

Segurança de Redes

Alan Nakai

Adaptado de: Kurose, J. F. e Keith, R. W. Redes de Computadores e a Internet.
Pearson Education, 2005.

Roteiro

- O que é segurança de rede?
- Princípios da criptografia
- Autenticação
- Integridade
- Distribuição de chaves e certificação
- Controle de acesso: firewalls
- Segurança para Email e Web
- Malware

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

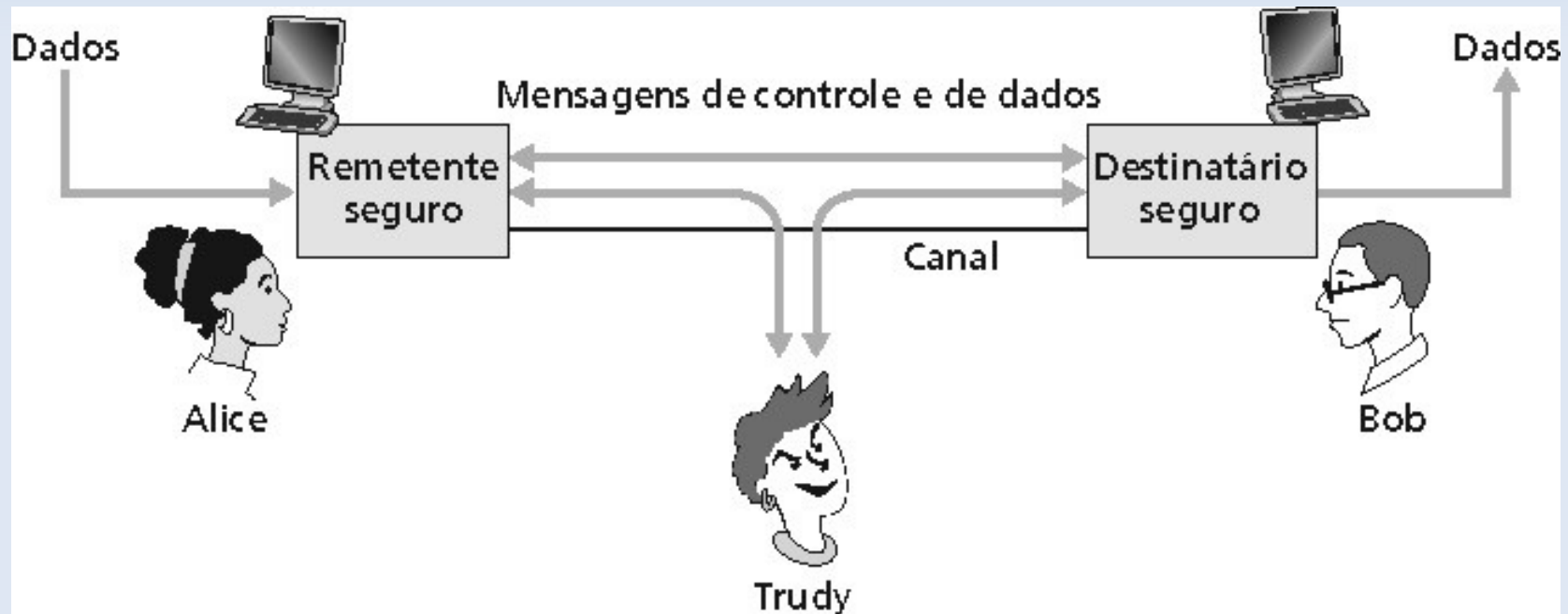
Autenticação: transmissor e receptor querem confirmar a identidade um do outro

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

Amigos e Inimigos

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



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 trocam atualizações de tabela de roteamento

Existem pessoas más por aí!

P.: O que uma “pessoa má” pode fazer?

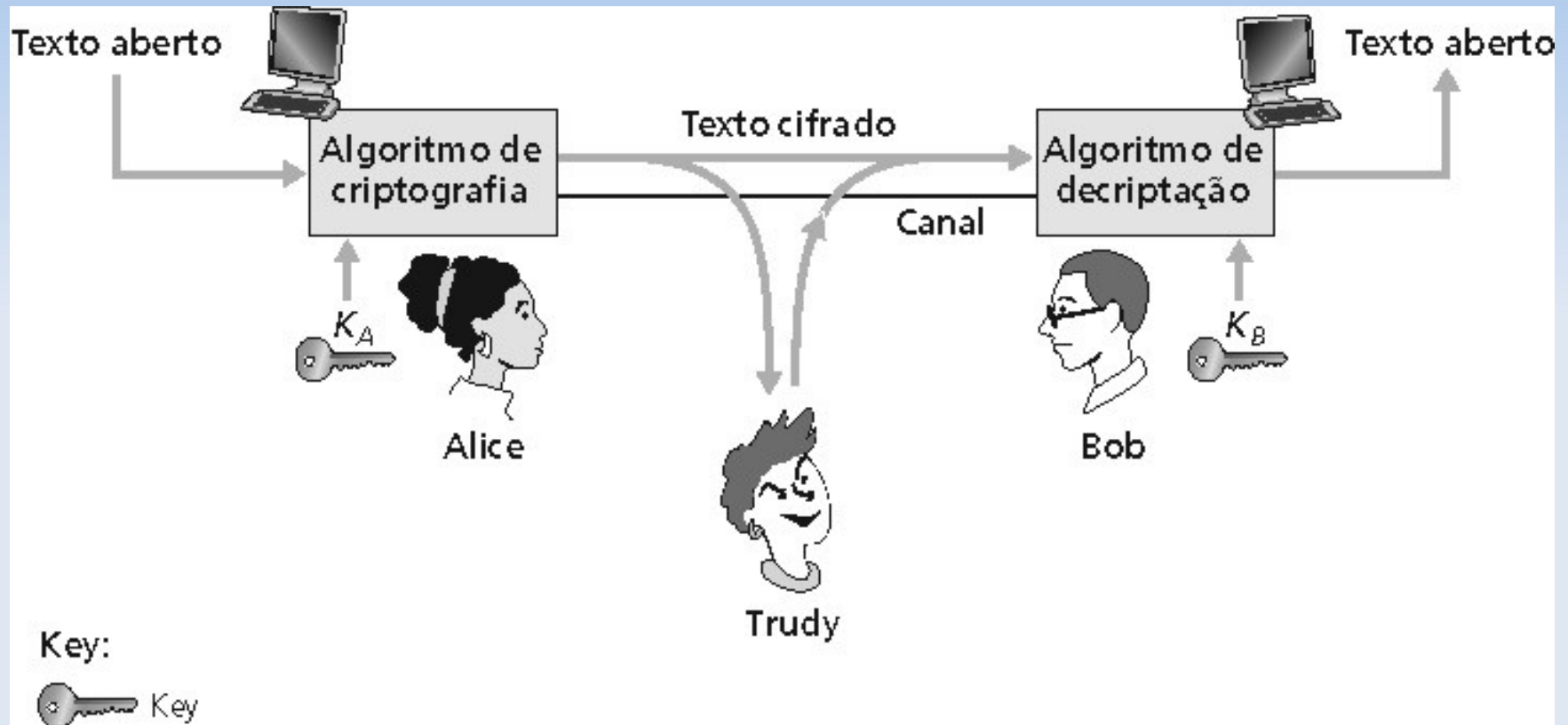
R.: Muito!

