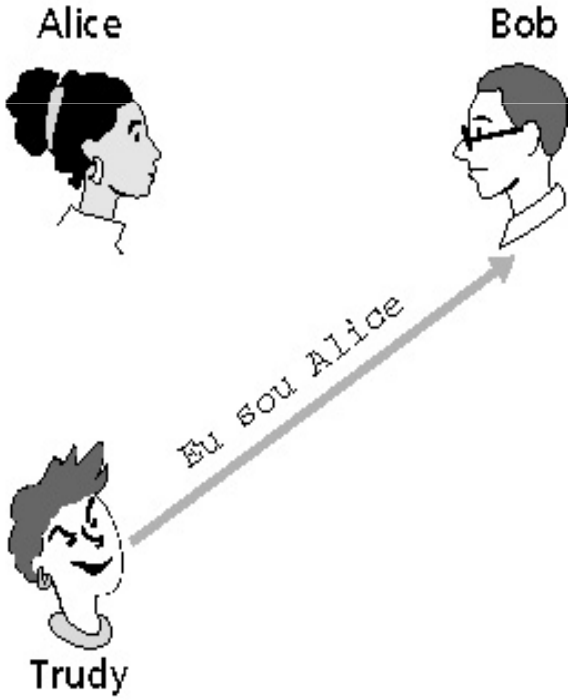
Protocolo ap1.0: Alice diz “Eu sou Alice”.

Cenário de falha??

Autenticação

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.)

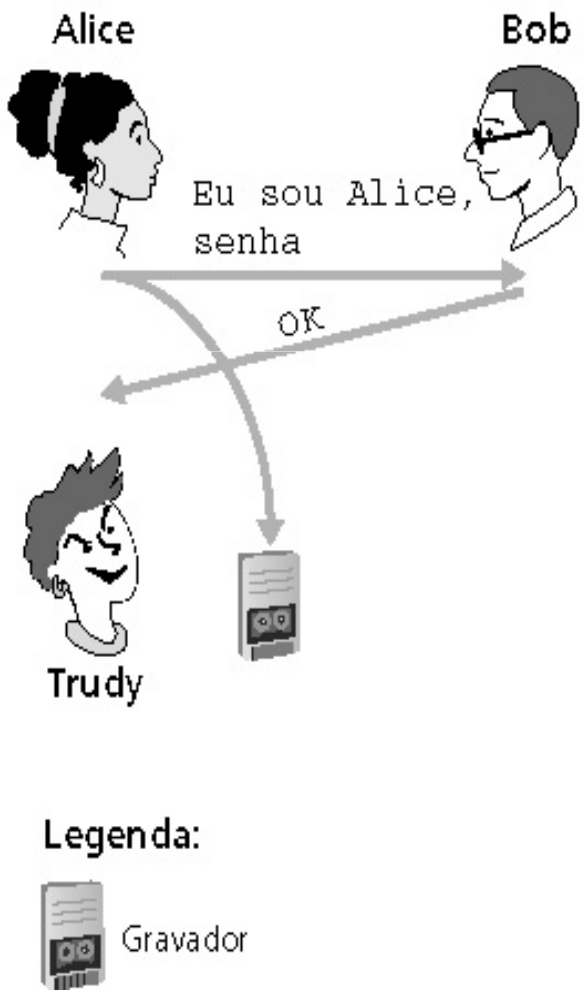
Protocolo ap2.0: Alice diz “Eu sou Alice” num pacote IP contendo seu endereço IP de origem.

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

Autenticação: outra tentativa (cont.)

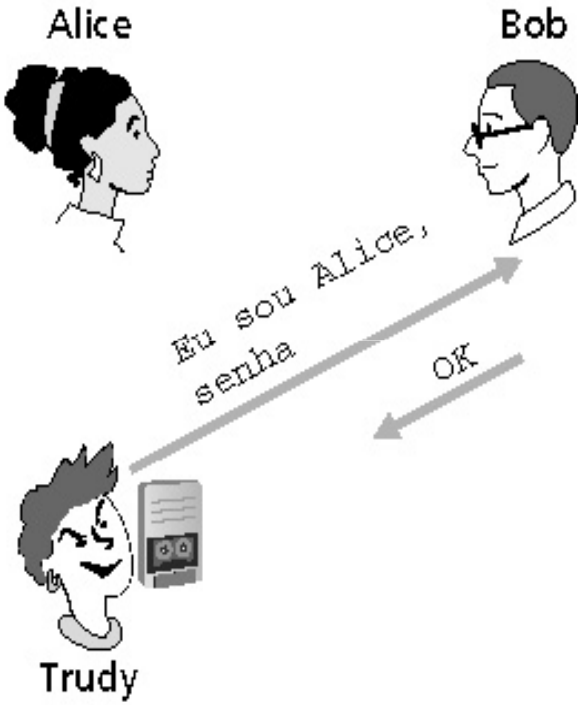
Protocolo ap3.0: Alice diz “Eu sou Alice” e envia sua senha secreta como prova.

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.

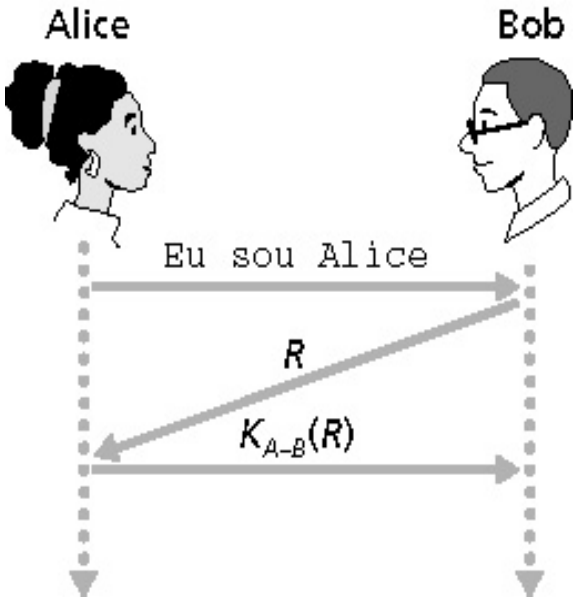
Autenticação: mais uma tentativa (cont.)

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.



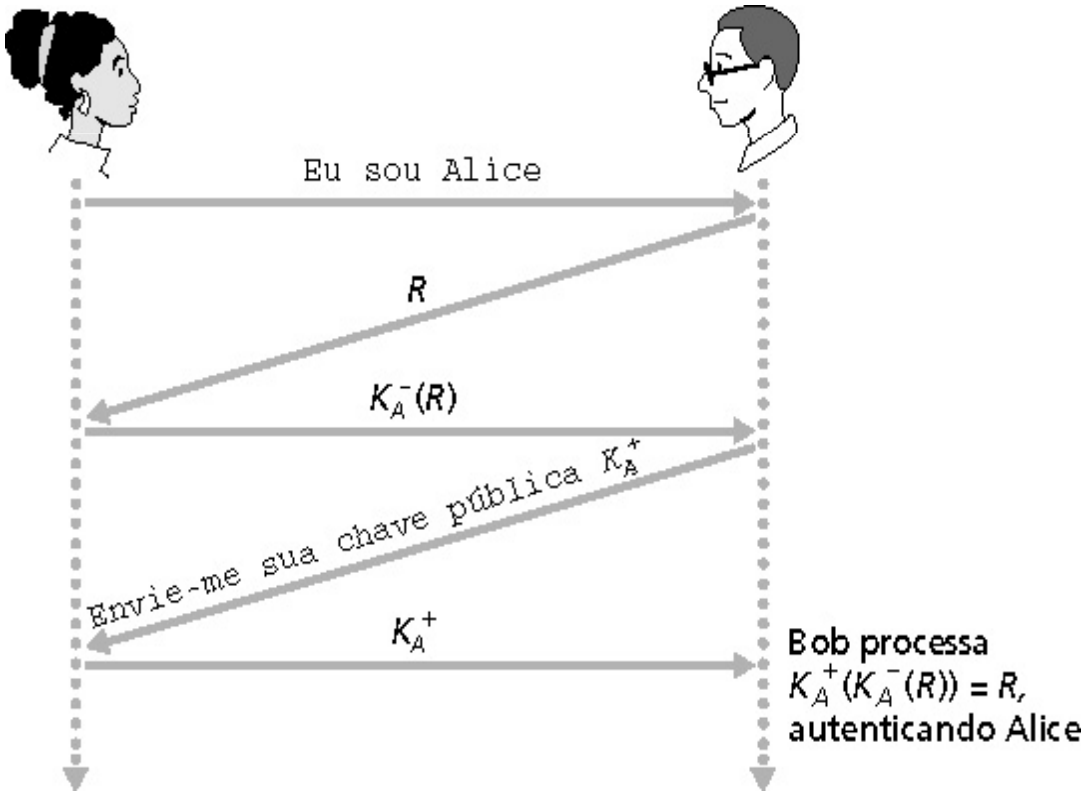
Alice está ao vivo, e apenas Alice conhece a chave para criptografar o nonce, então ela deve ser Alice!

Autenticação

ap4.0 exige chave secreta compartilhada.

- É possível autenticar usando técnicas de chave pública?

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



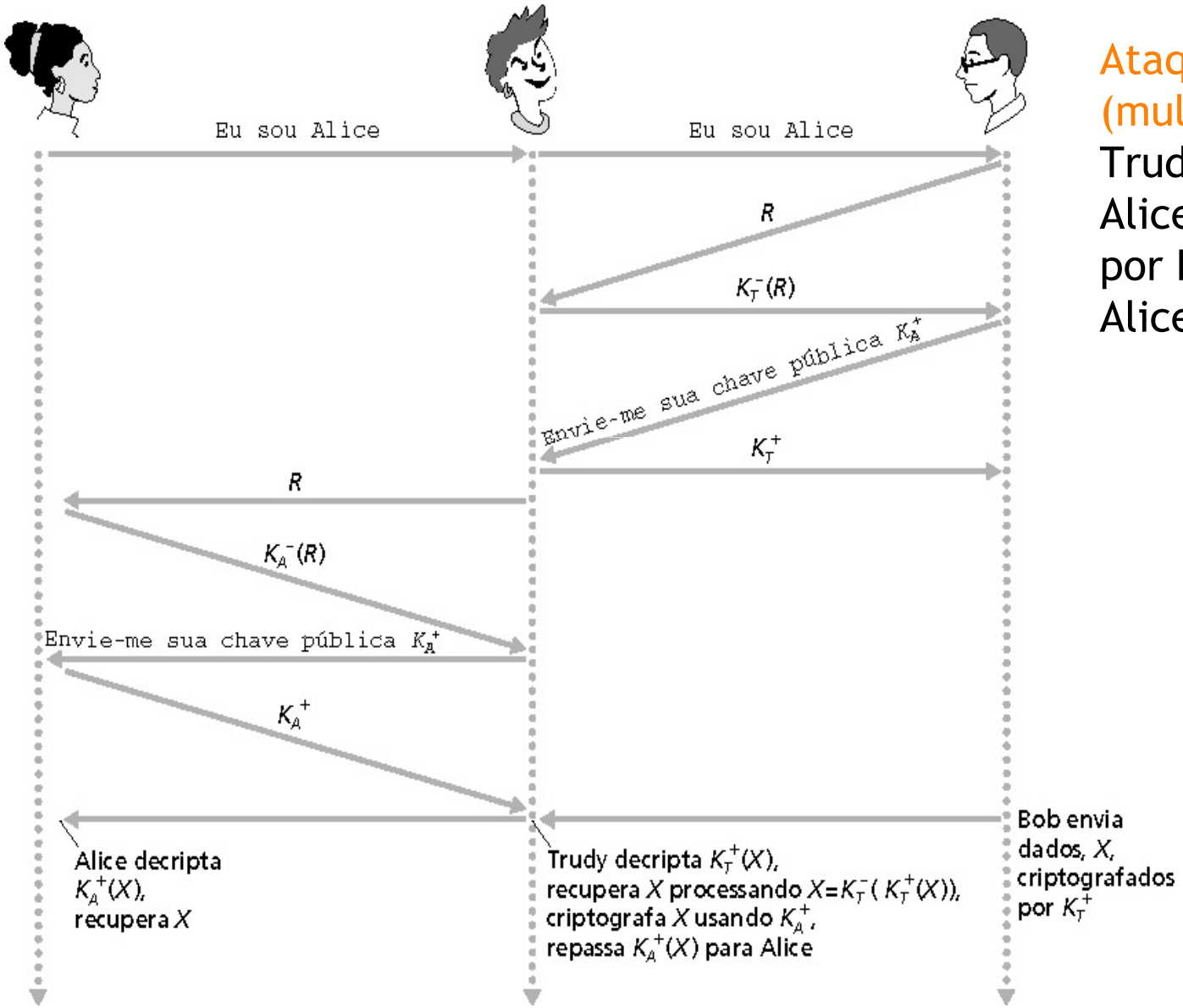
Bob calcula

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

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:

- Bob recebe tudo o que Alice envia e vice-versa. (Ex.: então Bob/Alice podem se encontrar uma semana depois e recordar a conversação.)

