UFMS DIGITAL

# Infraestrutura para Sistemas de Software

Prof. Dr. Carlos Alberto da Silva

UFMS DIGITAL

# Módulo 3 - Roteamento e segurança de redes

## Unidade 2 - Os princípios e mecanismos de segurança nas redes

# Mapa da aula

## Os princípios e mecanismos de segurança nas redes

- Princípios de segurança da informação
- Criptografia
- Mecanismos de segurança
- Firewall

# Princípios de segurança da informação

# Princípios de segurança

Devemos garantir os princípios de segurança para:

- Confidencialidade;
- Integridade;
- Disponibilidade;
- Autenticidade;
- Não-repúdio.

# Formas de proteger a informação

- Segurança computacional
  - são políticas, mecanismos e ferramentas que visam proteger e garantir os princípios de segurança para as informações.

# Formas de proteger a informação

- *Cyber Security*
  - é prática de proteger os dispositivos das redes contra ameaças do tipo:
    - crime virtual;
    - ataque cibernético;
    - terrorismo cibernético.

# Formas de proteger a informação

Ataques podem ser do tipo:

- *Malware* (Software malicioso)
  - Vírus, Cavalos de Troia, *Spyware*, *Ransomware*, *Adware* e *Botnets*.
- Injeção de SQL
- *Phishing*
- Ataques "*man-in-the-middle*"
- Ataque de negação de serviço (*Denial-of-service*, DoS/DDoS)

# Formas de proteger a informação

- Dicas de cibersegurança para proteger-se contra ataques cibernéticos:
  - Atualize seus *softwares* e os sistemas operacionais;
  - Evite usar redes *Wi-Fi* não seguras em locais públicos;
  - Não abra anexos de e-mail de remetentes desconhecidos;

# Formas de proteger a informação

- Não clique em *links* ou e-mails de remetentes desconhecidos ou em sites não familiares;
- Use um *software* antivírus;
- Use senhas fortes.

# Criptografia

# Criptografia

A criptografia tem o objetivo de garantir os princípios de segurança por meio de:

- algoritmos de encriptação e desencriptação;
- algoritmos de assinatura digital;
- algoritmos de certificado digital;
- algoritmos de hash.

# Criptografia

Criptografia deve proteger as informações:

- em repouso;
- em trânsito;
- ou em uso.

# Criptografia

Os algoritmos de encriptação podem ser agrupados em:

- Encriptação simétrica: utilizada para ocultar o conteúdo dos blocos ou fluxos contínuos de dados de qualquer tamanho:
  - Utilizando uma única chave.

- Encriptação assimétrica: usada para ocultar pequenos blocos de dados:
  - Utilizando uma chave pública e uma chave privada.

# Mecanismos de segurança

# Mecanismos de segurança

Modelo OSI específica serviços de segurança para:

- Certificado digital;
- Assinatura digital;
- Controle de acesso;
- Autenticação;
- Autorização;
- Auditoria;
- Detecção de eventos relevantes à segurança;
- Recuperação de segurança.