- *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)

Roteiro

- O que é segurança de rede?
- **Princípios da criptografia**
- Autenticação
- Integridade
- Distribuição de chaves e certificação
- Controle de acesso: firewalls
- Segurança para Email e Web
- Malware

Criptografia



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

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

Criptografia de Chave Simétrica

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 mono alfabético

Criptografia de Chave Simétrica

DES: Data encryption standard

- Padrão de criptografia dos EUA [NIST 1993]
- Chave simétrica de 56 bits, 64 bits de texto aberto na entrada
- Quanto 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
 - Não há ataque mais curto conhecido
- Tornando o DES mais seguro
 - Use três chaves em seqüência (3-DES) sobre cada dado
 - Use encadeamento de blocos de códigos

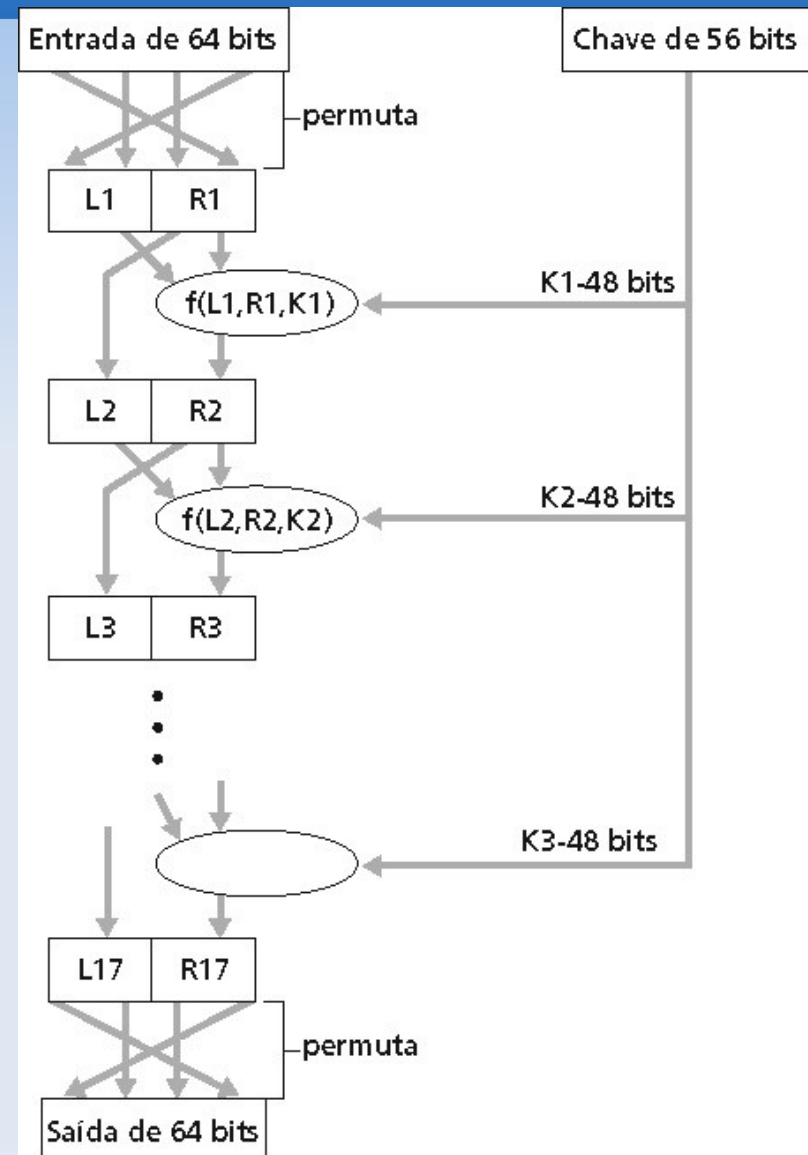
Criptografia de Chave Simétrica

Operação do DES

permutação inicial

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

permutação final



Criptografia de Chave Simétrica

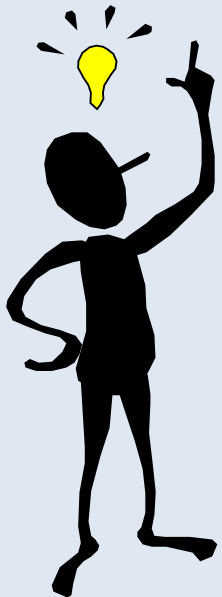
AES (Advanced Encryption Standard)

- 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

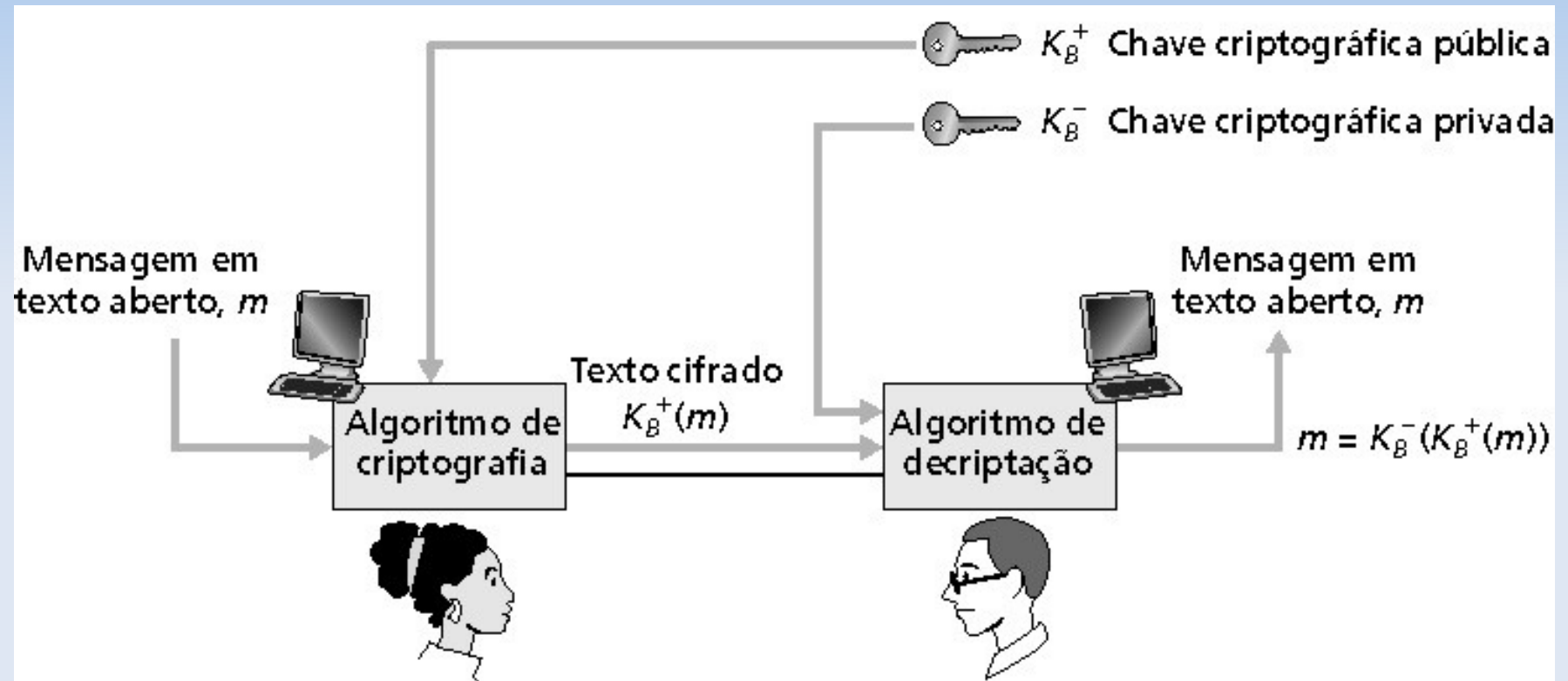
- Exige que o transmissor e o receptor compartilhem a chave secreta
- P.: como combinar a chave inicialmente (especialmente no caso em que eles nunca se encontram)?