- O problema é que Trudy recebe todas as mensagens também!

Segurança em redes de computadores

- 8.1 O que é segurança?
- 8.2 Princípios da criptografia
- 8.3 Autenticação
- 8.4 Integridade
- 8.5 Distribuição de chaves e certificação
- 8.6 Controle de acesso: firewalls
- 8.7 Ataques e medidas de defesa
- 8.8 Segurança em muitas camadas

Segurança em redes de computadores

- 8.1 O que é segurança?
- 8.2 Princípios da criptografia
- 8.3 Autenticação
- 8.4 Integridade e não repudiação
  - assegura que o conteúdo da comunicação não foi alterado
  - como um receptor pode provar que a mensagem deve ter vindo de um remetente especifico (assinatura digital)
- 8.5 Distribuição de chaves e certificação
- 8.6 Controle de acesso: firewalls
- 8.7 Ataques e medidas de defesa
- 8.8 Segurança em muitas camadas

Assinaturas digitais

Quer-se indicar claramente o dono ou criador de um documento ou deixar claro que alguém concorda com o conteúdo de um documento.

Assinaturas digitais

Técnica criptográfica análoga às assinaturas manuais

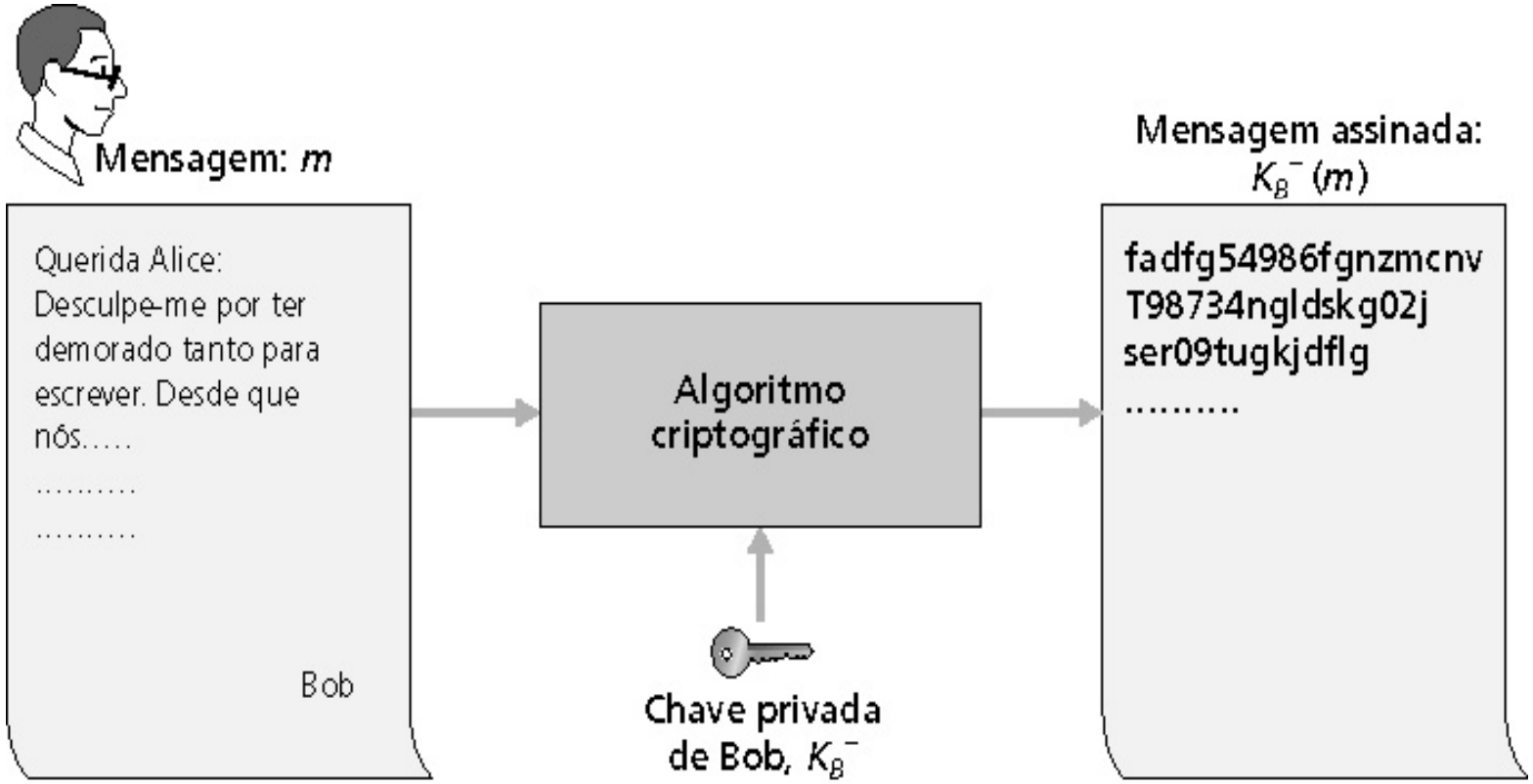
Transmissor (Bob) assina digitalmente um documento, estabelecendo que ele é o autor/criador

- Verificável - deve ser possível provar que um documento assinado por um indivíduo foi na verdade assinado por ele
- não forjável - somente aquele indivíduo poderia ter assinado o documento
- incontestável - o signatário não pode mais tarde repudiar o documento

Assinaturas digitais (cont.)

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

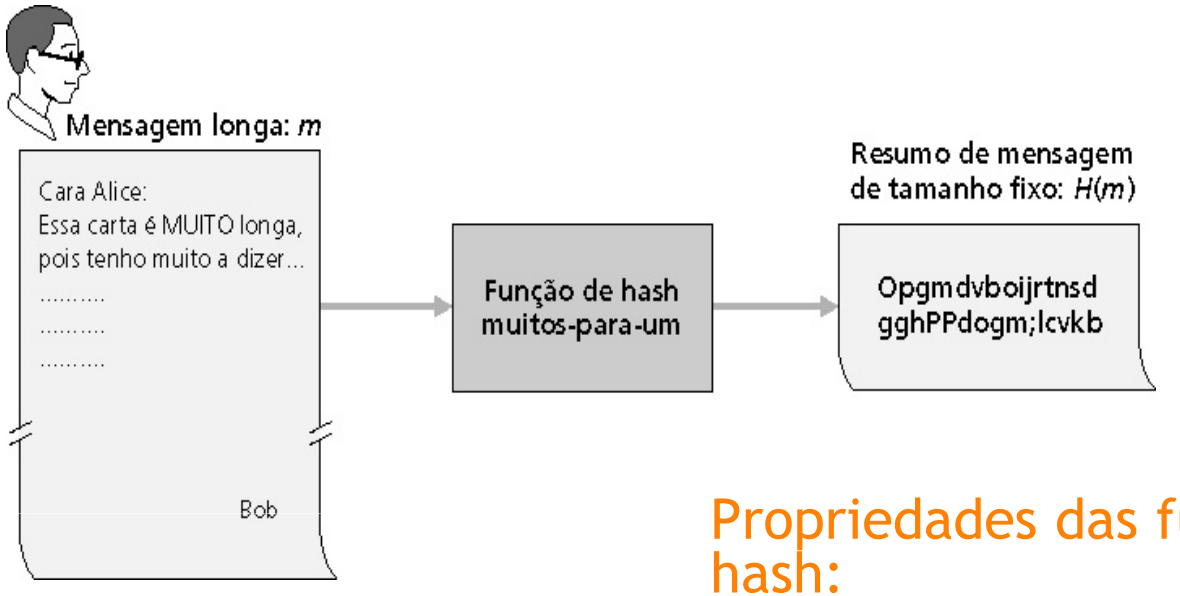
Alice verifica então que:

- Bob assinou *m;*
- ninguém mais assinou *m;*
- Bob assinou m e não *m'*.

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 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)*

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 x = H(m)

Figura 8.1 7 VerificacCo da integridade de uma mensagem assinada

Verificação da Internet (checksum) possui algumas propriedades de função de hash:

- Produz resumo de tamanho fixo (soma de 16 bits) de mensagem
- É muitos-para-um

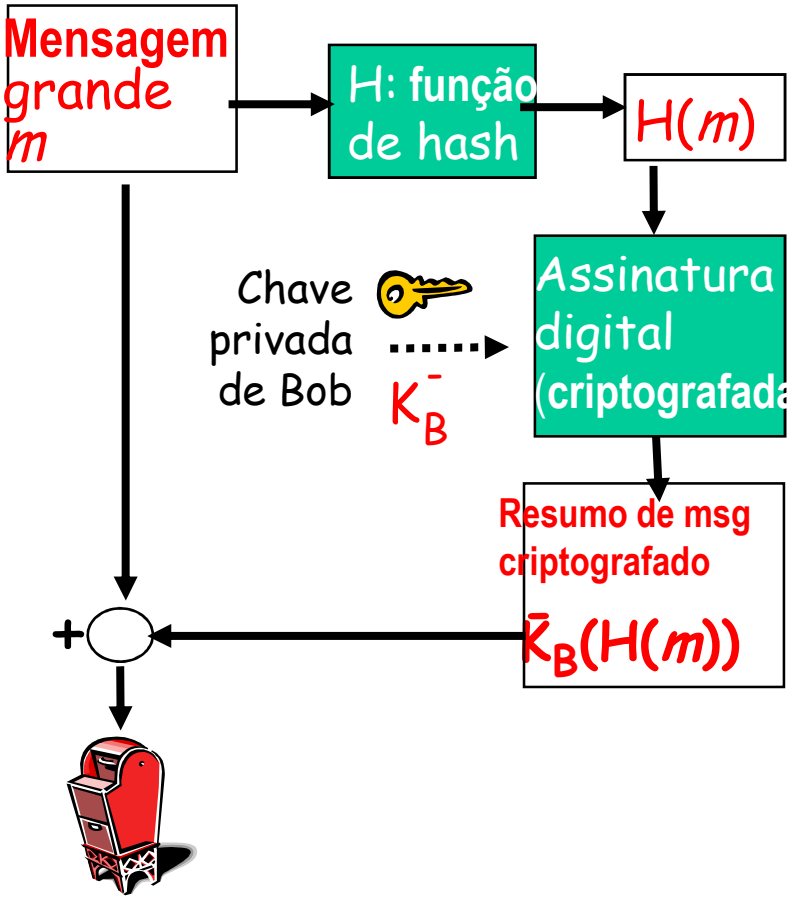
Mas dada uma mensagem com um dado valor de hash, é fácil encontrar outra mensagem com o mesmo valor de hash:

mensagem	formato ASCII
I O U 1	49 4F 55 31
0 0 . 9	30 30 2E 39
9 B O B	39 42 D2 42
	B2 C1 D2 AC