# Mecanismos de segurança

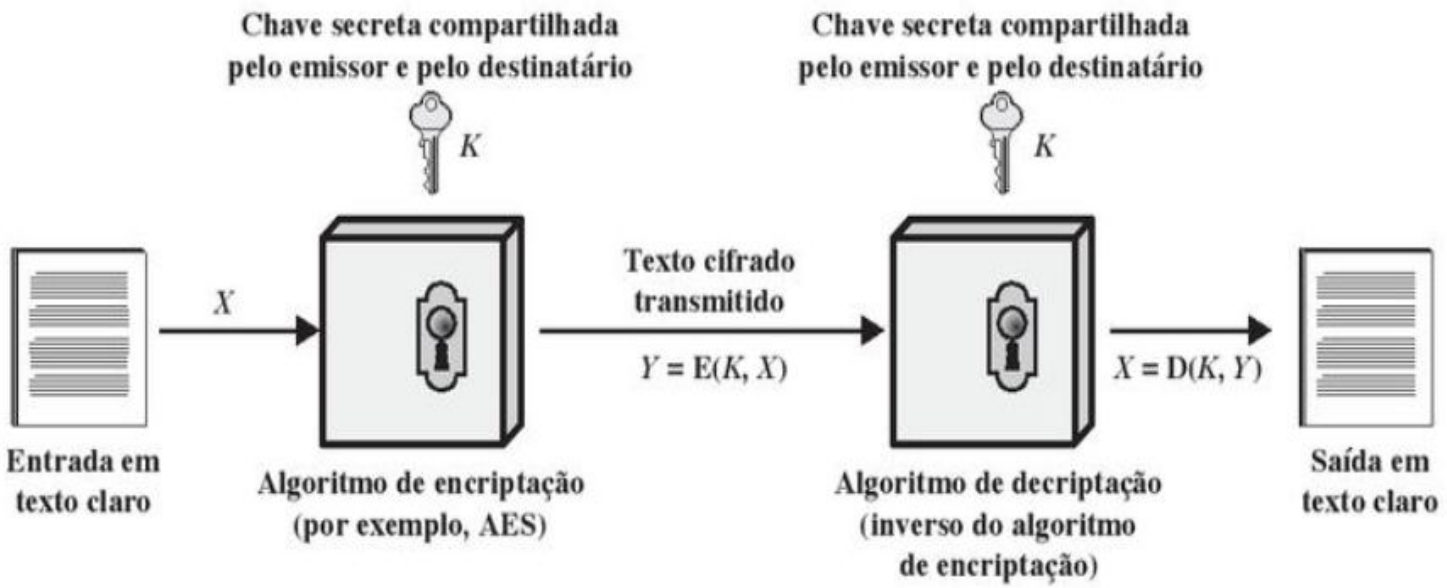
## Técnica de encriptação simétrica

Uma **única chave K** é utilizada para:

- encriptar / cifrar os dados;
- em seguida, para decripatação / decifrar os dados.

# Técnica de encriptação simétrica

## Exemplo

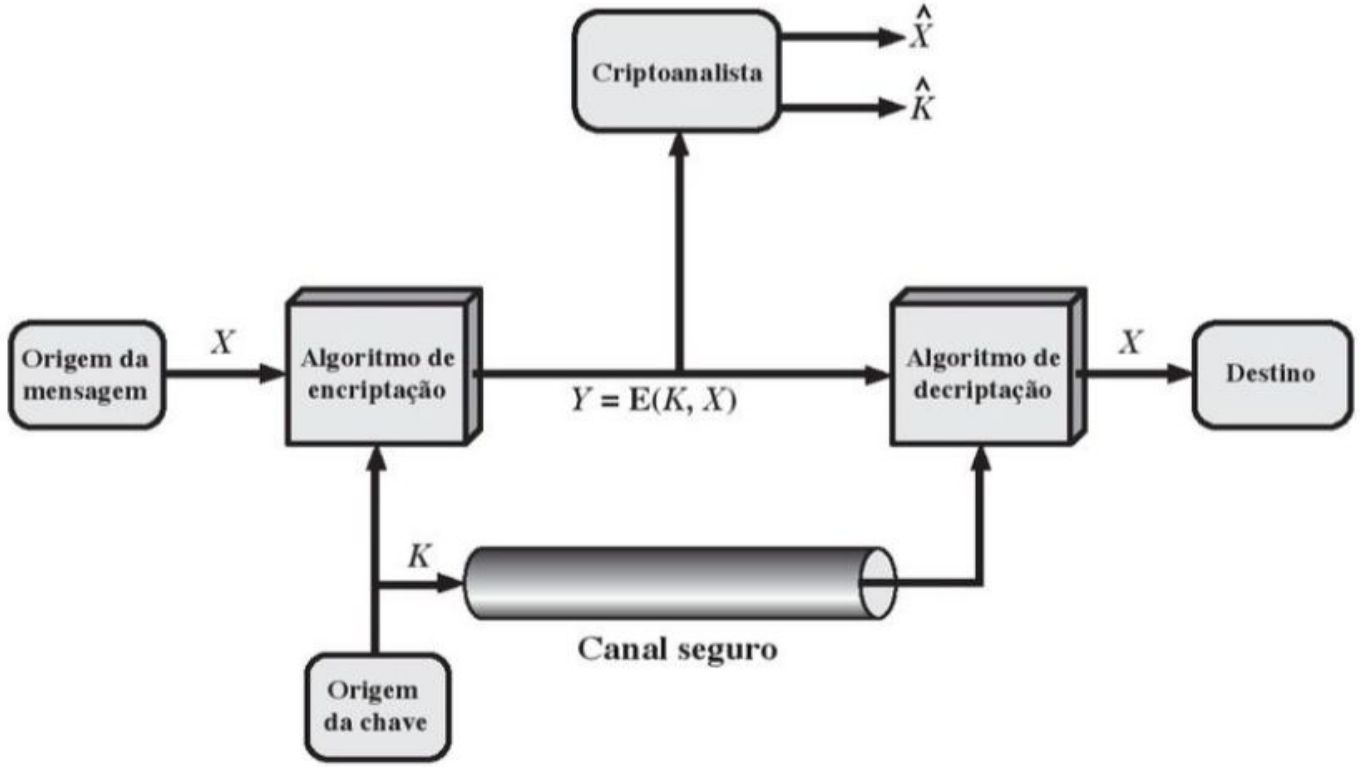



Fonte: Stallings, 2015, p. 21 (plataforma de leitura).