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 decifração é **privada** (conhecida somente pelo receptor)

Criptografia de Chave Pública



Criptografia de 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: $ed \bmod z = 1$).
5. Chave pública é (n, e) . Chave privada é (n, d) .

K_B^+

K_B^-

RSA: Criptografia e decifração

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

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

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

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

$$m = c^d \bmod n \quad (\text{i.e., resto quando } c^d \text{ é dividido } n).$$

Mágica
acontece!

$$m = (m^e \bmod n)^d \bmod n$$

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).

	<u>letra</u>	<u>m</u>	<u>m^e</u>	<u>c = m^e mod n</u>	
criptografia:		12	1524832	17	
	<u>c</u>	<u>c^d</u>	<u>m = c^d mod n</u>	<u>letra</u>	
decriptografia:	17	481968572106750915091411825223072000	12		

RSA: Propriedade Importante

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

$$\underbrace{K_B^-(K_B^+(m))}_{\text{usa chave pública primeiro, seguida pela chave privada}} = m = \underbrace{K_B^+(K_B^-(m))}_{\text{usa chave privada primeiro, seguida pela chave pública}}$$

usa chave pública primeiro, seguida pela chave privada

usa chave privada primeiro, seguida pela chave pública

O resultado é o mesmo!

Roteiro

- O que é segurança de rede?
- Princípios da criptografia
- Autenticação
- Integridade
- Distribuição de chaves e certificação
- Controle de acesso: firewalls
- Segurança para Email e Web
- Malware

Autenticação

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

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

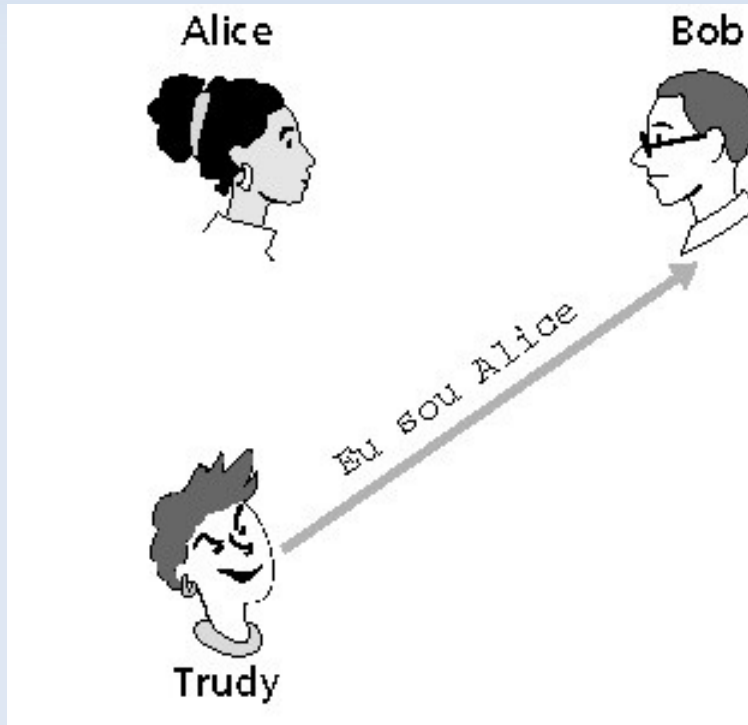


Cenário de falha?? 22

Autenticação

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

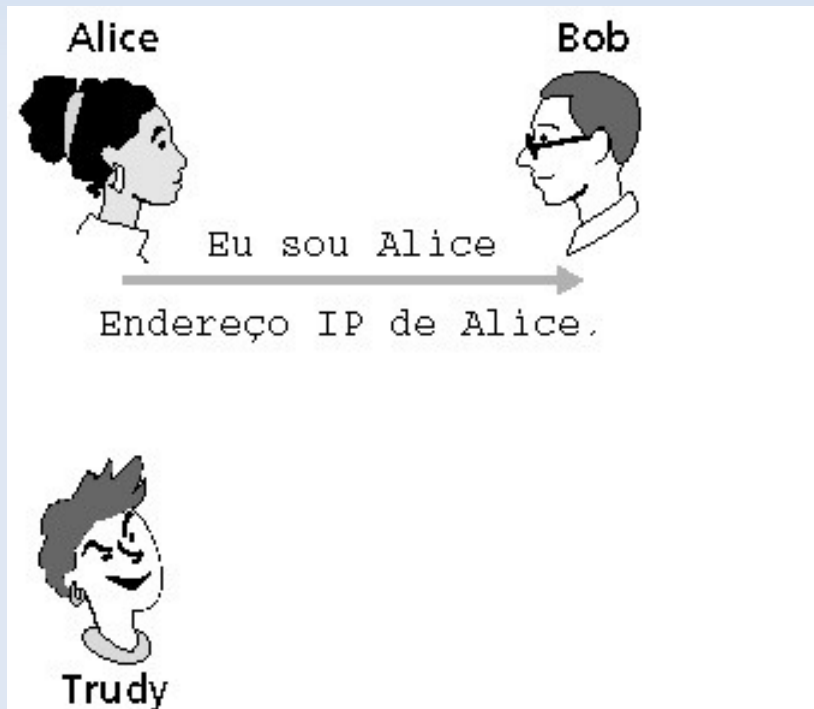
Protocolo ap1.0: Alice diz “Eu sou Alice”



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

Autenticação

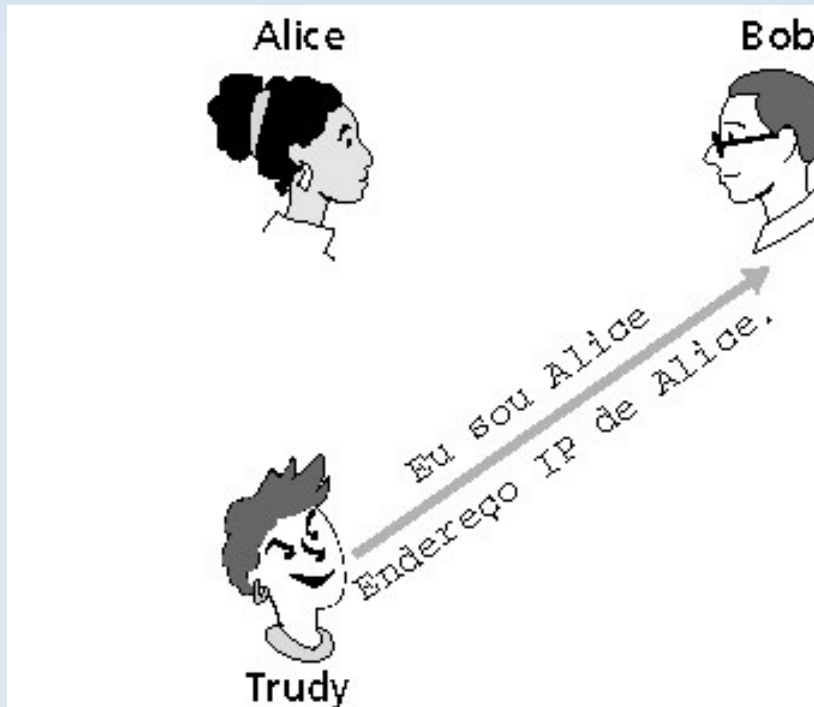
Protocolo ap2.0: Alice diz “Eu sou Alice” e envia seu endereço IP junto como prova.