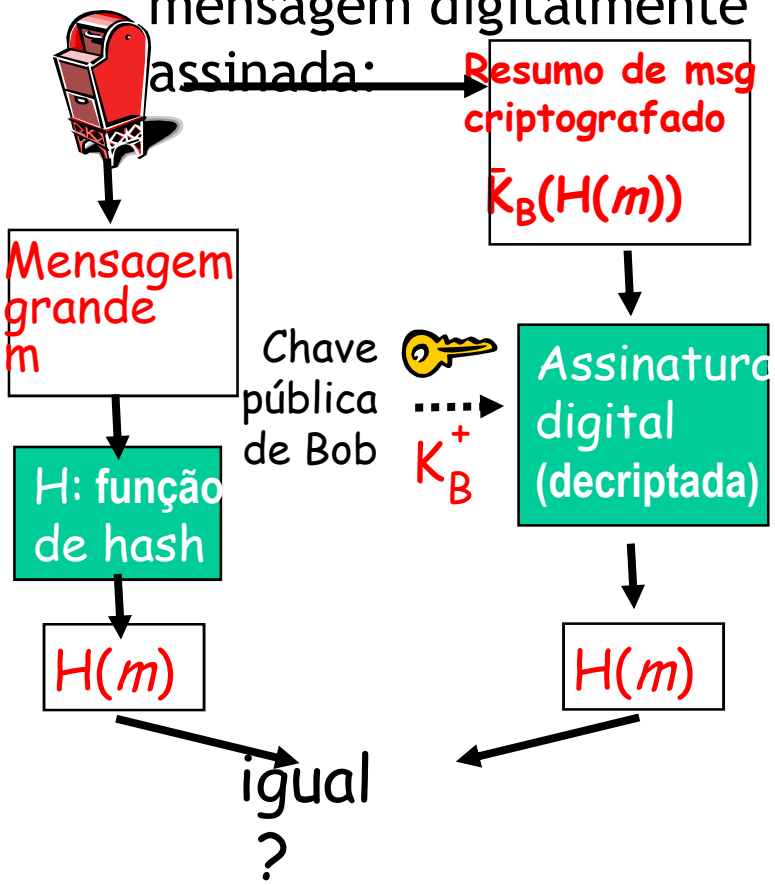
mensagem	formato ASCII
I O U 9	49 4F 55 39
0 0 . 1	30 30 2E 31
9 B O B	39 42 D2 42
	B2 C1 D2 AC

mensagens diferente
mas resumos idênticos!

Bob envia mensagem digitalmente assinada:



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



- MD5 é a função de hash mais usada (RFC 1321)
  - Calcula resumo de 128 bits da mensagem num processo de 4 etapas

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

- 8.1 O que é segurança?
- 8.2 Princípios da criptografia
- 8.3 Autenticação
- 8.4 Integridade
- 8.5 Distribuição de chaves e certificação
- 8.6 Controle de acesso: firewalls
- 8.7 Ataques e medidas de defesa
- 8.8 Segurança em muitas camadas

Problema da chave simétrica:

- Como duas entidades estabelecem um segredo mútuo sobre a rede?

Solução:

- Centro de distribuição de chaves confiável (KDC) atuando como intermediário entre entidades

Problema da chave pública:

- Quando Alice obtém a chave pública de Bob (de um site Web, e-mail, disquete), como ela sabe que é a chave pública de Bob e não de Trudy?

Solução:

- Autoridade de certificação confiável (CA)

- 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, $K_{A\text{-}KDC}$ $K_{B\text{-}KDC}$, para comunicação com o KDC

P.: Como o KDC permite que Bob e Alice determinem uma chave simétrica comum para se comunicarem entre si?

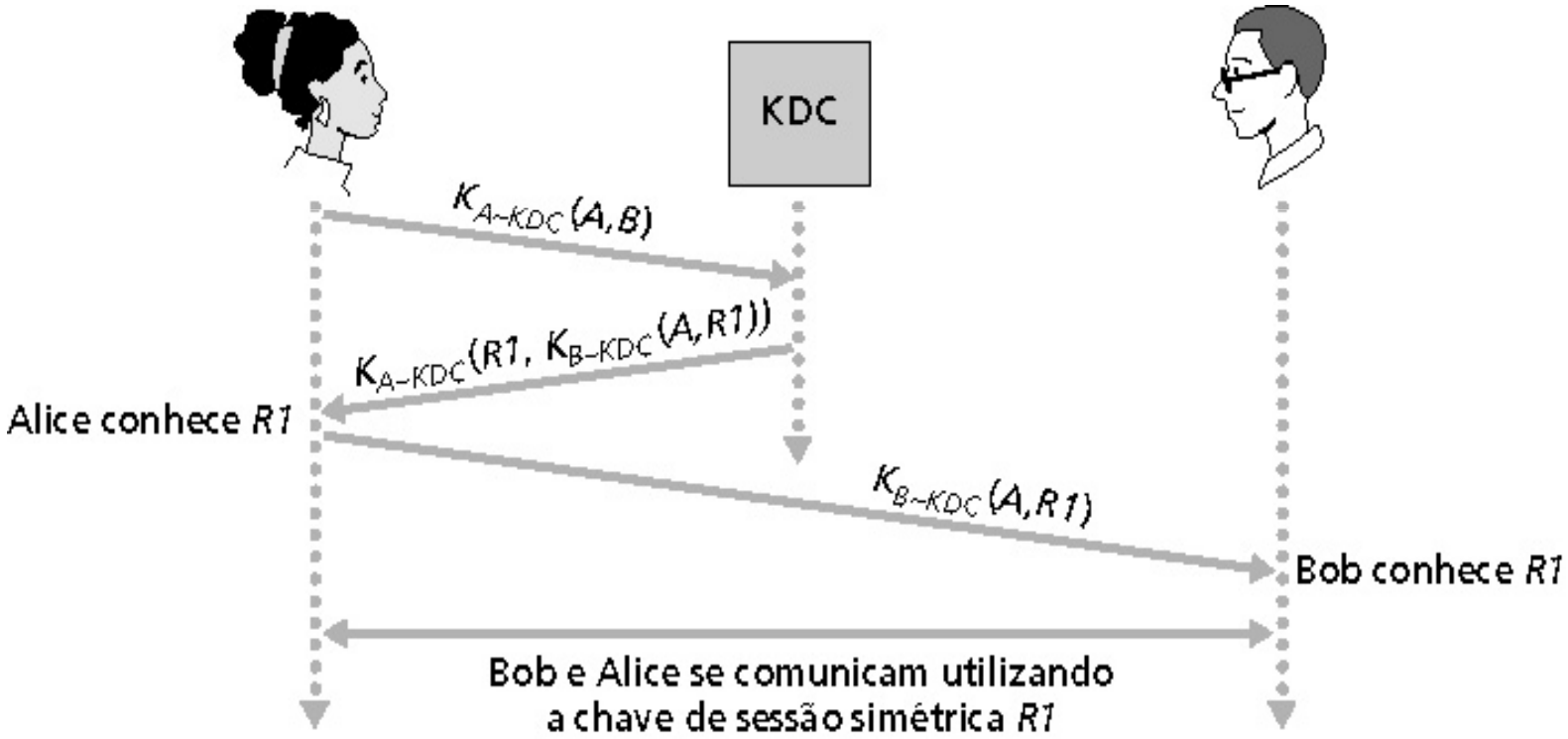
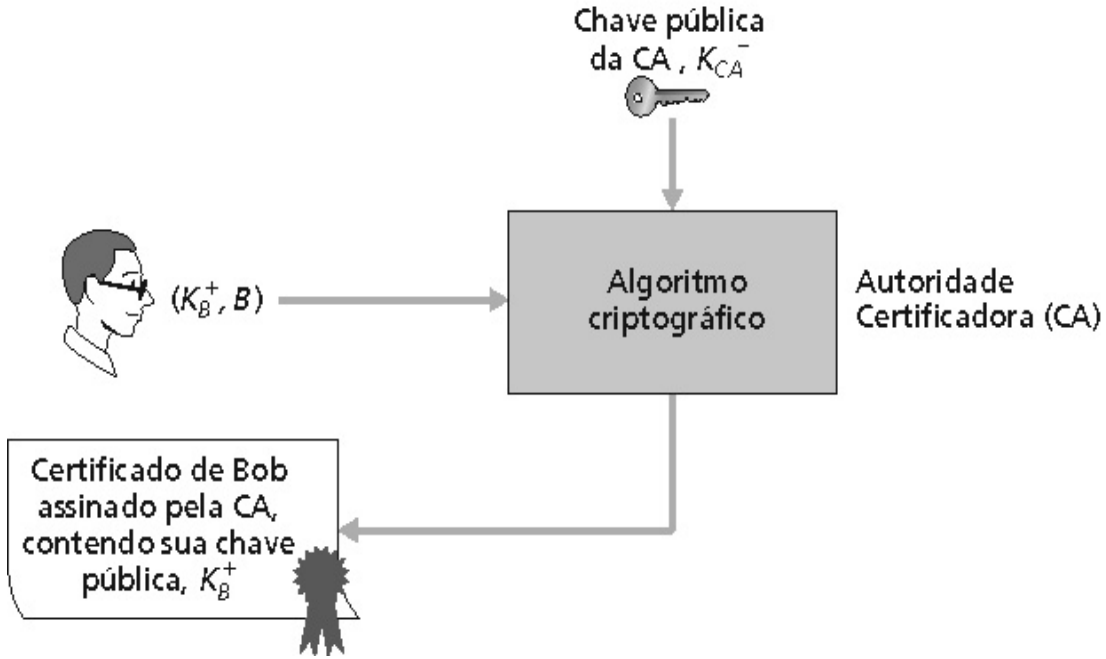


Figura 8.20 Trudy se passa par Bob usando criptografia de chaves publitas

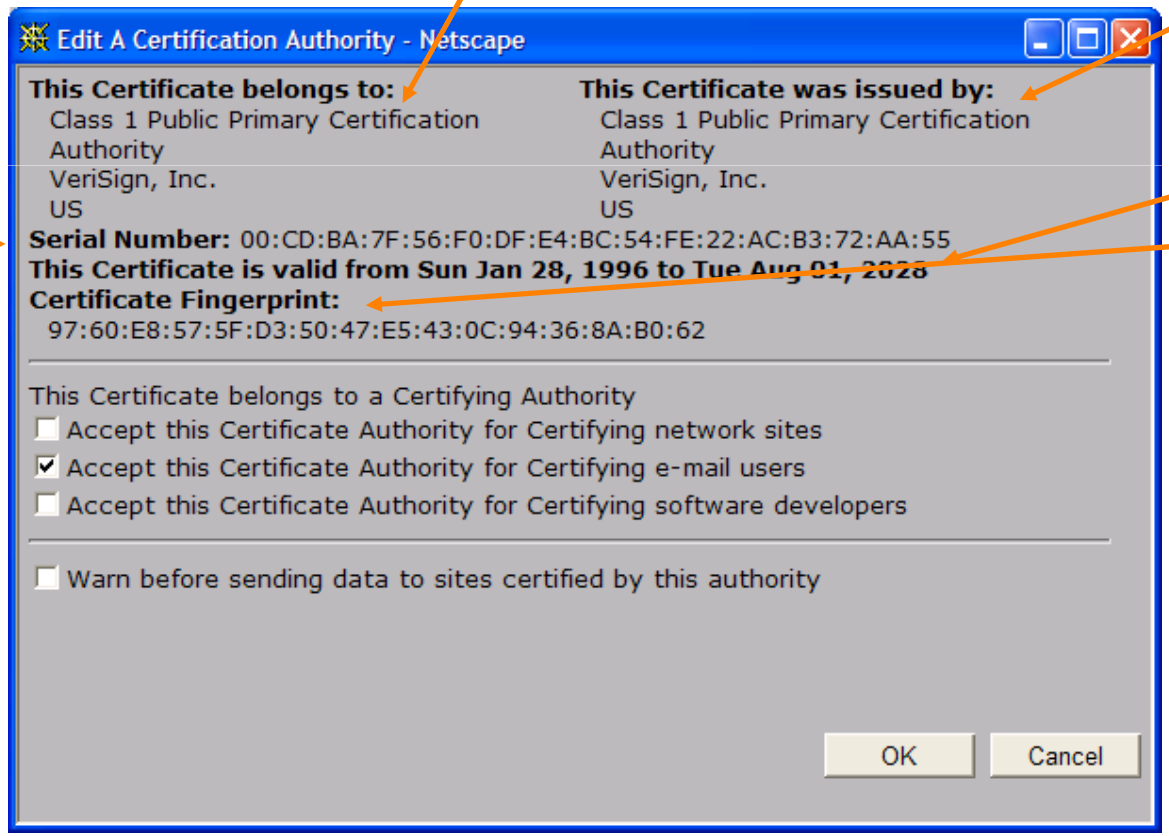
Autoridade certificadora (CA): associa uma chave pública a uma entidade em particular, E