# Técnica de encriptação simétrica

## Canal seguro

- Deve haver um canal seguro para o transporte da chave K para utilizada no destino.




Fonte: Stallings, 2015, p. 22 (plataforma de leitura).

# Mecanismos de segurança

## Técnica de encriptação assimétrica (pública)

Os algoritmos assimétricos contam:

- Chave Pública para encriptação;
- Chave Privada (uma chave diferente) para a decriptação:
  - Diferente da pública, porém relacionada;
  - Exemplo:
    - números primos;
    - curvas elípticas.

# Técnica de encriptação assimétrica

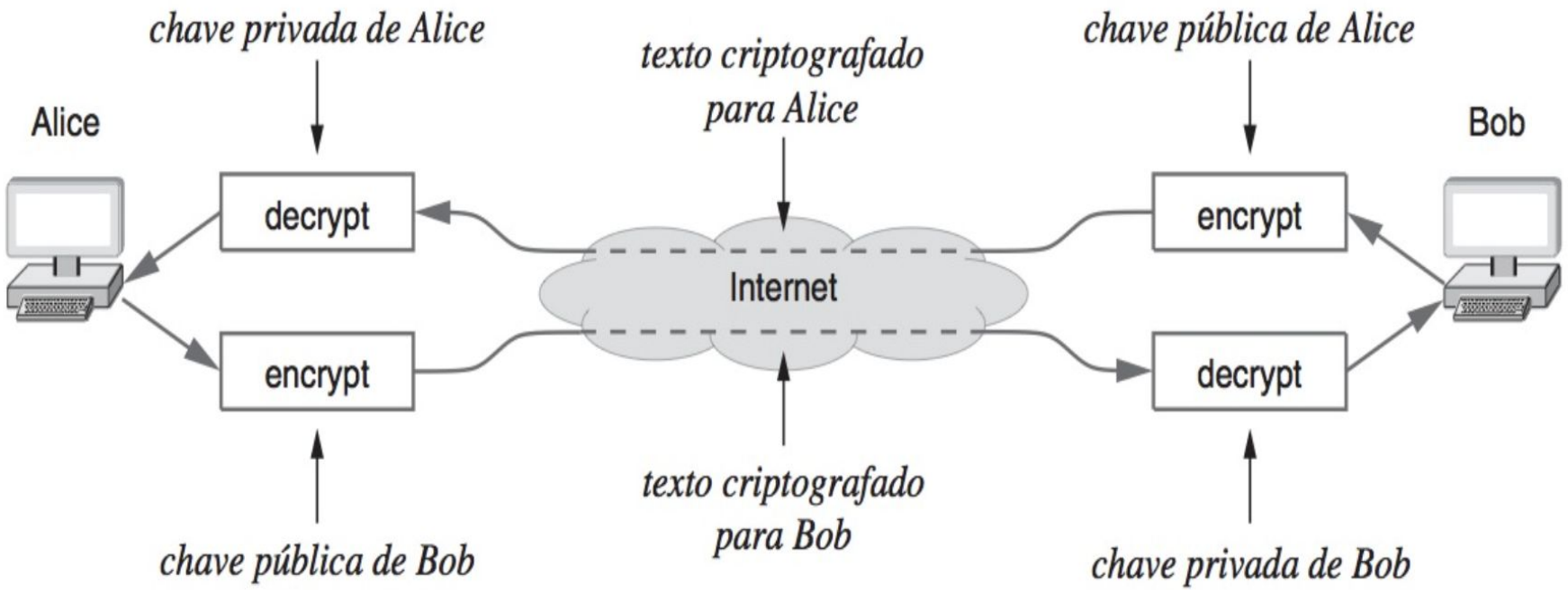
## Criptossistemas de chaves assimétricas (pública)

- Qualquer uma das duas chaves relacionadas pode ser usada para encriptação com a outra para a decriptação.

- Estabelecendo um canal seguro de comunicação entre um cliente-servidor, exemplos:
  - Aplicativos bancários na *Web;*
  - Comércio eletrônico.

# Técnica de encriptação assimétrica

## Criptossistemas de chaves assimétricas (pública)




Fonte: Comer, 2016, p. 496.