Cenário de falha??

Autenticação

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

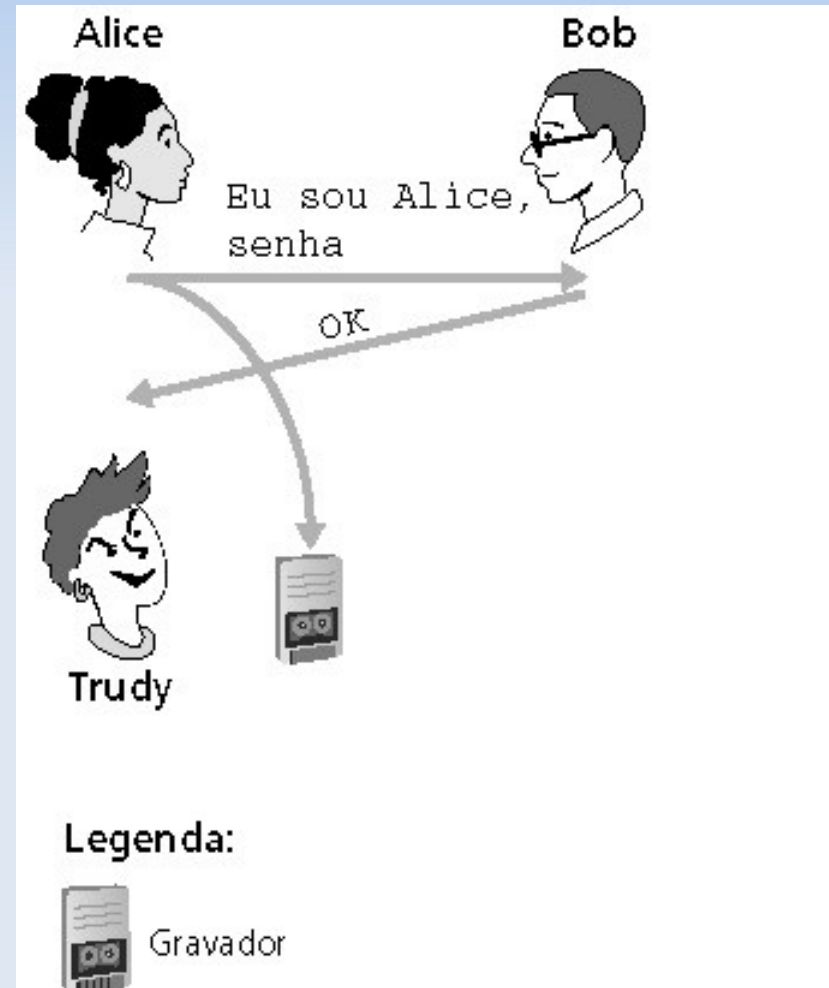


Trudy pode criar um pacote “trapaceando” (*spoofing*) o endereço de Alice

Autenticação

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

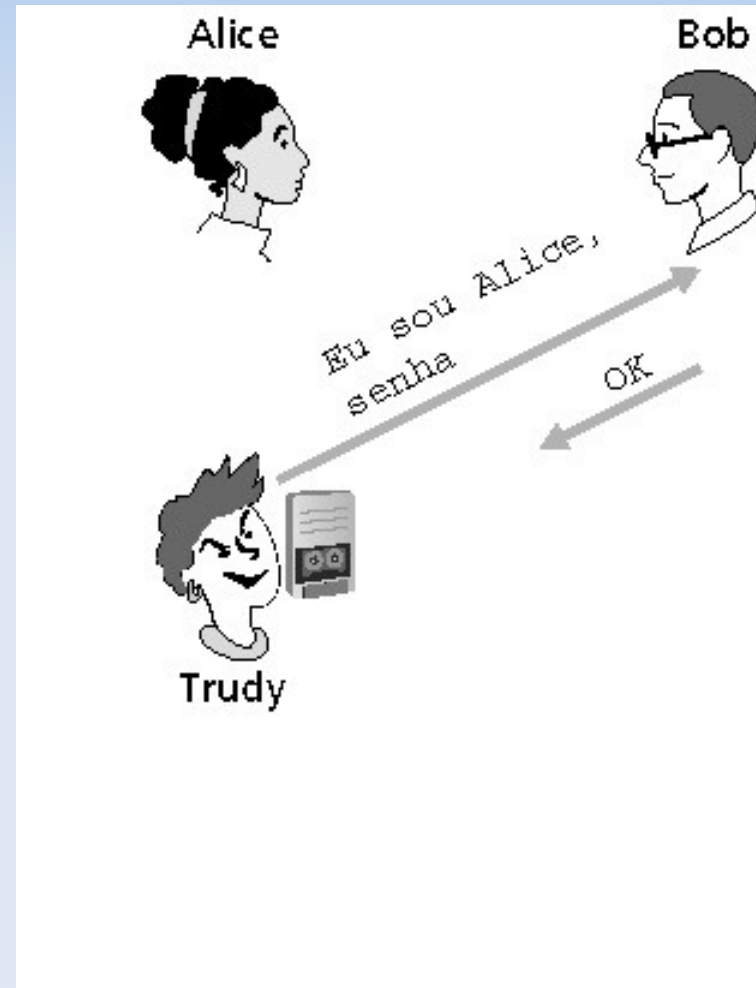
Cenário de falha??



Autenticação

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

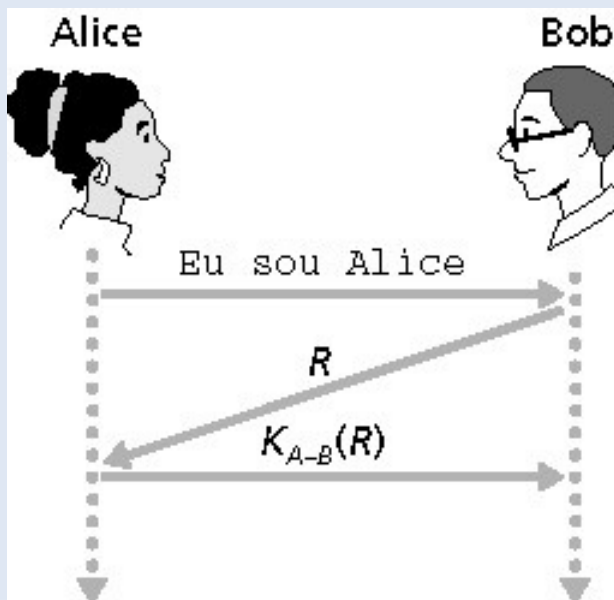


Autenticação

Meta: evitar ataque de reprodução (playback).