- 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"



- Quando Alice quer a chave pública de Bob:
- Obtém o certificado de Bob (de Bob ou em outro lugar)
- Aplica a chave pública da CA ao certificado de Bob, obtém a chave pública de Bob

- Número serial (único para o emissor)
- Informação sobre o dono do certificado, incluindo o algoritmo e o valor da própria chave (não mostrada)

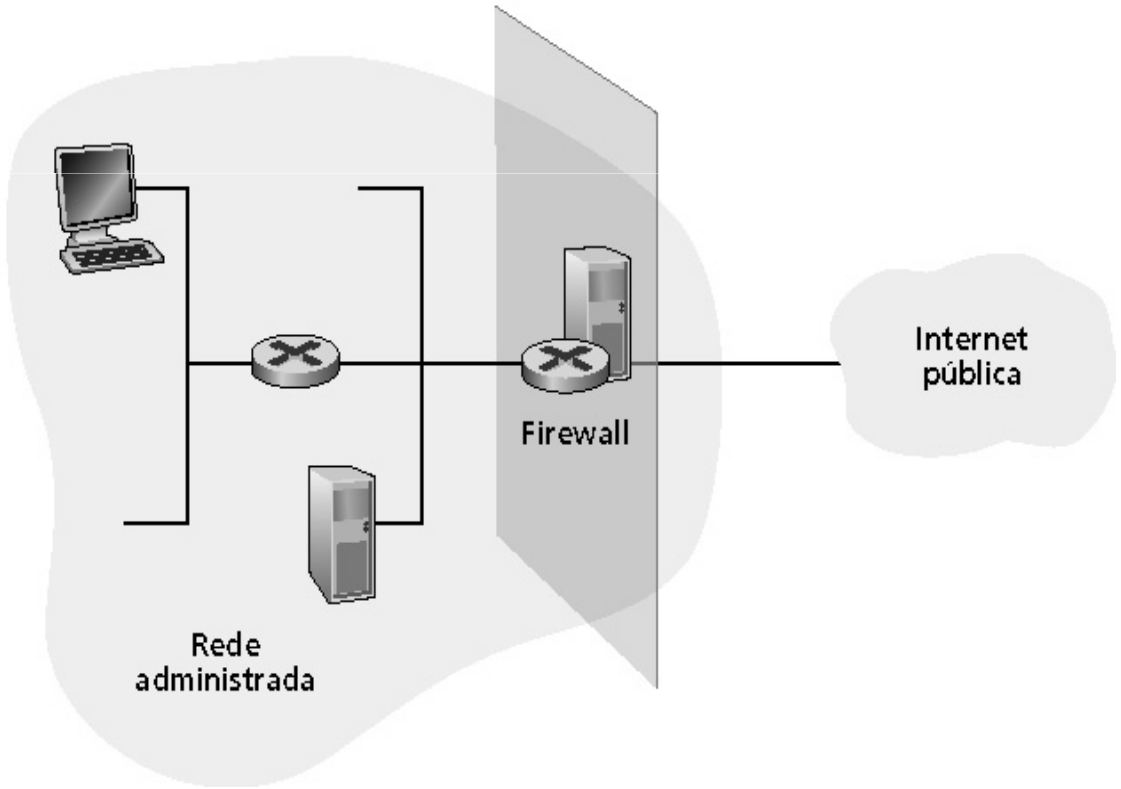


- Informação sobre o emissor do certificado
- Data de validade
- Assinatura digital do emissor

- 8.1 O que é segurança?
- 8.2 Princípios da criptografia
- 8.3 Autenticação
- 8.4 Integridade
- 8.5 Distribuição de chaves e certificação
- 8.6 Controle de acesso: firewalls
- 8.7 Ataques e medidas de defesa
- 8.8 Segurança em muitas camadas

Firewall

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



Previne ataques de negação de serviço:

- Inundação de SYN: atacante 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

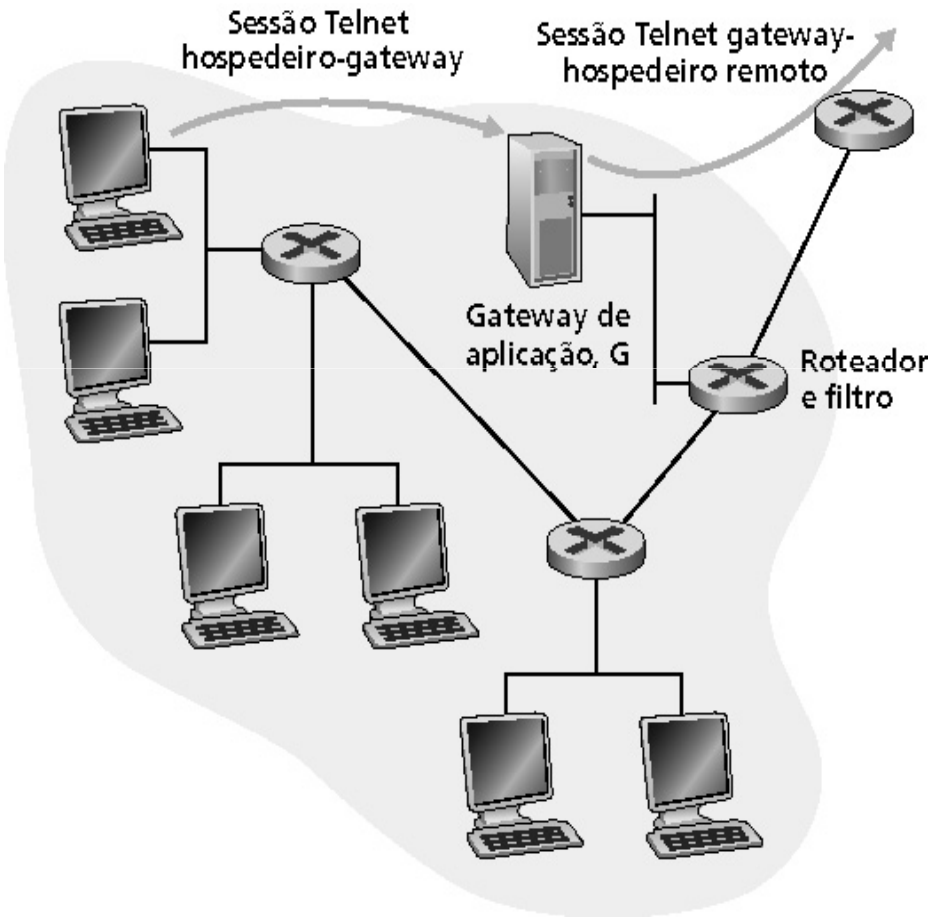
Permite apenas acesso autorizado à rede interna (conjunto de usuários e hospedeiros autenticados)

Dois tipos de firewalls:

- Nível de aplicação
- Filtro de pacotes

- 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

- Exemplo 1: bloqueia datagramas que chegam e que saem com campo de protocolo = 17 e com porta de destino ou de origem = 23
  - Todos os fluxos UDP que entram e que saem e as conexões Telnet são bloqueadas
- Exemplo 2: bloqueia segmentos TCP entrantes com ACK = 0
  - Evita que os clientes externos façam conexões com clientes internos, mas permite que os clientes internos se conectem para fora



- 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

- **IP spoofing:** roteador não pode saber se os dados realmente vêm da fonte declarada
- Se múltiplas aplicações requerem um tratamento especial, cada uma deve ter seu próprio gateway de aplicação
- O software cliente deve saber como contatar o gateway

  Exemplo: deve configurar o endereço IP do proxy no browser Web
- Filtros muitas vezes usam uma regra radical para UDP: bloqueiam tudo ou deixam passar tudo
- Compromisso: grau de comunicação com mundo exterior *versus* nível de segurança
- Muitos sites altamente protegidos sofrem ataques mesmo assim

- 8.1 O que é segurança?
- 8.2 Princípios da criptografia
- 8.3 Autenticação
- 8.4 Integridade
- 8.5 Distribuição de chaves e certificação
- 8.6 Controle de acesso: firewalls
- 8.7 Ataques e medidas de defesa
- 8.8 Segurança em muitas camadas

Mapeamento:

- Antes do ataque: “teste a fechadura” — descubra quais serviços estão implementados na rede
- Use `ping` para determinar quais hospedeiros têm endereços acessíveis na rede
- Varredura de portas: tente estabelecer conexões TCP com cada porta em seqüência (veja o que acontece)

  vnmap (http://www.insecure.org/nmap/) mapeador: “exploração de rede e auditoria de segurança”

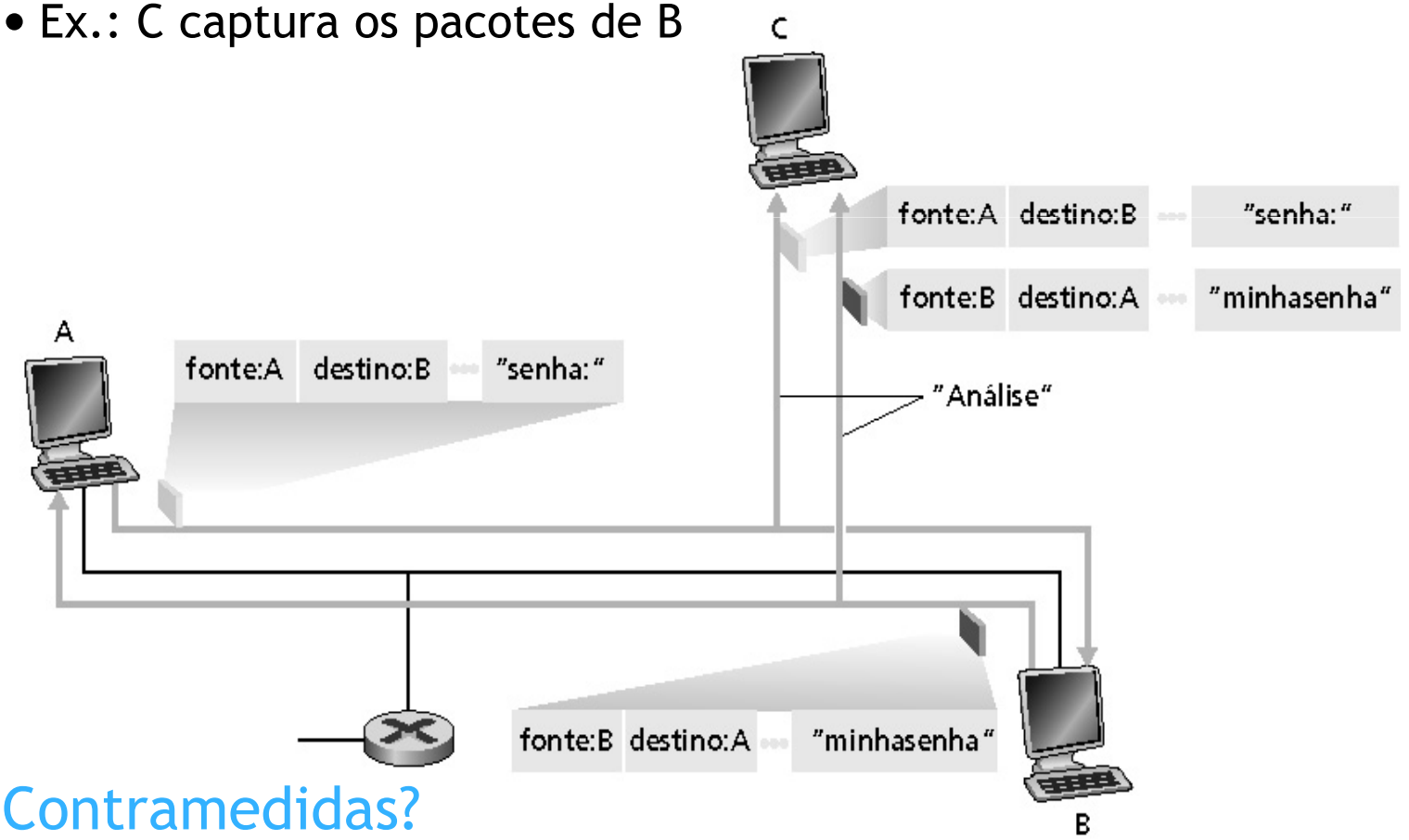
Contramedidas?