# Mecanismos de segurança

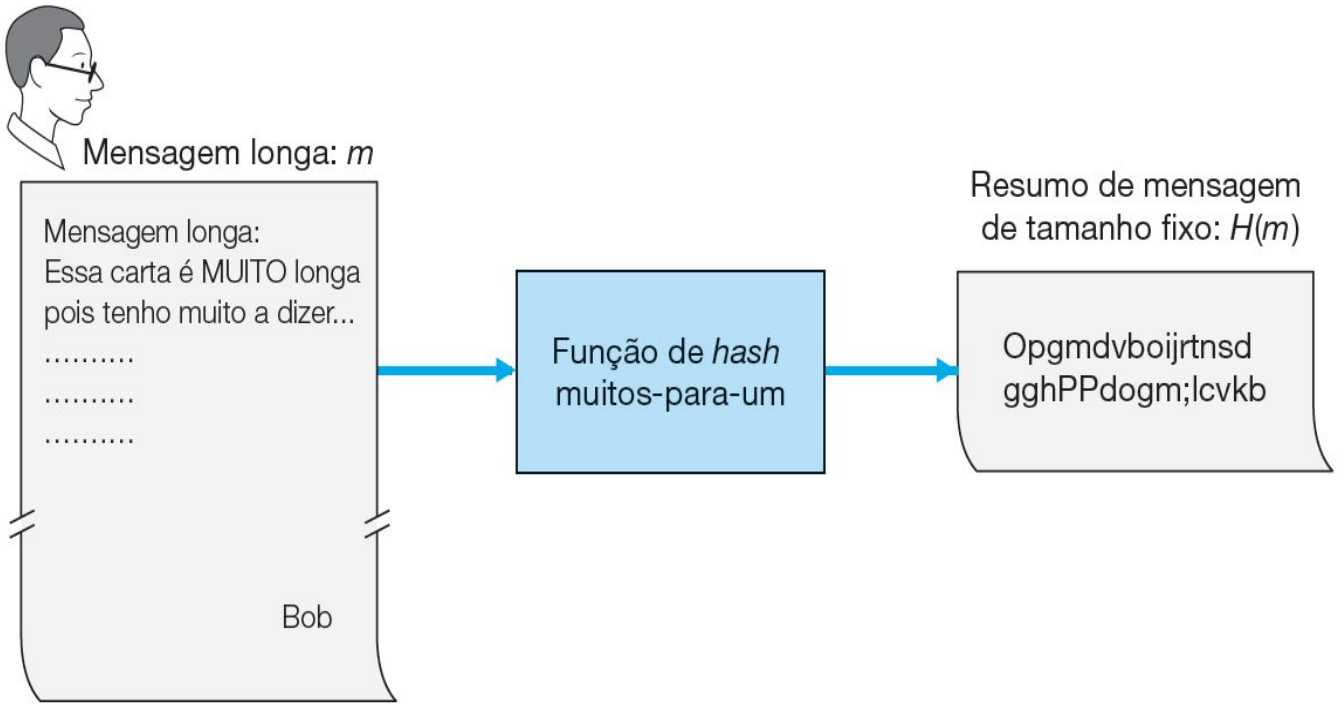
## Assinaturas digitais

A assinatura digital precisa garantir as características:

- verificar o autor, a data e hora da assinatura;
- autenticar o conteúdo no momento da assinatura;
- ser verificável por terceiros para resolver disputas.