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

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



Falhas, problemas?

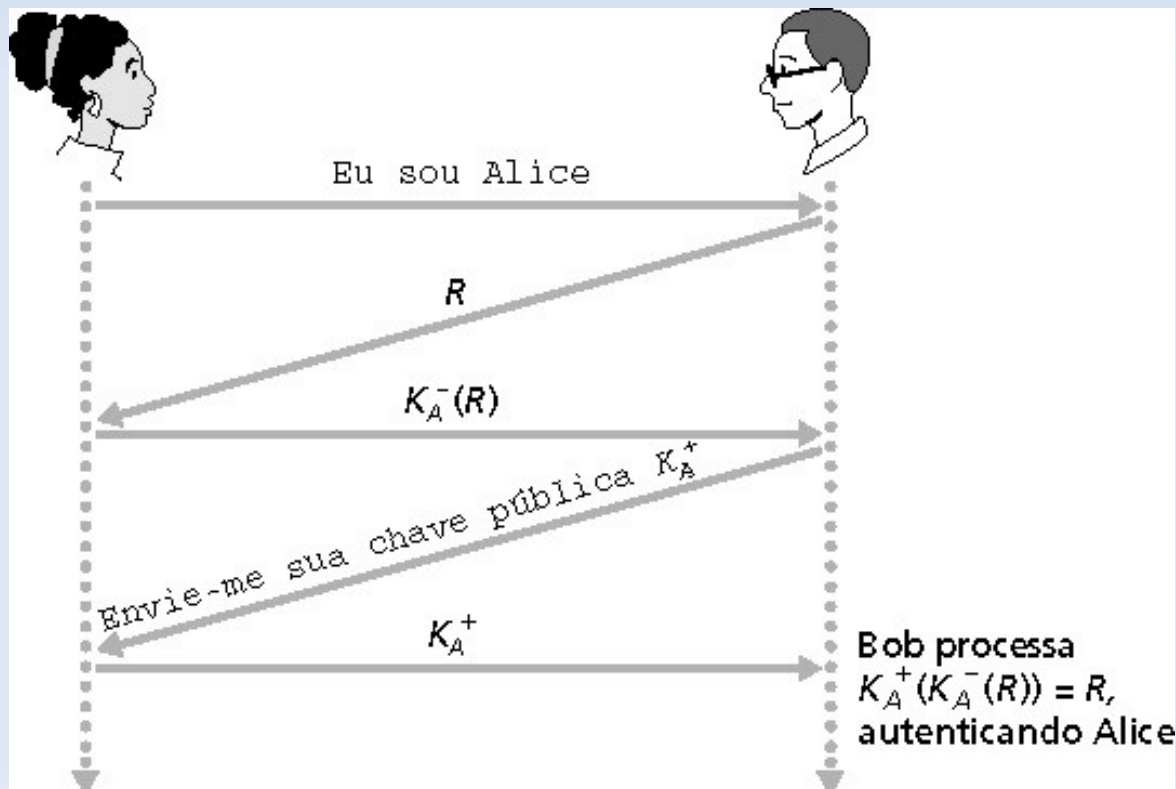
Alice está ao vivo,
e apenas Alice
conhece a chave
para criptografar o
nonce, então ela
deve ser Alice!

Autenticação

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

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

Roteiro

- O que é segurança de rede?
- Princípios da criptografia
- Autenticação
- **Integridade**
- Distribuição de chaves e certificação
- Controle de acesso: firewalls
- Segurança para Email e Web
- Malware

Assinaturas Digitais

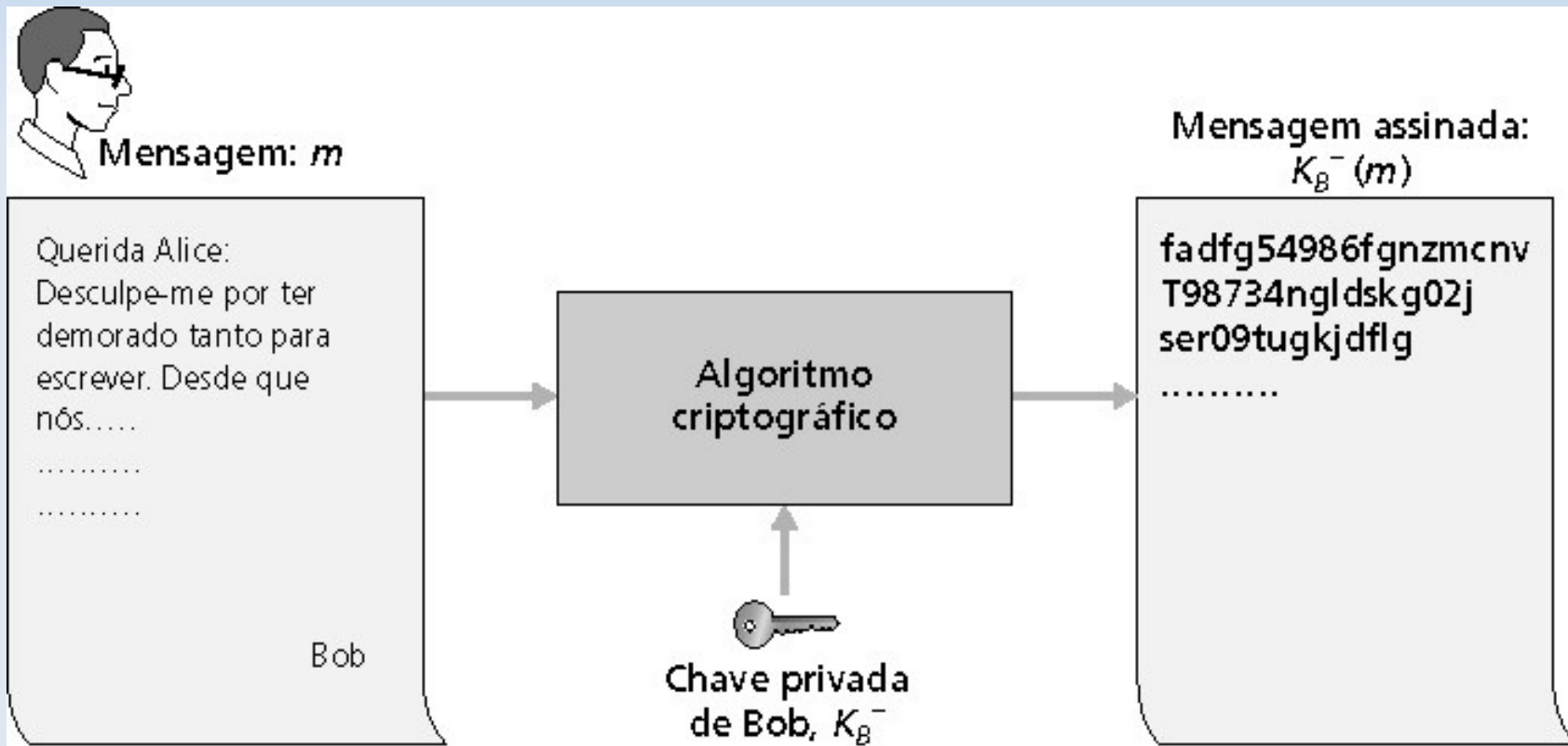
Técnica criptográfica análoga às assinaturas manuais.