Mapeamento: contramedidas

- Grave o tráfego entrando na rede
- Examine atividades suspeitas (endereços IP e portas sendo varridas seqüencialmente)

Packet sniffing:

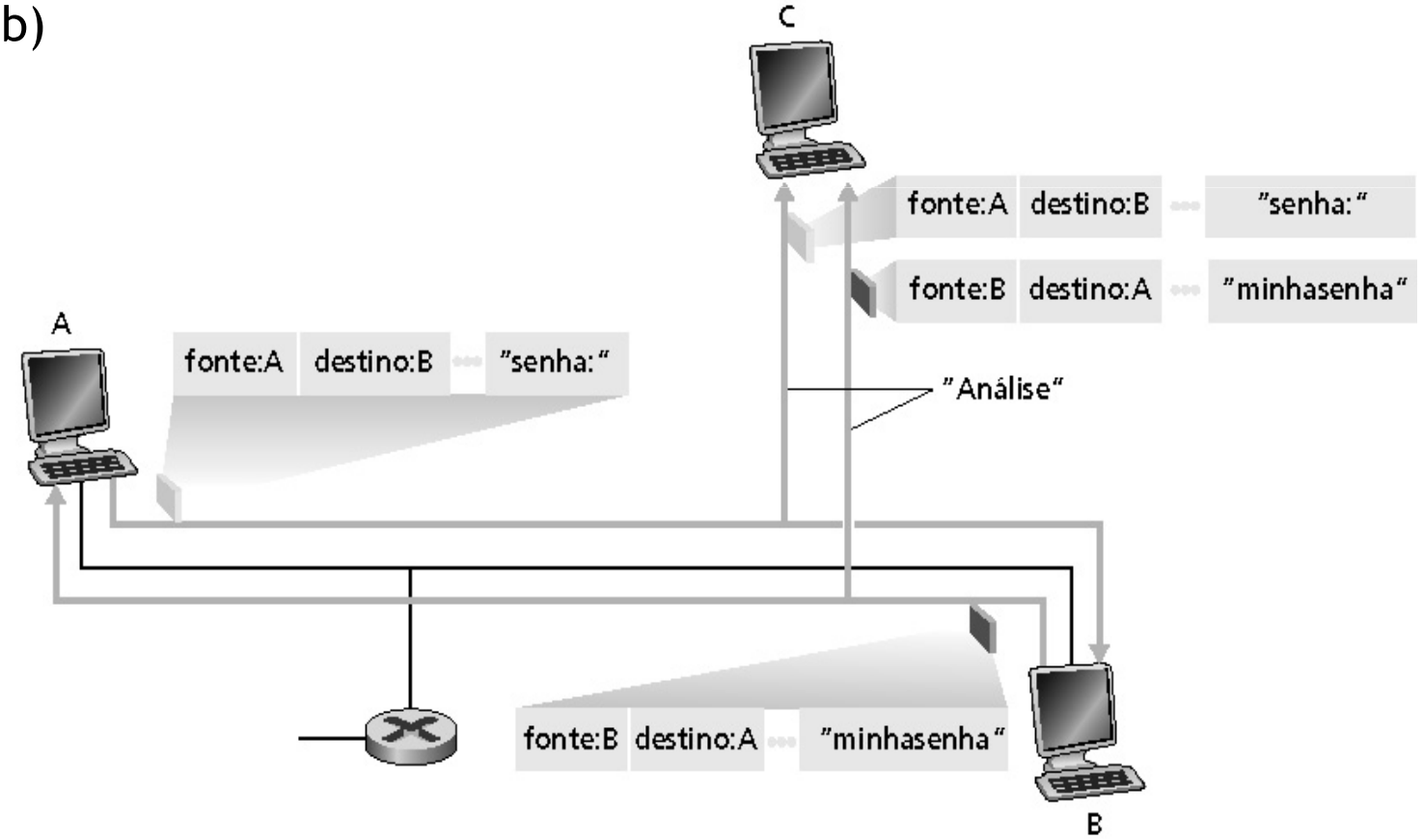
- Meio broadcast
- NIC em modo promíscuo lêem todos os pacotes que passam
- Pode ler todos os dados não criptografados (ex.: senhas)
- Ex.: C captura os pacotes de B



Contramedidas?

Packet sniffing: contramedidas

- Todos os hospedeiros na organização executam software que examina periodicamente se a interface do hospedeiro está operando em modo promíscuo
- Um hospedeiro por segmento de meio broadcast (Ethernet comutada no hub)



IP Spoofing:

- Pode gerar pacotes IP “puros” diretamente da aplicação, colocando qualquer valor do endereço IP no campo de endereço de origem
- Receptor não sabe se a fonte é verdadeira ou se foi forjada

  Ex.: C finge ser B

IP Spoofing: filtro de entrada

- Roteadores não devem repassar pacotes para a saída com endereço de origem inválido (ex.: endereço de fonte do datagrama fora do endereço da rede local)
- Grande, mas filtros de entrada não podem ser obrigatórios para todas as redes

Negação de serviço (DoS):

- Inundação de pacotes maliciosamente gerados invade o receptor receiver
- DoS Distribuído (DDoS): múltiplas fontes coordenadas atacam simultaneamente o receptor

  Exemplo: C e um hospedeiro remoto atacam A com inundação de SYN

TCP transmissor estabelece conexão com o receptor antes de trocar segmentos de dados

- Inicializar variáveis:
  - Números de seqüência
  - Buffers, controle de fluxo (ex.: **`RcvWindow`**)
- **Cliente**: iniciador da conexão

```
Socket clientSocket = new Socket("hostname","port number");
```

- **Servidor**: chamado pelo cliente

```
Socket connectionSocket = welcomeSocket.accept();
```

Three way handshake:

Passo 1: sistema final cliente envia TCP SYN ao servidor
- Especifica número de seqüência inicial

Passo 2: sistema final servidor que recebe o SYN, responde com segmento SYNACK
- Reconhece o SYN recebido
- Aloca buffers
- Especifica o número de seqüência inicial do servidor

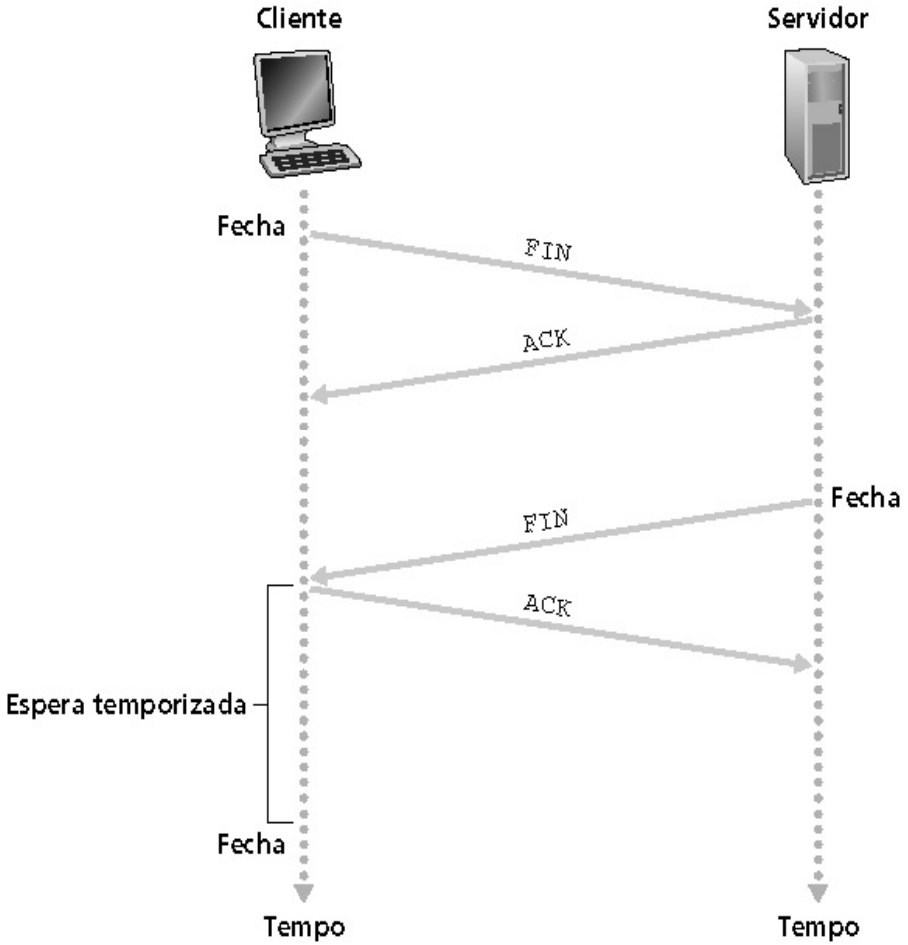
Passo 3: sistema final cliente reconhece o SYNACK

Fechando uma conexão:

cliente fecha o socket:
clientSocket.close();

