

# Ciência da Computação

## Redes de Computadores

### Aula 6

Prof. Dr. Diego R. Moraes  
[diego.moraes@docente.unip.br](mailto:diego.moraes@docente.unip.br)



# Agenda da Aula

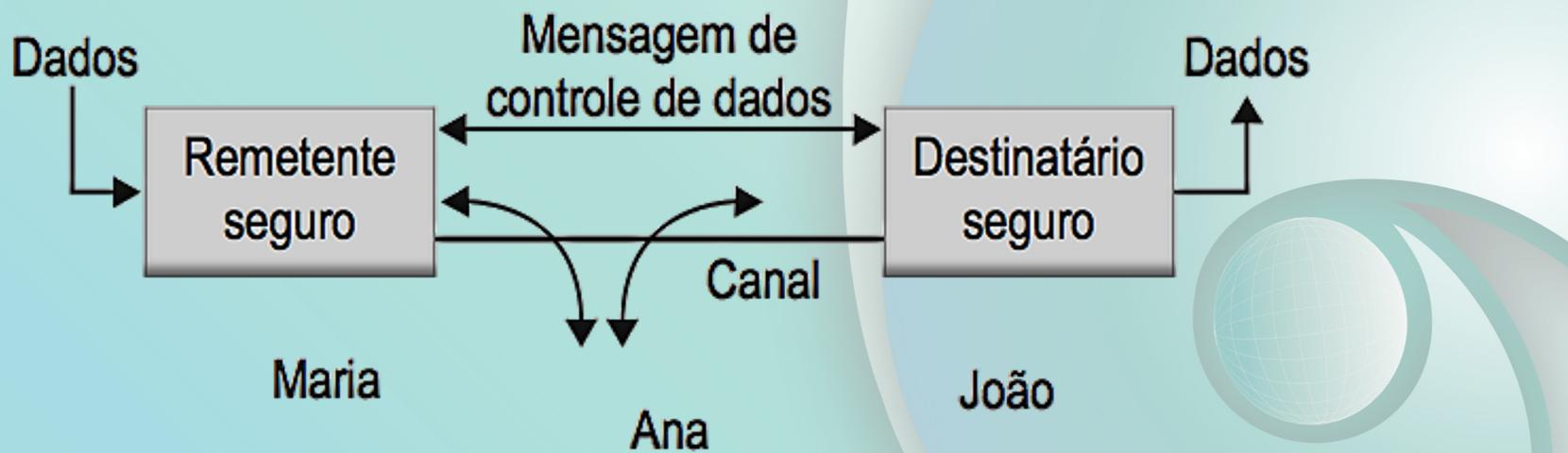
- Fundamentos de Segurança
  - Sigilo, Autenticação, Integridade e Intruso
- Criptografia
  - Chaves: simétricas, assimétricas e híbridas
- Assinatura Digital
- Hash
- Certificado Digital
- Firewall

# Introdução

- Objetivo da rede é a comunicação entre computadores
- Porém precisa ser feita de forma segura
  - Informações na internet
  - Compra e venda de mercadorias
  - Transações financeiras
- Vamos conhecer:
  - Criptografia e chaves
  - Assinatura e certificado digital
  - HTTPS; SSL; Firewalls etc

# Fundamentos de Segurança

- Comunicação segura só acontece quando nenhum **intruso** interfere na comunicação
- Ex:



- **Como garantir???**
  - Maria está se comunicando com o João.
  - João recebe a mensagem de Maria.
  - Ambos não querem alterações no conteúdo.

# Fundamentos de Segurança

- Propriedades para comunicação segura:
- **Sigilo:** mensagem deve ser disfarçada para que apenas remetente/destinatário entendam o conteúdo.
- **Autenticação:** técnica onde o processo confirma que não trata-se de um impostor/intruso.
- **Integridade:** assegurar que o conteúdo não seja alterado durante a transmissão.

# Fundamentos de Segurança

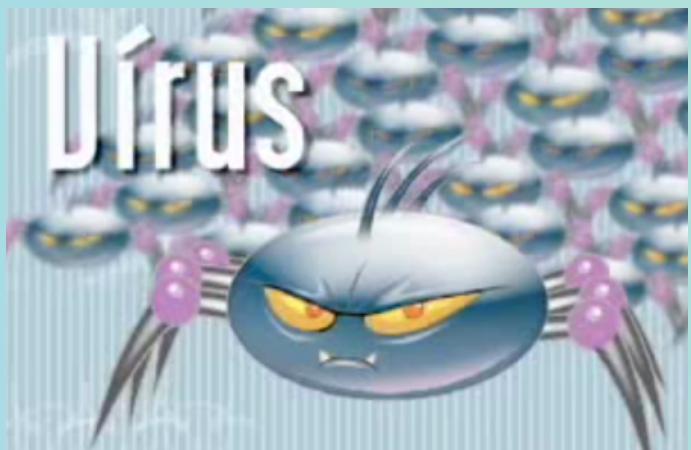
- **Intruso:** Indivíduo que age numa rede de forma indesejada. Várias formas:
  - **Intruso passivo:**
    - Ouvir e gravar mensagens do canal
  - **Intruso ativo:**
    - Remover ou adicionar mensagens do canal
- **Como é possível?**
  - **Analisador de pacotes (packet sniffer):**
    - Lê mensagens na rede analisando os quadros
    - BEM (administrador procurando erro na rede)
    - MAL (roubar informações sigilosas)