# Assinaturas digitais

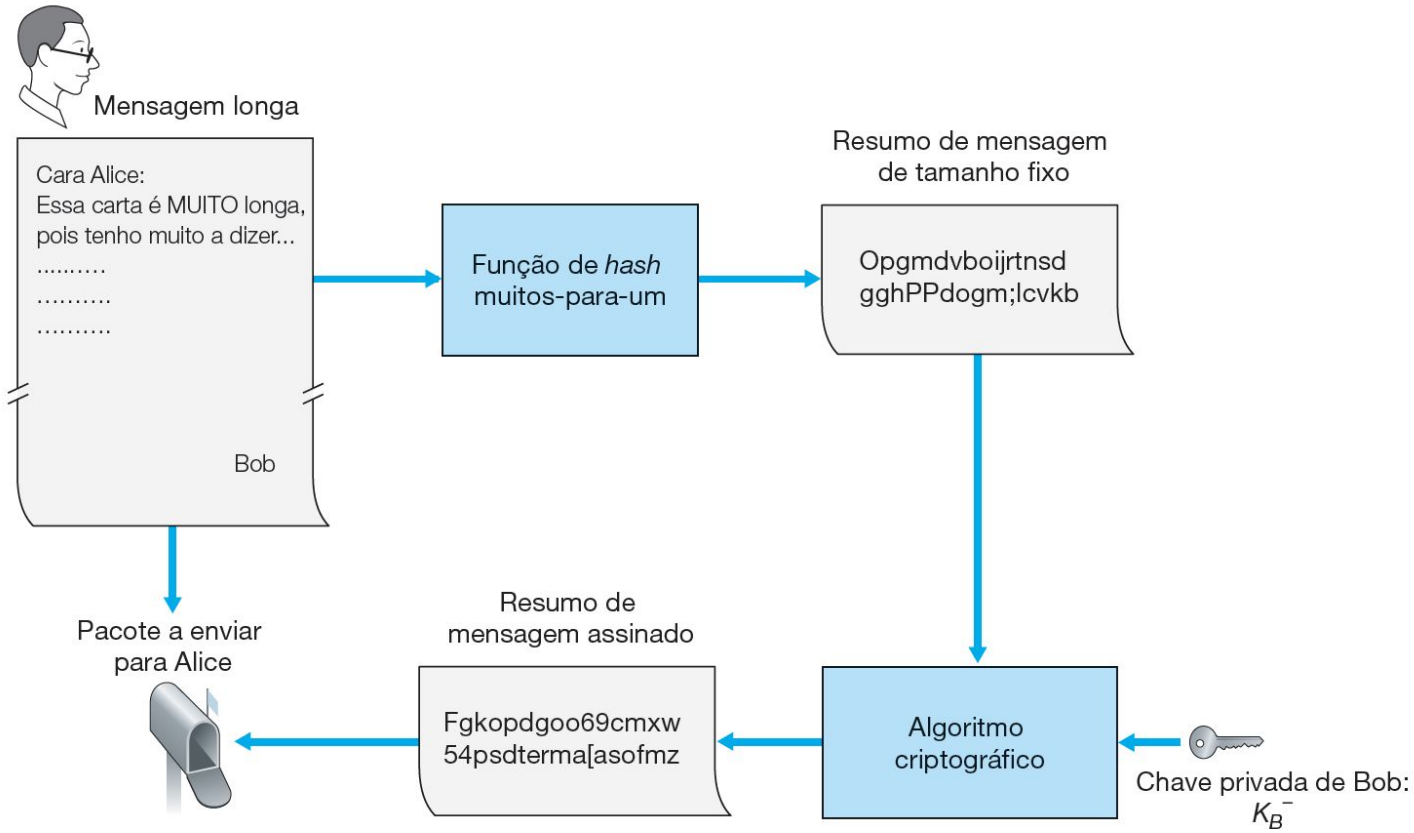
## Função HASH criptográficas




Fonte: Kurose, 2020, p. 507.

# Assinaturas digitais

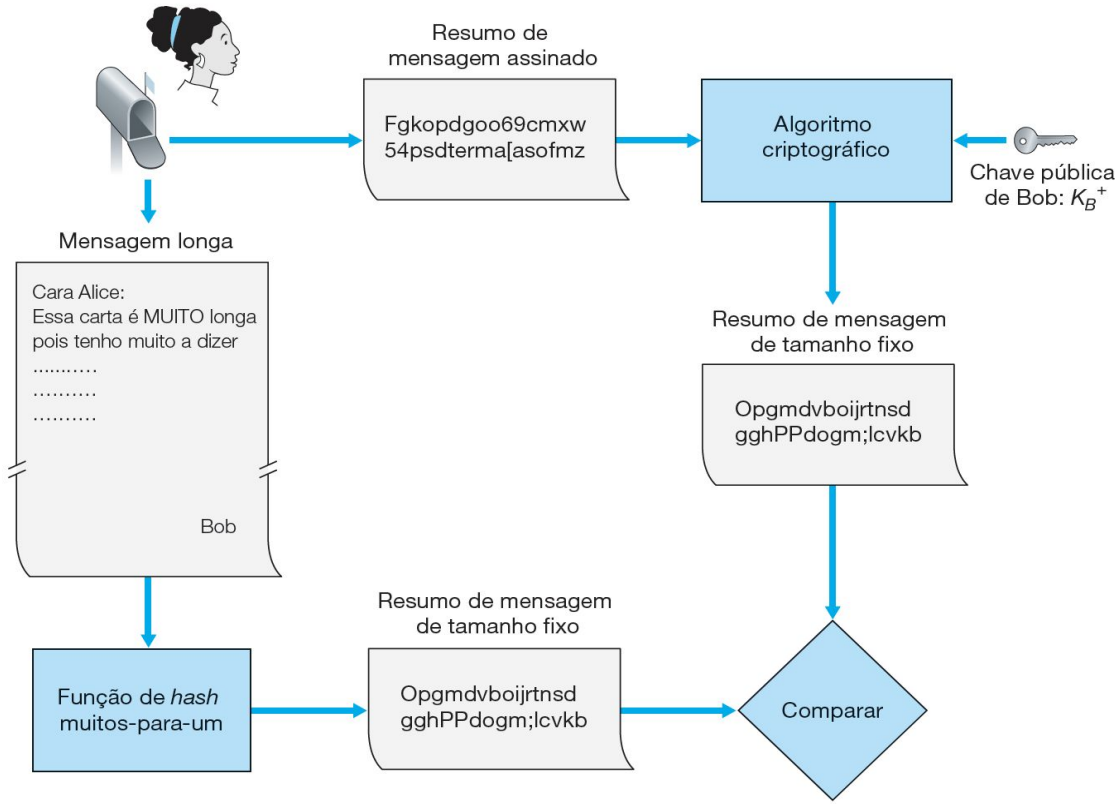
## Enviando um documento assinado digitalmente