Passo 1: o cliente envia o segmento TCP FIN ao servidor

Passo 2: servidor recebe FIN, responde com ACK. Fecha a conexão, envia FIN

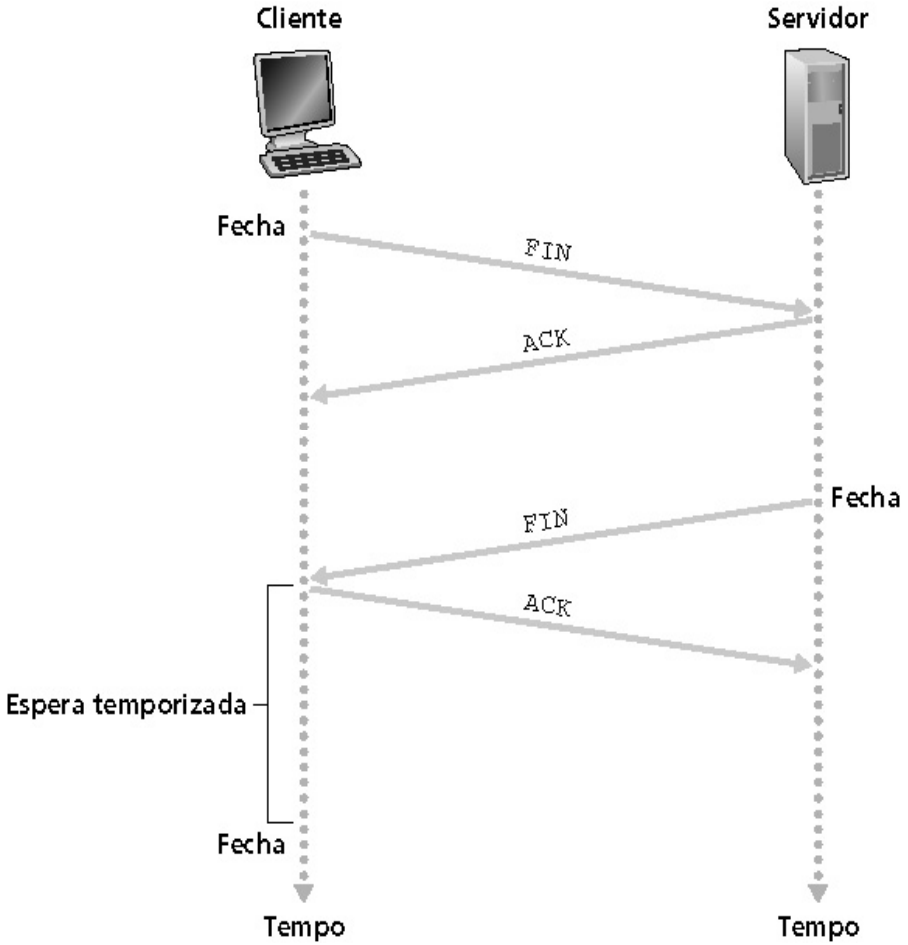


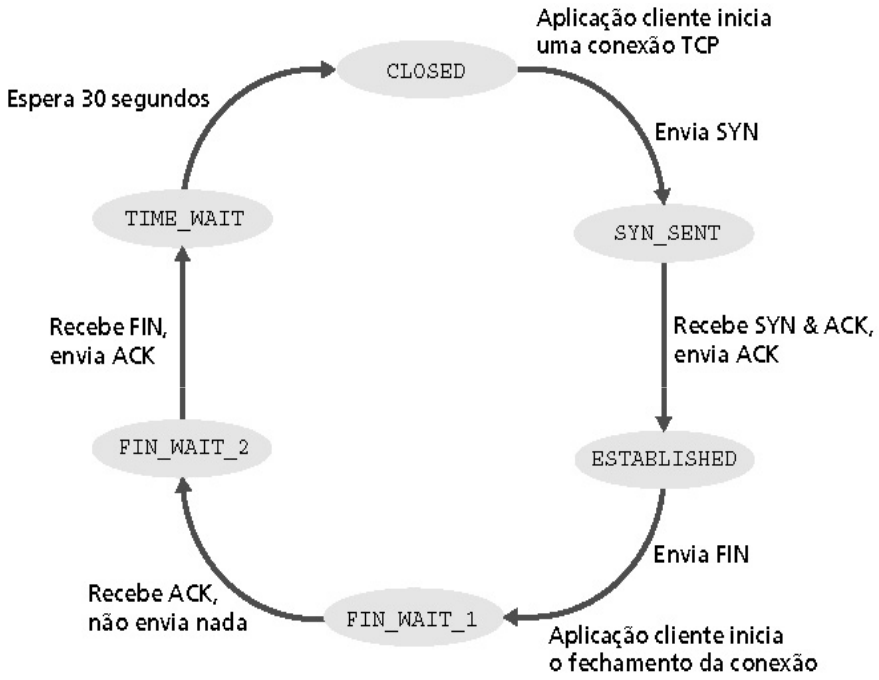
Passo 3: cliente recebe FIN, responde com ACK

• Entra “espera temporizada” - vai responder com ACK a FINs recebidos

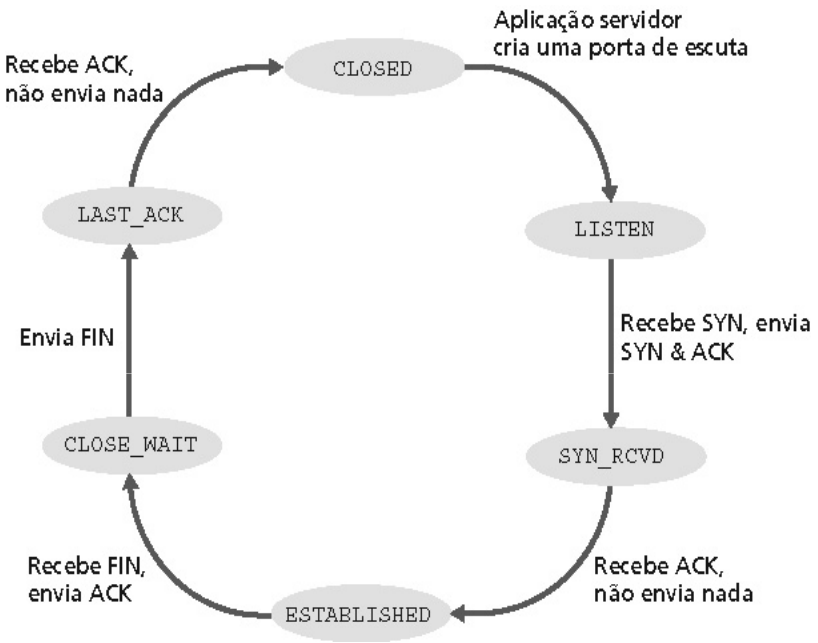
Passo 4: servidor, recebe ACK
Conexão fechada

Nota: com uma pequena modificação, pode-se manipular FINs simultâneos





Estados do cliente



Estados do servidor

Negação de serviço (DoS): contramedidas

- Filtragem de pacotes de inundação (ex.: SYN) antes de atingirem o alvo: corta os pacotes bons e os maus
- Rastrear em busca da fonte da inundação (mais provavelmente uma máquina inocente que foi invadida)

Ataque smurf

Um grande numero de maquinas inocentes respondem a pacotes ICMP de solicitação de eco que contem um endereço de IP de fonte falsificado (o atacado). Isso resulta no envio de um grande número de pacotes ICMP de resposta de eco ao IP sob ataque.

- Usado por computadores e roteadores para troca de informação de controle da camada de rede
  - Error reporting: hospedeiro, rede, porta ou protocolo
  - Echo request/reply (usado pela aplicação ping)
- Transporte de mensagens:
  - Mensagens ICMP transportadas em datagramas IP
- ICMP message: tipo, código, mais primeiros 8 bytes do datagrama IP que causou o erro

Tipo	Código	Descrição
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestio control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

Sequestro (hyjacking)

- Alice e Bob estão se comunicando. Trudy está monitorando (conhece tamanho de janelas, números de sequência, etc)
- Trudy pode se apossar da conexão
  - tirando Alice da conversa com um ataque de DoS à sua máquina
  - gerando pacotes com endereços de Alice (spoofing)

Provinha 25.03.2009

Delineie, baseado no que foi visto até agora, uma estratégia de segurança para proteger a rede 143.107.231/24, dentro da rede da USP (143.107/16) e seus serviços básicos

- 8.1 O que é segurança?
- 8.2 Princípios da criptografia
- 8.3 Autenticação
- 8.4 Integridade
- 8.5 Distribuição de chaves e certificação
- 8.6 Controle de acesso: firewalls
- 8.7 Ataques e medidas de defesa

- 8.8 Segurança na pilha Internet
  - 8.8.1 e-mail seguro (aplicação)
  - 8.8.2 sockets seguros (para transporte)
  - 8.8.3 Ipsec (para a rede)
  - 8.8.4 segurança em 802.11 (para o enlace)

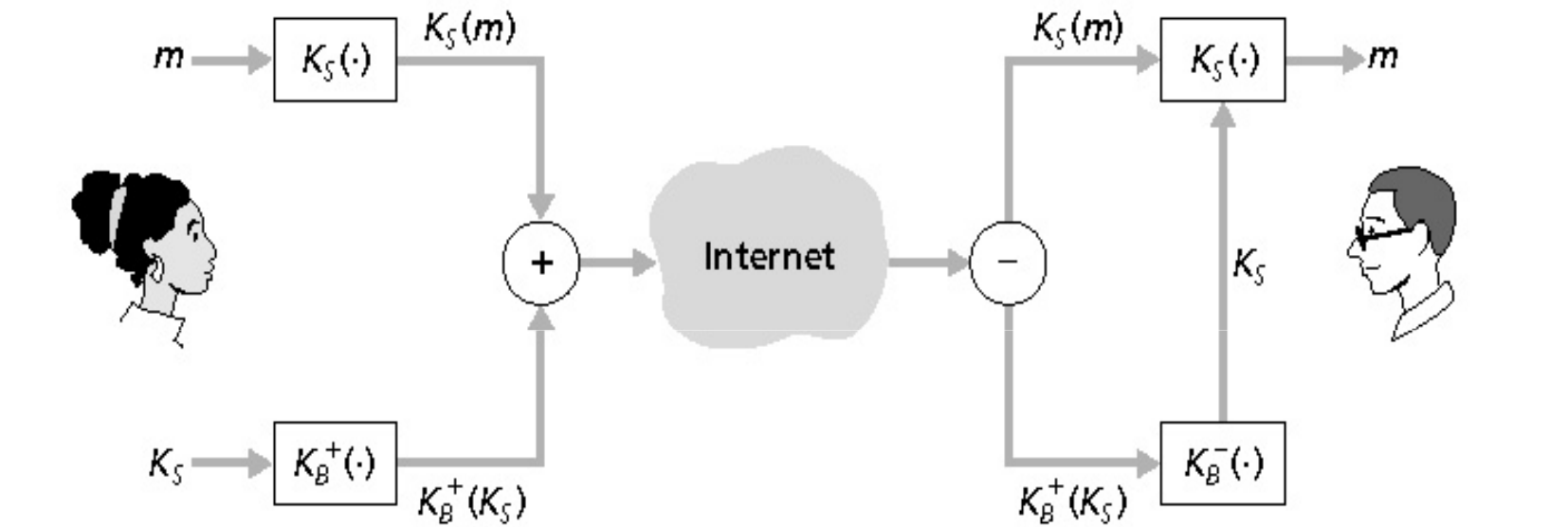
Provinha 01.04.2009

A utilização de Ipsec em redes sem fio provê segurança necessária e suficiente para uma aplicação? Porque?

Um esquema parecido com PGP poderia ser utilizado num link wireless?

Quais seriam os problemas encontrados para a implantação e gerenciamento de um sistema como este?