# Fundamentos de Segurança

- **Como aumentar a segurança?**
  - Existem vários métodos e técnicas
  - O mais comum é a **criptografia**
    - Escrever em código (esconder informação)
    - Inverso (recuperar informação original)
    - Utiliza a própria informação mais uma **chave**
      - Caracteres (números e letras)
      - Embaralhando os dados

# Segurança na internet: Os Invasores

Duração: 0'18" – 5'13"



C - 1429

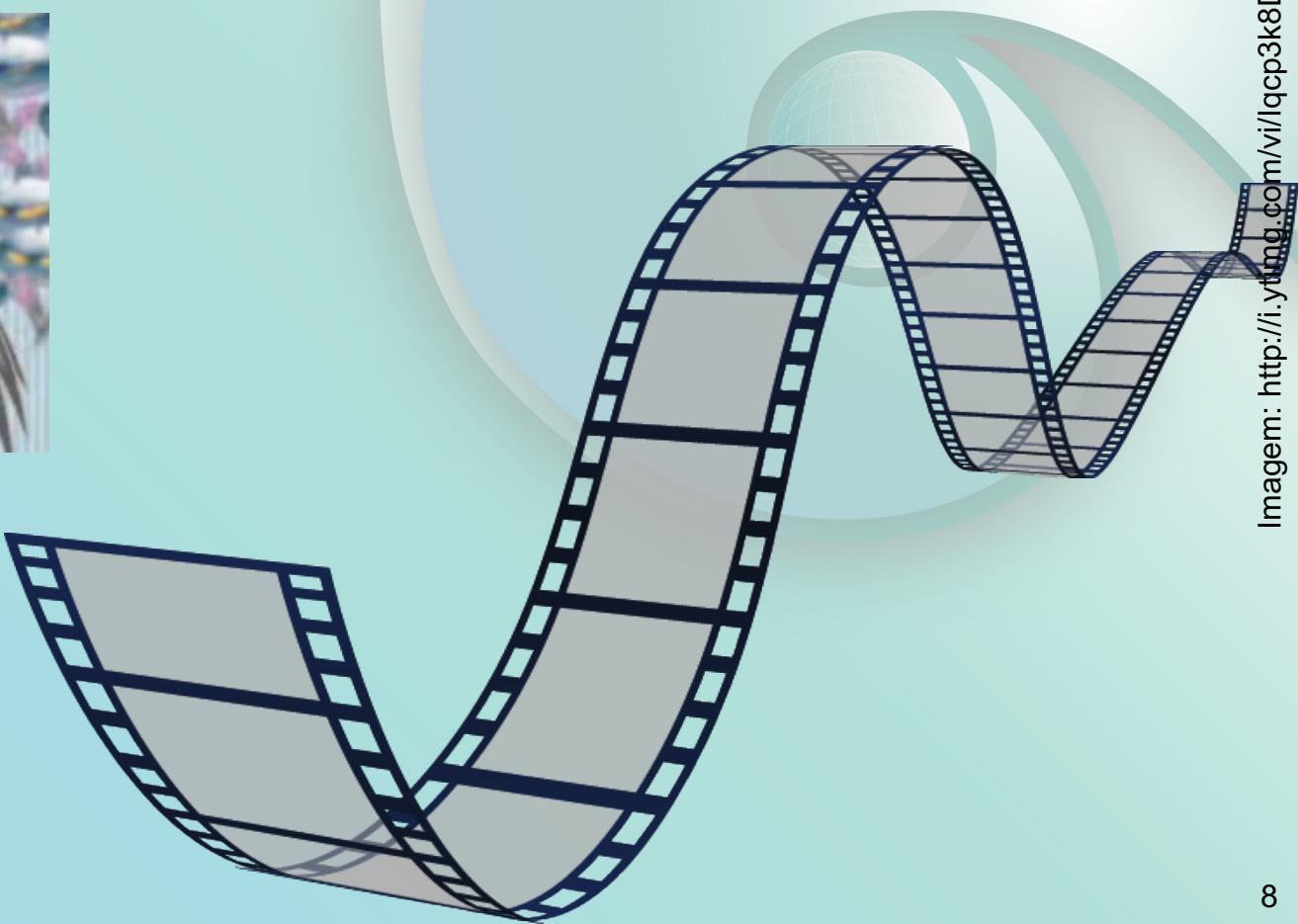


Imagen: <http://i.ytimg.com/vi/lqcp3k8DgGw/mqdefault.jpg>

# Criptografia

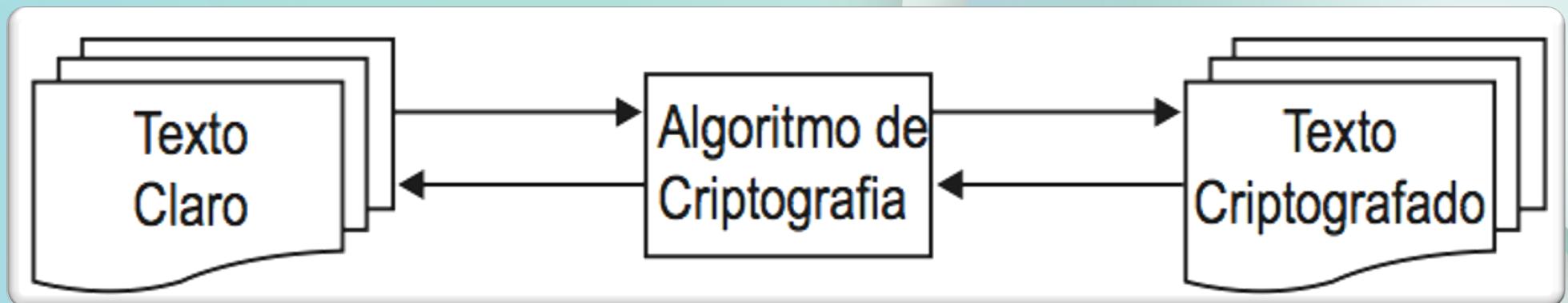
## O que é criptografia?

- Conjunto de métodos e técnicas para codificar uma informação
- Utiliza um algoritmo para:
  - **Criptografar:**