Fonte: Kurose, 2020, p. 512.

# Assinaturas digitais

## Verificando um documento assinado digitalmente




Fonte: Kurose, 2020, p. 512.

# Assinaturas digitais

## Requisitos de assinatura digital

- Deve impedir falsificação e negação.

- É preciso ser relativamente fácil para produzir a assinatura digital, reconhecer e verificar a assinatura digital.

- É preciso ser computacionalmente inviável falsificar uma assinatura digital.

# Assinaturas digitais

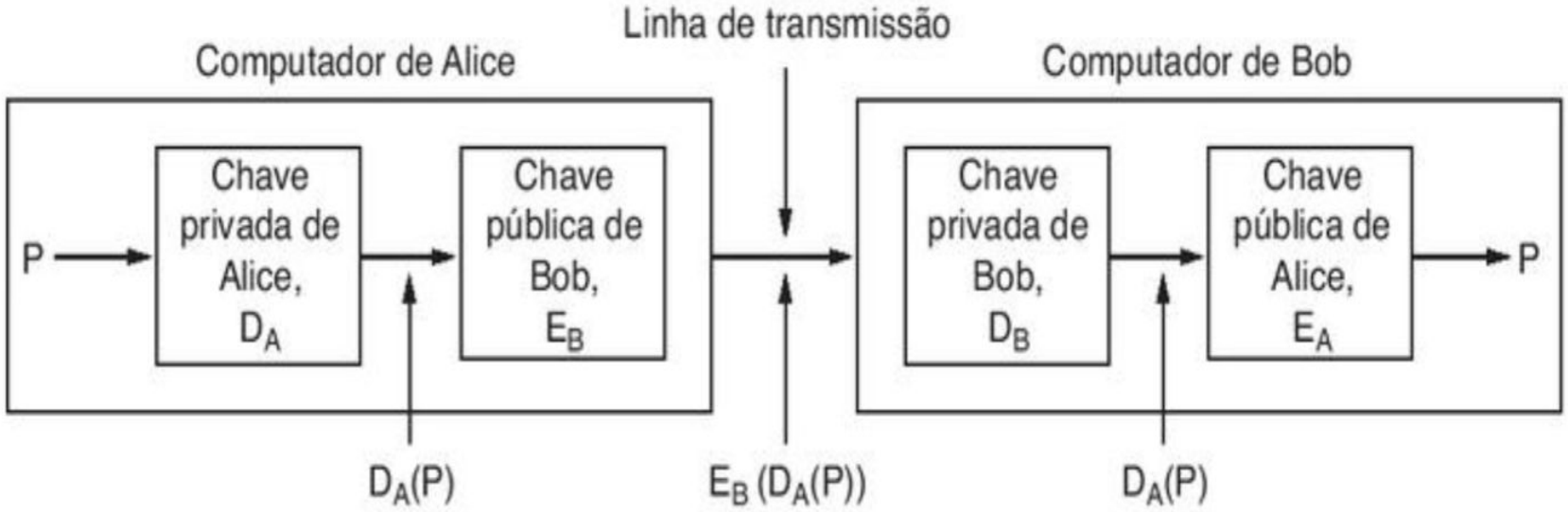
## Assinatura digital direta

Refere-se a técnica de assinatura digital que envolve apenas as partes em comunicação (origem, destino).

- Esta técnica utiliza encriptação de chaves assimétrica.

# Assinaturas digitais

## Assinatura digital direta




Fonte: Tanembaum, 2021, p. 502.

# Autenticidade

## Princípios de Autenticação de usuário remoto

A autenticação do usuário é a base para:

- Controle de acesso;
- Irretratabilidade do usuário (não repúdio).

- Definida pela RFC 4949.

# Autenticidade

## Princípios de Autenticação de usuário remoto

Autenticação é o processo de verificar uma identidade alegada por ou para uma entidade do sistema.