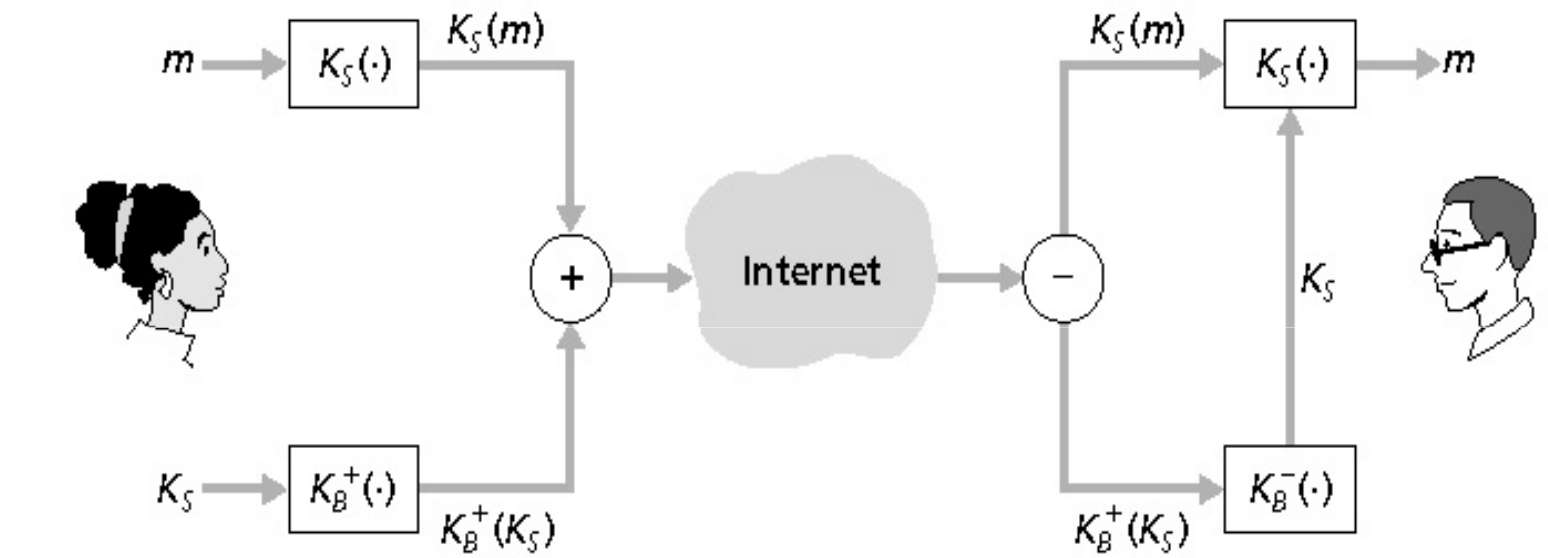
- Alice quer enviar e-mail protegido, *m*, para Bob.



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

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



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

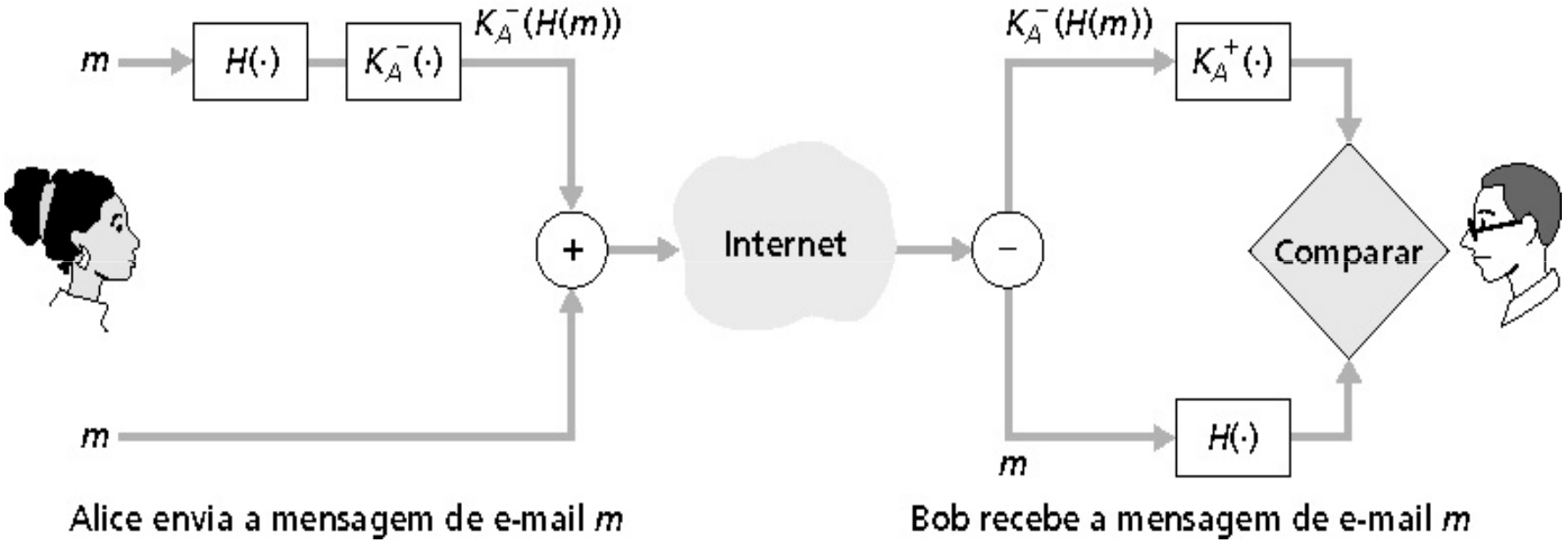
Bob recebe uma mensagem de e-mail, *m*

Bob:

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

Que tipo de proteção está sendo garantida? Porque duas chaves?

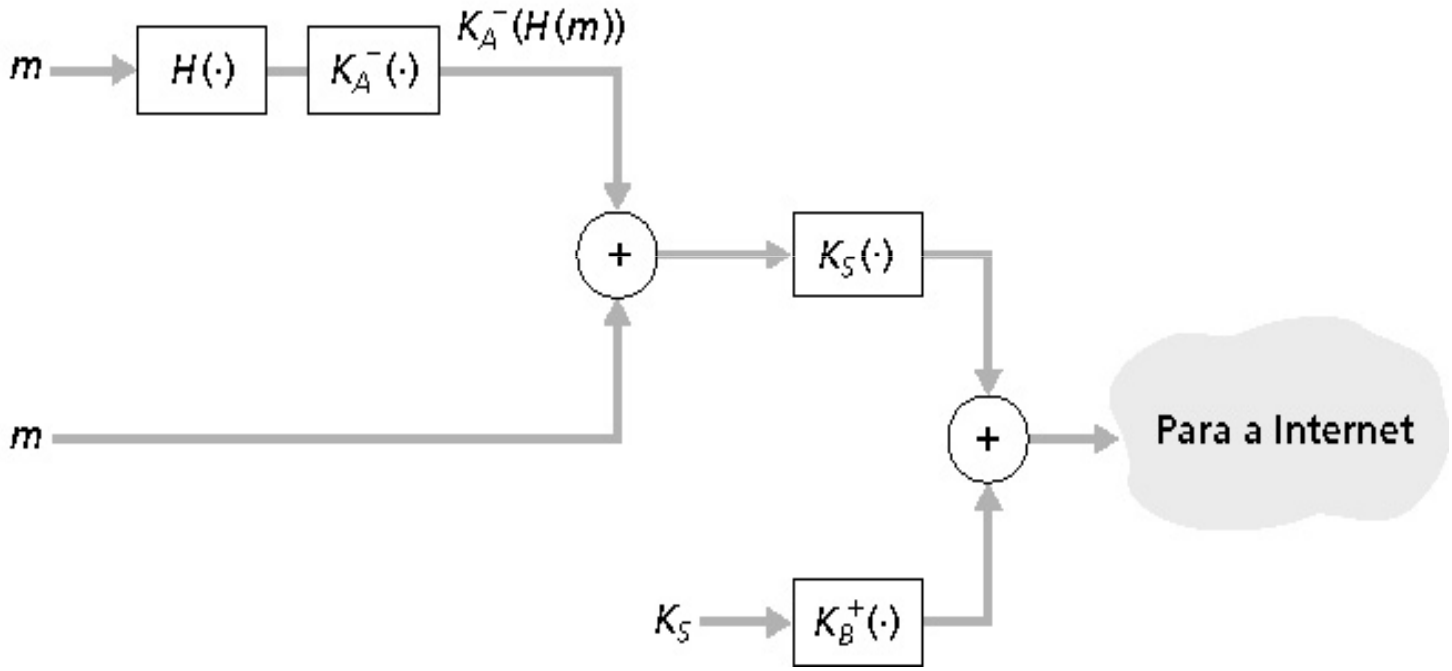
• Alice quer fornecer proteção de mensagem.



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

Que tipo de proteção é feita agora?

- 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

- 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, como descrito nos exemplos anteriores
- Fornece confidencialidade, autenticação do emissor, integridade
- Seu inventor, Phil Zimmermann, foi alvo durante 3 anos de uma investigação federal

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+lo8gE4vB3mqJ
   hFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

Que tipo de proteção leva esta mensagem?

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

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

  Serviços de segurança:
  - Autenticação de servidor
  - Criptografia de dados
  - Autenticação de cliente (opcional)

- Servidor de autenticação:
  - Browser com 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
- Você pode verificar o menu de segurança do seu browser para ver suas CAs confiáveis

- 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: base do padrão transport layer security (TLS) do IETF
- SSL pode ser usado por aplicações fora da Web; ex., IMAP e POP
- Autenticação do cliente pode ser feita com certificados do cliente

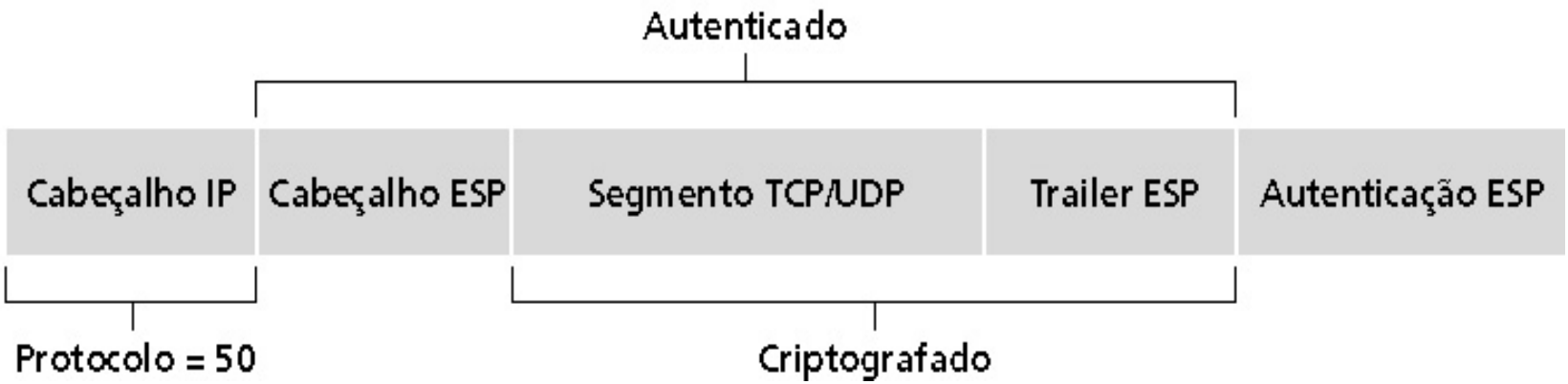
- Confidencialidade na camada de rede:
  - Hospedeiro transmissor criptografa os dados no datagrama IP
  - Segmentos TCP e UDP; mensagens ICMP e SNMP
- Autenticação na camada de rede
  - Hospedeiro de destino pode autenticar o endereço IP da origem
- Integridade na camada de rede
  - Hospedeiro de origem gera hash da mensagem
- Dois protocolos principais:
  - Protocolo de autenticação de cabeçalho (AH)
  - Protocolo de encapsulamento seguro dos dados (ESP)
- Tanto o AH quanto o ESP realizam uma associação da fonte e do destino:
  - Cria um canal lógico de camada de rede denominado associação de segurança (SA — Security association)
- Cada SA é unidirecional
- Unicamente determinado por:
  - Protocolo de segurança (AH ou ESP)
  - Endereço IP de origem
  - ID de conexão de 32 bits

- Oferece autenticação de fonte, integridade dos dados, mas não confidencialidade
- Cabeçalho AH é inserido entre o cabeçalho IP e o campo de dados
- Campo de protocolo 51
- Roteadores intermediários processam o pacote na forma usual

Cabeçalho AH inclui:

- Identificador de conexão
- Dados de autenticação de dados: resumo da mensagem assinado pela fonte calculado sobre o datagrama IP original
- Campo de próximo cabeçalho: especifica tipo de dado (ex.: TCP, UDP, ICMP)

- Oferece confidencialidade, autenticação de hospedeiro e integridade dos dados
- Dados e trailer ESP são criptografados
- Campo de próximo cabeçalho vai no trailer ESP
- Campo de autenticação do ESP é similar ao campo de autenticação do AH
- Protocolo = 50