- Transmissor (Bob) assina digitalmente um documento, estabelecendo que ele é o autor/criador.
- **Verificável, não forjável:** receptor (Alice) pode verificar que Bob, e ninguém mais, assinou o documento.

Assinaturas Digitais

Assinatura digital simples para mensagem m :

- Bob assina m criptografado com sua chave privada K_B^- , criando a mensagem “assinada”, $K_B^-(m)$



Assinaturas Digitais

- 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 .

Não-repúdio:

- Alice pode provar que Bob assinou m .

Roteiro

- O que é segurança de rede?
- Princípios da criptografia
- Autenticação
- Integridade
- Distribuição de chaves e certificação
- Controle de acesso: firewalls
- Segurança para Email e Web
- Malware

Intermediários Confiáveis

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 site, e-mail, disquete), como ela sabe que é a chave pública de Bob e não de Trudy?

Solução:

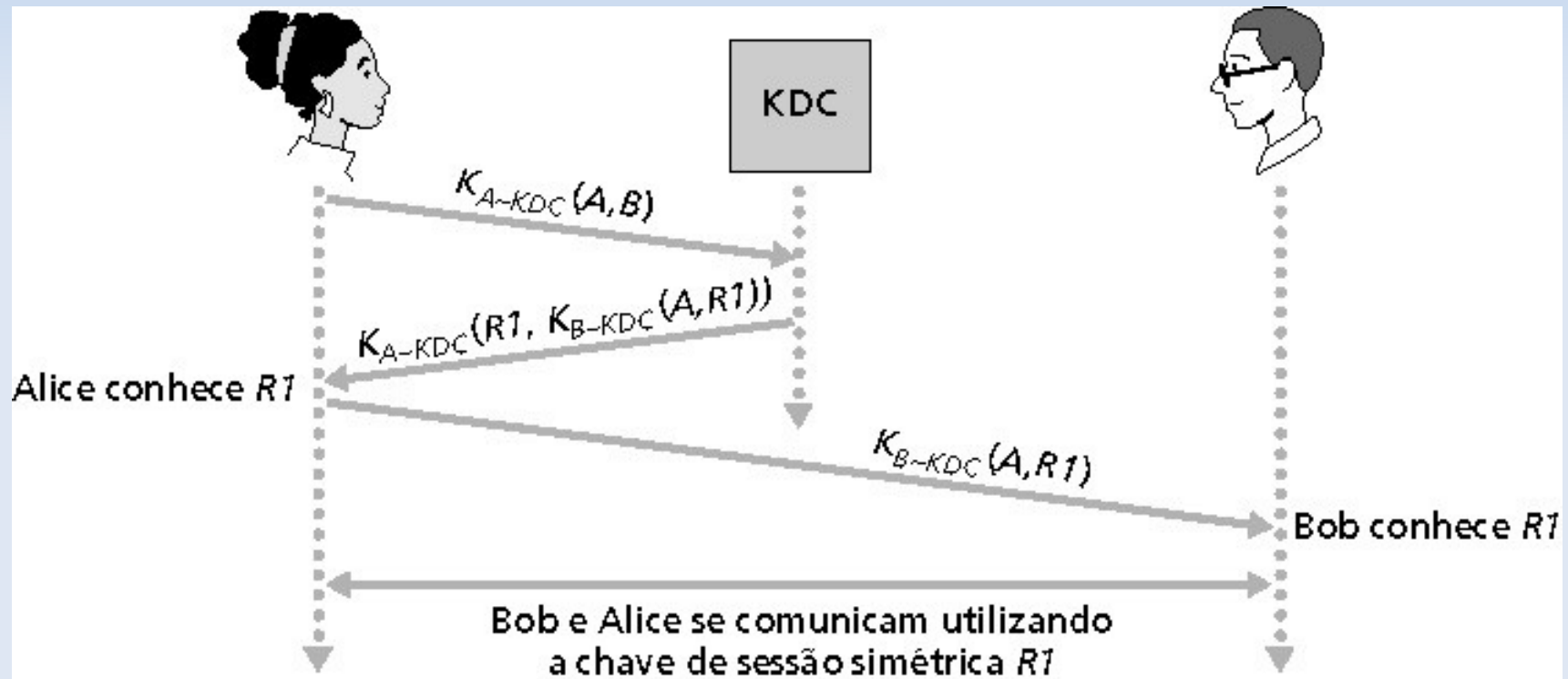
- Autoridade de certificação confiável (CA)

Centro de Distribuição de Chave

- 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-KDC} K_{B-KDC} , para comunicação com o KDC.

Centro de Distribuição de Chave

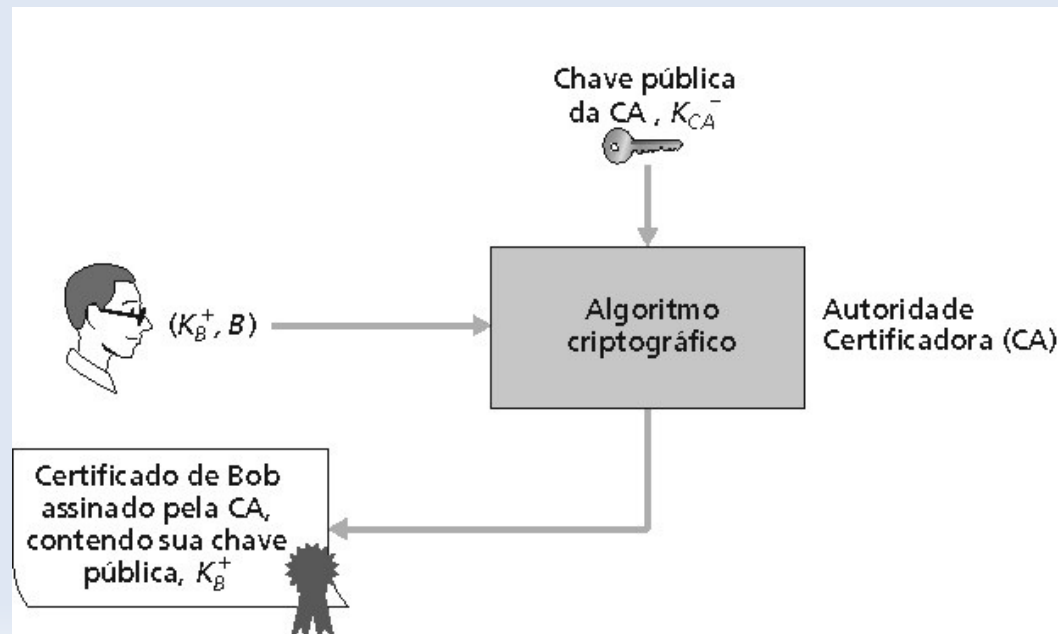
P.: Como o KDC permite que Bob e Alice determinem uma chave simétrica comum para comunicarem-se entre si?