Um processo de autenticação consiste em duas etapas:

- Etapa de identificação;
- Etapa de verificação.

# Autenticidade

## Princípios de Autenticação de usuário remoto

As formas de autenticação da identidade de um usuário podem ser:

- Algo que o indivíduo sabe (senha, PIN);
- Algo que o indivíduo possui (*token*);
- Algo que o indivíduo é (biometria estática);
- Algo que o indivíduo faz (biometria dinâmica).

# *Firewall*

# Dispositivos de segurança

A **segurança lógica** se preocupa com os dados que trafegam na rede e provê sistemas de segurança para:

- Firewall;
- Sistemas de Detecção de Intrusos (IDS);
- Sistemas de Prevenção de Intrusos (IPS).

# Dispositivos de segurança

***Firewall***

Tem a função de autenticar e de autorizar o tráfego da rede:

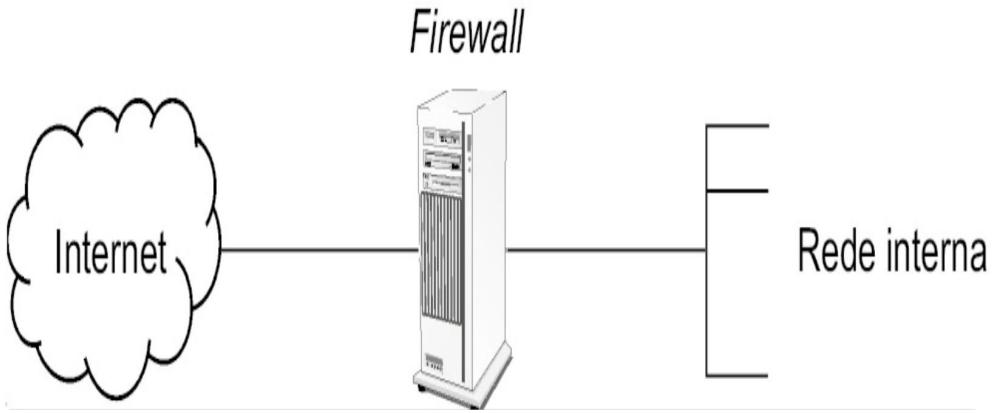
- Isola a rede interna (*intranet*) da rede externa (*internet*).
  - Basicamente filtrando o tráfego TCP/IP.
    - Por meio regras de entrada (*In*) e de saída (*Out*).

# Dispositivos de segurança

## *Firewall*

Pode ser um dispositivo do tipo:

- um servidor com função de roteador com duas placas de rede:
  - isolando uma rede da outra;
  - ou um roteador com Firewall.



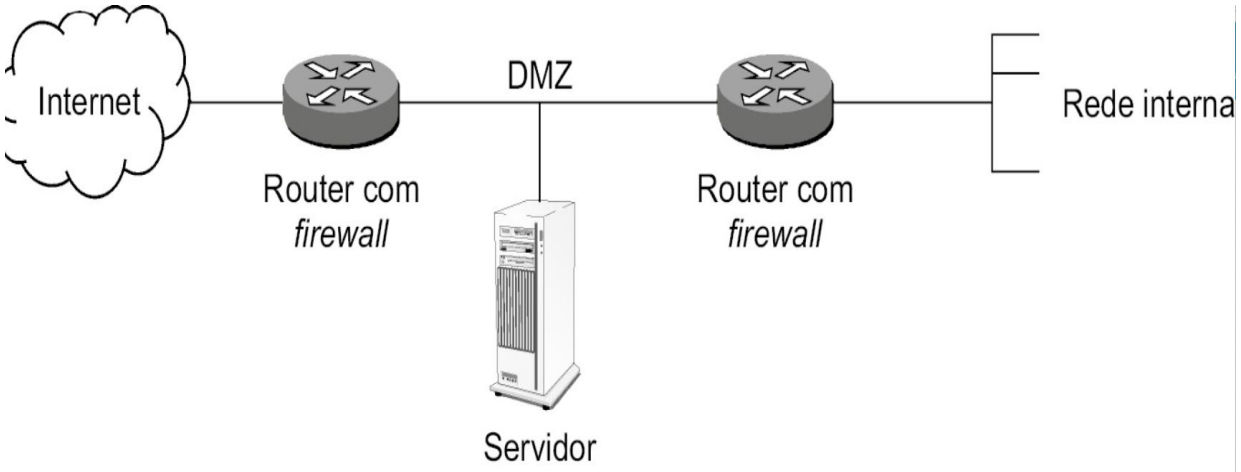

Fonte: Souza, 2020, p. 63

# Dispositivos de segurança

## *Firewall*

Analisa os cabeçalhos dos pacotes IP:

- IP de origem;
- IP de destino;
- Portas de origem;
- Porta de destino;
- Tráfego de Entrada;
- Tráfego de Saída.