- *Guerra:* uma pesquisa na área da Baía de San Francisco procurou encontrar redes 802.11 acessíveis
  - Mais de 9.000 acessíveis a partir de áreas públicas
  - 85% não usam criptografia nem autenticação
  - Packet-sniffing e vários outros ataques são fáceis!
- Tornando 802.11 seguro
  - Criptografia, autenticação
  - Primeira tentativa no padrão 802.11: Wired Equivalent Privacy (WEP): um fracasso
  - Tentativa atual: 802.11i

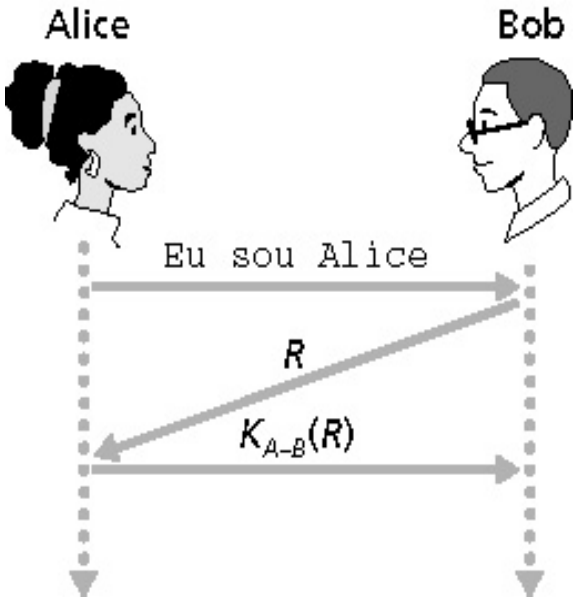
- Autenticação como no protocolo *ap4.0*
  - Hospedeiro solicita autenticação do ponto de acesso
  - Ponto de acesso envia um nonce de 128 bits
  - Hospedeiro criptografa o nonce usando uma chave simétrica compartilhada
  - Ponto de acesso decodifica o nonce, autentica o hospedeiro
- Faltam mecanismos de distribuição de chaves
- Autenticação: conhecer a chave compartilhada é o bastante

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.

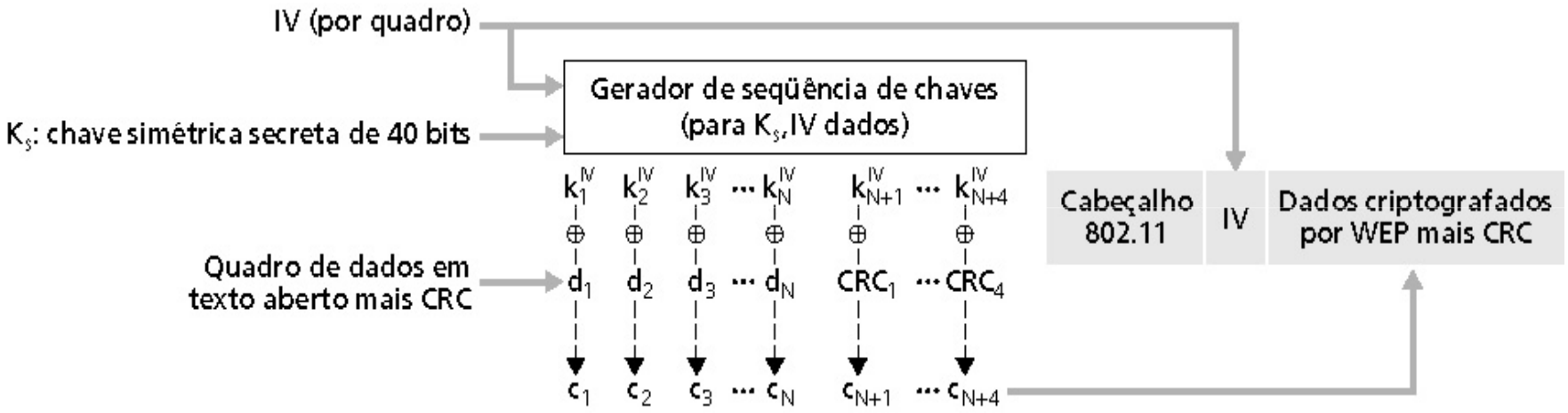


Alice está ao vivo, e apenas Alice conhece a chave para criptografar o nonce, então ela deve ser Alice!

- Hospedeiro e AP compartilham uma chave simétrica de 40 bits (semipermanente)
- Hospedeiro acrescenta vetor de inicialização de 24 bits (IV) para criar uma chave de 64 bits
- A chave de 64 bits é usada para gerar uma seqüência de chaves, k_i^{IV}
- k_i^{IV} é usada para criptografar o I-ésimo byte, d_i, no quadro:

$$c_i = d_i \text{ XOR } k_i^{IV}$$

- IV e bytes criptografados, c_i , são enviados no quadro


IV (por quadro)
Gerador de seqüência de chaves
(para K_s, IV dados)
K_s: chave simétrica secreta de 40 bits
k_1^{IV} k_2^{IV} k_3^{IV} ··· k_N^{IV} k_{N+1}^{IV} ··· k_{N+4}^{IV}
⊕ ⊕ ⊕ ⊕ ⊕ ⊕
Quadro de dados em
texto aberto mais CRC
d_1 d_2 d_3 ··· d_N CRC_1 ··· CRC_4
c_1 c_2 c_3 ··· c_N c_{N+1} ··· c_{N+4}
Cabeçalho
802.11
IV
Dados criptografados
por WEP mais CRC

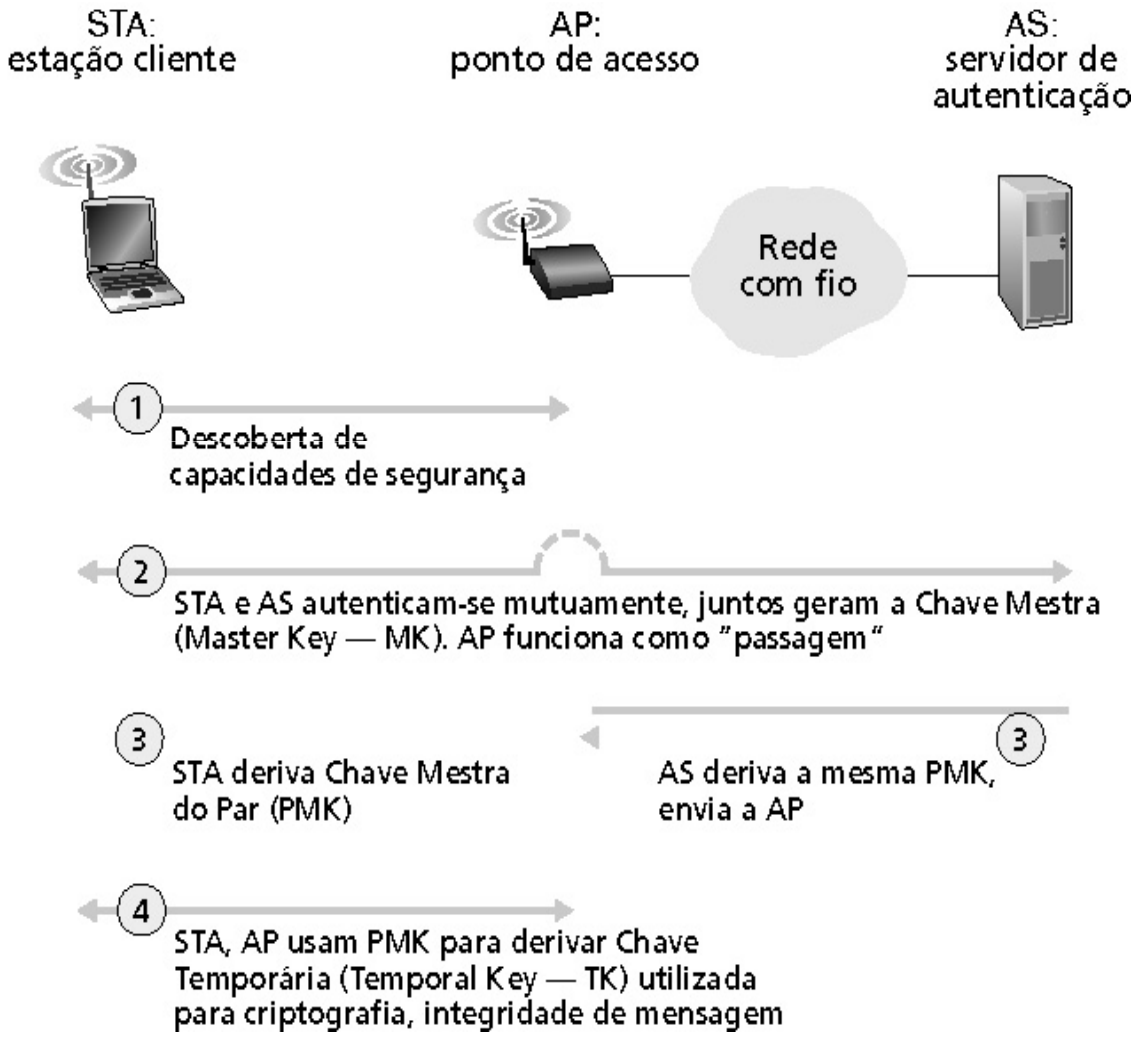
Furo de segurança:

- 24 bits IV, um IV por quadro, -> IV's são reusados eventualmente
- IV é transmitido aberto -> reuso do IV é detectado

Ataque:

- Trudy provoca Alice para criptografar um texto conhecido d_1 d_2 d_3 d_4 …
- Trudy vê: $c_i = d_i$ XOR k_i^{IV}
- Trudy conhece c_i d_i; logo, pode calcular k_i^{IV}
- Trudy sabe a seqüência de chaves criptográfica k_1^{IV} k_2^{IV} k_3^{IV} …
- Da próxima vez que IV for usado, Trudy pode decodificar!

- Numerosas (e mais fortes) forma de criptografia são possíveis
- Oferece distribuição de chave
- Usa autenticação de servidor separada do ponto de acesso


STA:
estação cliente
AP:
ponto de acesso
AS:
servidor de
autenticação
Rede
com fio
1
Descoberta de
capacidades de segurança
2
STA e AS autenticam-se mutuamente, juntos geram a Chave Mestra
(Master Key — MK). AP funciona como "passagem"
3
STA deriva Chave Mestra
do Par (PMK)
3
AS deriva a mesma PMK,
envia a AP
4
STA, AP usam PMK para derivar Chave
Temporária (Temporal Key — TK) utilizada
para criptografia, integridade de mensagem

- EAP: protocolo fim-a-fim entre o cliente (móvel) e o servidor de autenticação
- EAP envia sobre “enlaces” separados
  - Móvel para AP (EAP sobre LAN)
  - AP para servidor de autenticação (RADIUS sobre UDP)

EAP TLS	
EAP	
EAP por LAN (EAPoL)	RADIUS
IEEE 802.11	UDP/IP

Técnicas básicas...

- Criptografia (simétrica e pública)
- Autenticação
- Integridade de mensagens
- Distribuição de chaves

...usadas em muitos cenários diferentes de segurança

- E-mail seguro
- Transporte seguro (SSL)
- IP sec
- 802.11

Provinha – 17.11.2009

- Explique os 4 principais parâmetros de segurança. Para cada um deles, explique como pode interferir no desempenho de aplicações em rede.
- Explique como o uso de chaves públicas pode garantir o não repúdio na comunicação em rede.

- Provona:
  - 2.6 - O sistema de telefonia móvel
  - 4.4 a 4.6 - Comunicação sem fio
  - 4.7 - switching (+ infiniband e noções de IDC)
  - 5.4 - Quality of Service (and ATM and noçoes de streaming)
  - Cap8 Kurose - Security