Autoridade Certificadora

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 a sua chave pública
- Certificado contendo a chave pública de E digitalmente assinada pela CA – CA diz “esta é a chave pública de E”



Autoridade Certificadora

- 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

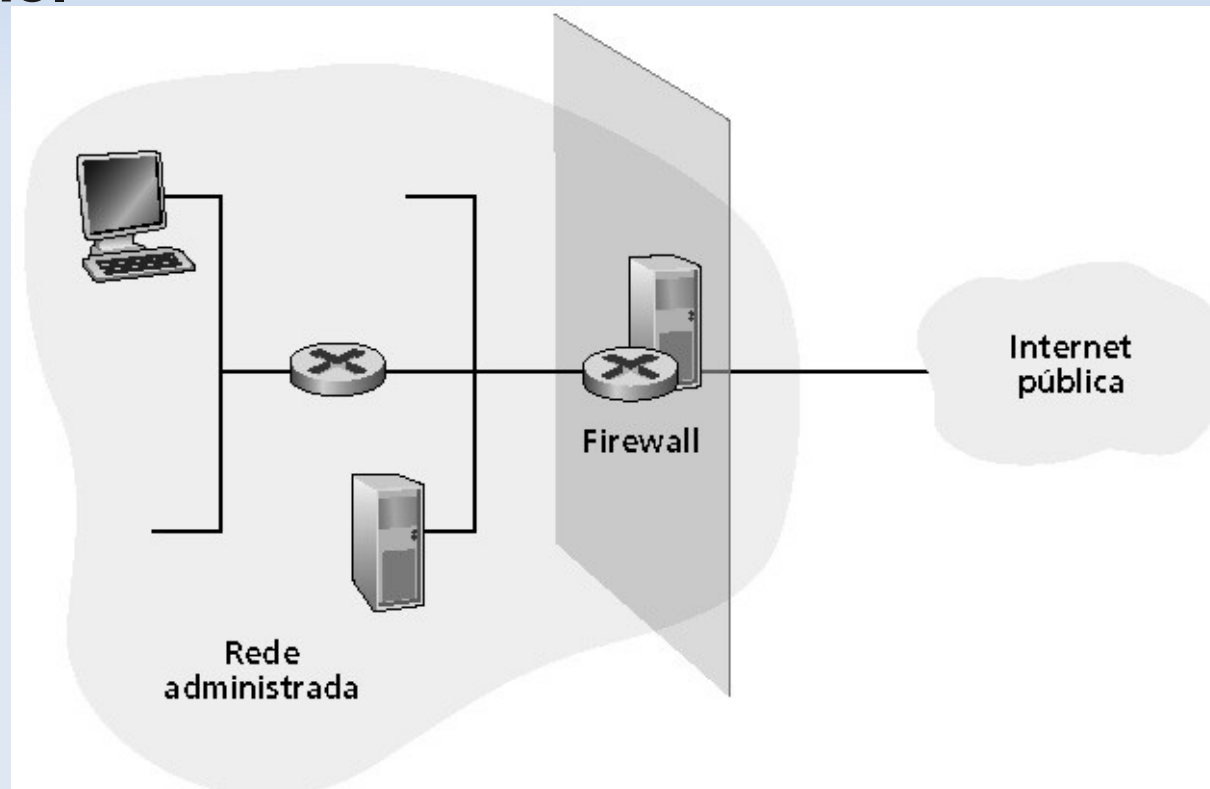
Roteiro

- O que é segurança de rede?
- Princípios da criptografia
- Autenticação
- Integridade
- Distribuição de chaves e certificação
- Controle de acesso: firewalls
- Segurança para Email e Web
- Malware

Firewalls

Firewall

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



Firewalls

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)

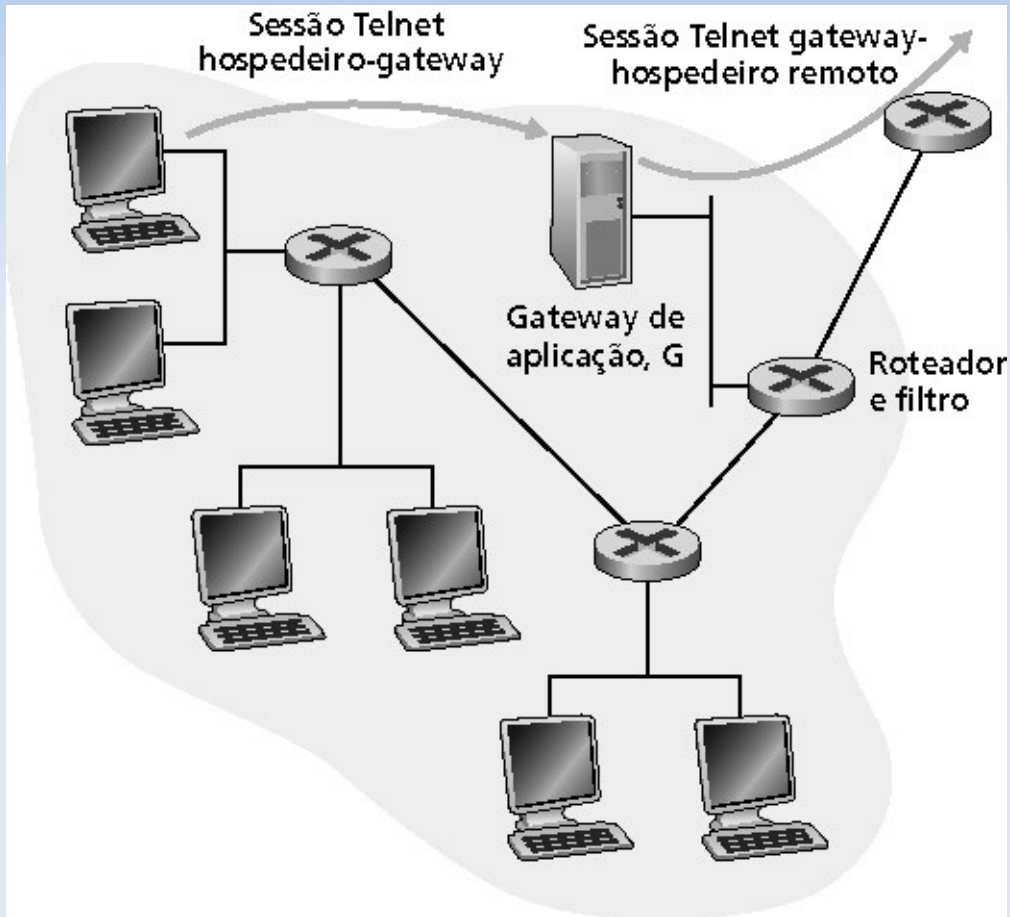
Dois tipos de firewalls:

- Filtro de pacotes
- Nível da 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