Fonte: Souza, 2020, p. 64

# Dispositivos de segurança

## *Firewall*

Não analisa o conteúdo dos pacotes (dados).

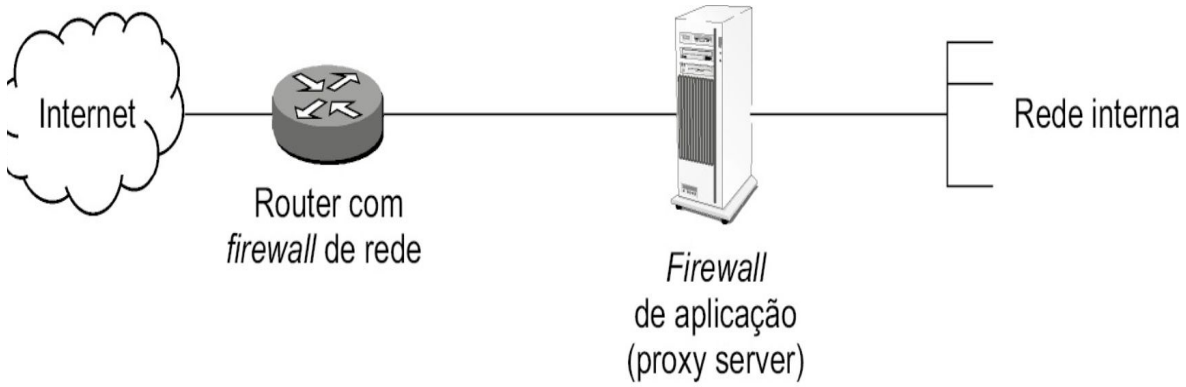
| Dir | Tipo de quadro | IP de origem | IP de destino | Tipo | Porta de origem | Porta de destino |
|---|---|---|---|---|---|---|
| In | 0x0800 | * | 192.5.48.1 | TCP | * | 80 |
| In | 0x0800 | * | 192.5.48.2 | TCP | * | 25 |
| In | 0x0800 | * | 192.5.48.3 | TCP | * | 53 |
| In | 0x0800 | * | 192.5.48.3 | UDP | * | 53 |
| Out | 0x0800 | 192.5.48.1 | * | TCP | 80 | * |
| Out | 0x0800 | 192.5.48.2 | * | TCP | 25 | * |
| Out | 0x0800 | 192.5.48.3 | * | TCP | 53 | * |
| Out | 0x0800 | 192.5.48.3 | * | UDP | 53 | * |

Fonte: Comer, 2016, p. 457

# Dispositivos de segurança

## *Firewalls* de nível de aplicação (*proxy servers*)

- Intercepta a solicitação de informação (tráfego recebido) e envia as respostas às aplicações correspondentes;
  - permite a auditoria do controle do tráfego que passa por ele.




Fonte: Souza, 2020, p. 64

# Dispositivos de segurança

## Sistemas de Prevenção de Intrusos (IPS)

- É um sistema passivo;
- Monitorar uma rede em busca de eventos que possam violar as regras de segurança dessa rede.

# Dispositivos de segurança

## Sistemas de Detecção de Intrusos (IDS)

- É sistema ativo;
- Projetado com o objetivo de bloquear automaticamente a atividade maliciosa.

⇒ como encerramento de conexão via envio de pacotes ***reset***.

# Referências


COMER, Douglas E. **Redes de computadores e internet**. Editora Bookman, 2016. **p. 444-464**. ISBN 9788582603734. Disponível na Biblioteca Digital da UFMS.

KUROSE, Jim; ROSS, Keith W. **Redes de Computadores e a Internet:** uma Abordagem Top-down, 8 Edição. Editora Pearson, 2021. ISBN: 9788582605592. **p. 493-546**. Disponível na Biblioteca Digital da UFMS.

SOUZA, Lindeberg Barros de. **Administração de redes locais**. 2. São Paulo: Érica, 2020. 1 recurso online. (Eixos). **p. 63-64.** ISBN 9788536533698. Disponível na Biblioteca Digital da UFMS.

TANENBAUM, Andrew S.; FEAMSTER, Nicholas; WETHERALL, David J.; **Redes de Computadores,** 6ª Edição. Editora Pearson, 2021. ISBN: 9788582605615. **p. 502**. Disponível na Biblioteca Digital da UFMS.

# Licenciamento