Gateways de Aplicação



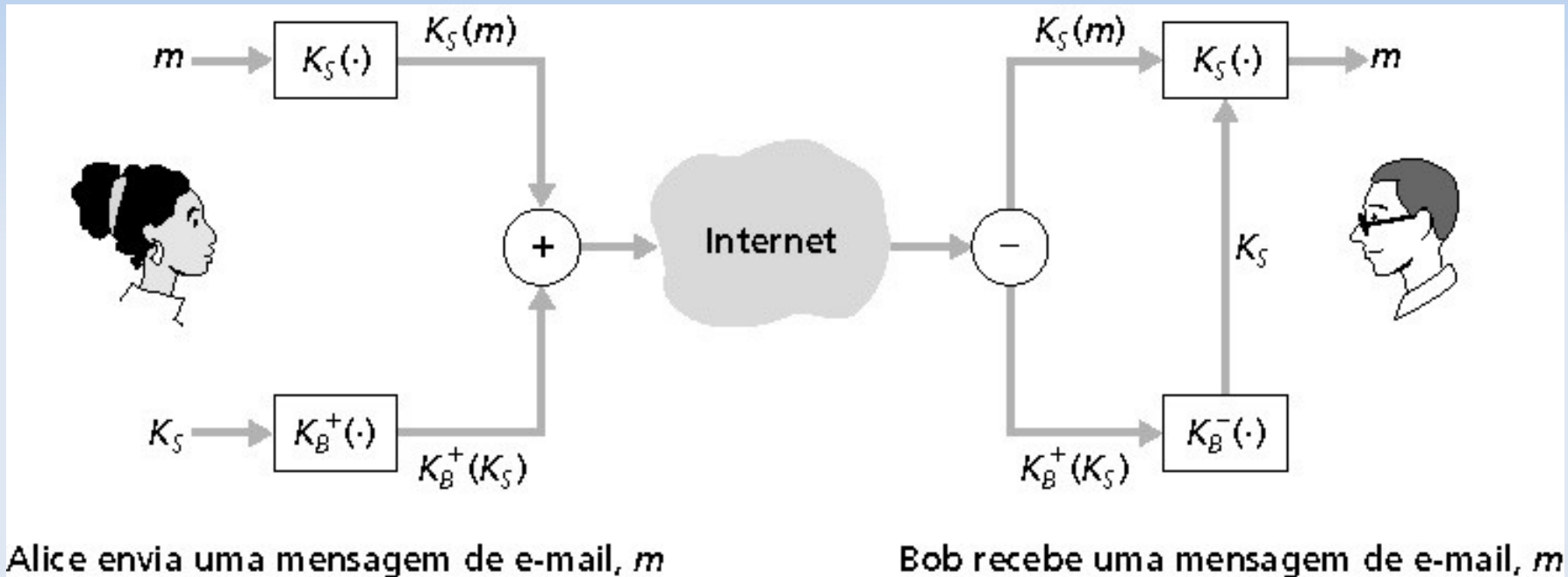
- Filtra pacotes em função de dados de aplicação, assim como de campos do IP/TCP/UDP
- **Exemplo:** permite selecionar usuários internos que podem usar o Telnet

Roteiro

- O que é segurança de rede?
- Princípios da criptografia
- Autenticação
- Integridade
- Distribuição de chaves e certificação
- Controle de acesso: firewalls
- **Segurança para Email e Web**
- Malware

E-mail Seguro

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

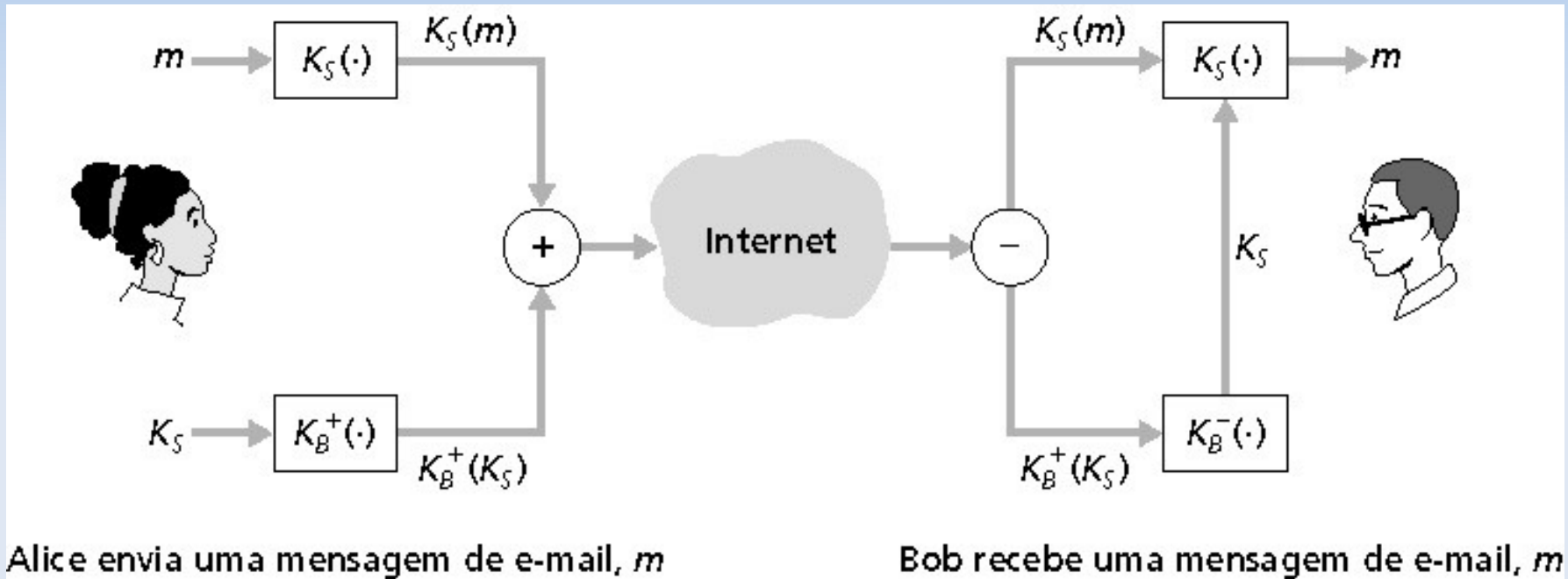


Alice:

- 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

E-mail Seguro

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



Bob:

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

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)
- **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

Camada de Sockets Segura (SSL)

- **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
- Autenticação do cliente pode ser feita com certificados do cliente

Roteiro

- O que é segurança de rede?
- Princípios da criptografia
- Autenticação
- Integridade
- Distribuição de chaves e certificação
- Controle de acesso: firewalls
- Segurança para Email e Web
- Malware

Malware

Conjunto de instruções executadas no seu computador que fazem seu sistema realizar algo que o *atacante* deseja.

- Apagar arquivos;
- Disseminar o malware;
- Monitorar o teclado;
- Coletar informações;
- Executar comandos;
- Roubar informações;
- Upload de arquivos;
- Usar a sua máquina para realizar crimes; etc...

Malware

Tipos de Malware

- Vírus
 - Auto-replicável;
 - Infecta outros arquivos - (parasita) - requer interação humana;
 - Executa ações maliciosas.
- Worms
 - Propagação pela rede;
 - Diferença para vírus: não necessita interação humana.

Malware

Tipos de Malware

- Código móvel malicioso
 - Pequenos programas “baixados” e executados no computador, usualmente pelo browser;
 - Ex. JavaScript, ActiveX, JavaApplets, etc.
- Backdoors
 - Facilita ao atacante ultrapassar o sistema de segurança e controlar seu computador.
- Cavalo de Tróia (Trojans)
 - Um programa que parece benigno, mas esconde algo ruim...

Malware

Tipos de Malware

- Rootkits
 - Trojans que alteram o sistema operacional para facilitar o acesso ao computador;
- Spyware
 - Programa espião: coleta de dados do usuário;
 - Adware: propaganda;
 - Ransomware: “Resgate”.

Referências

- Computer Networking: A Top-Down Approach - Fifth Edition, James Kurose e Keith Ross, Addison-Wesley.
- Malware: Fighting Malicious Code
<http://proquest.safaribooksonline.com/0-13-101405-6>