    - Converte dados legíveis em ilegíveis
    - Fora do padrão conhecido
  - **Descriptografar:**
    - Processo inverso (recuperar original)



# Criptografia

- **Esquema para criptografar texto**



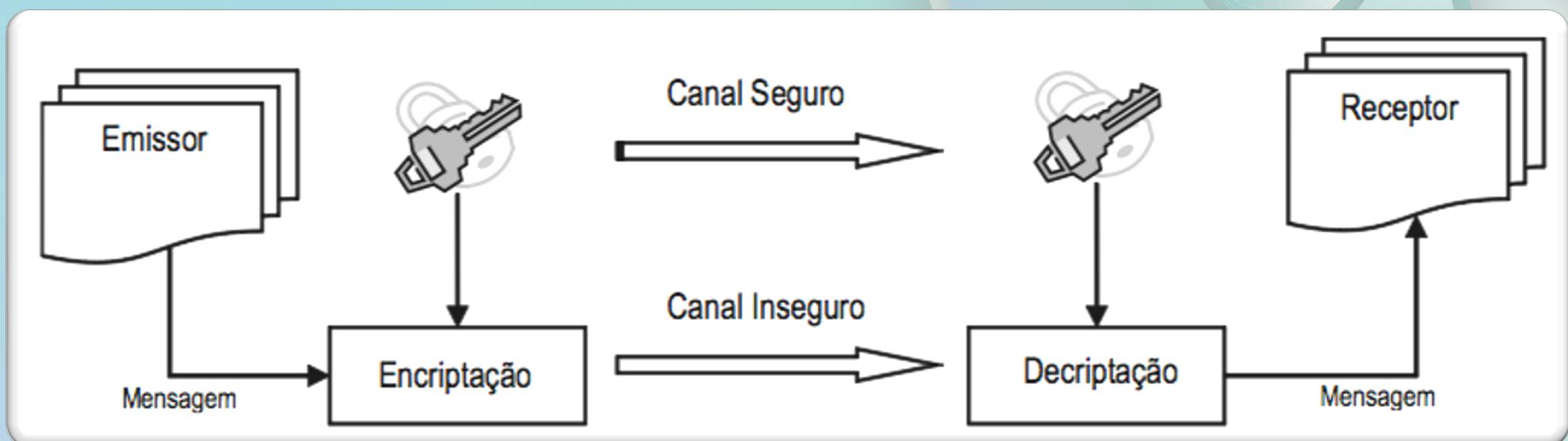
- É tão antigo quanto a escrita
  - Egípcios: escrita hieroglífica (desenhos)
  - Romanos: códigos secretos (estratégia de guerra)

# Termos oficiais em criptografia

- **Encriptar:** transforma legível em ilegível
- **Descriptar:** inverso da encriptação
- **Algoritmo criptográfico:** função matemática utilizada para encriptar/descriptar
- **Chave criptográfica:** parâmetro (caracteres) utilizado pelo algoritmo. Chave maior é mais difícil de ser quebrada, porém NÃO é impossível

# Chave Simétrica e Assimétrica

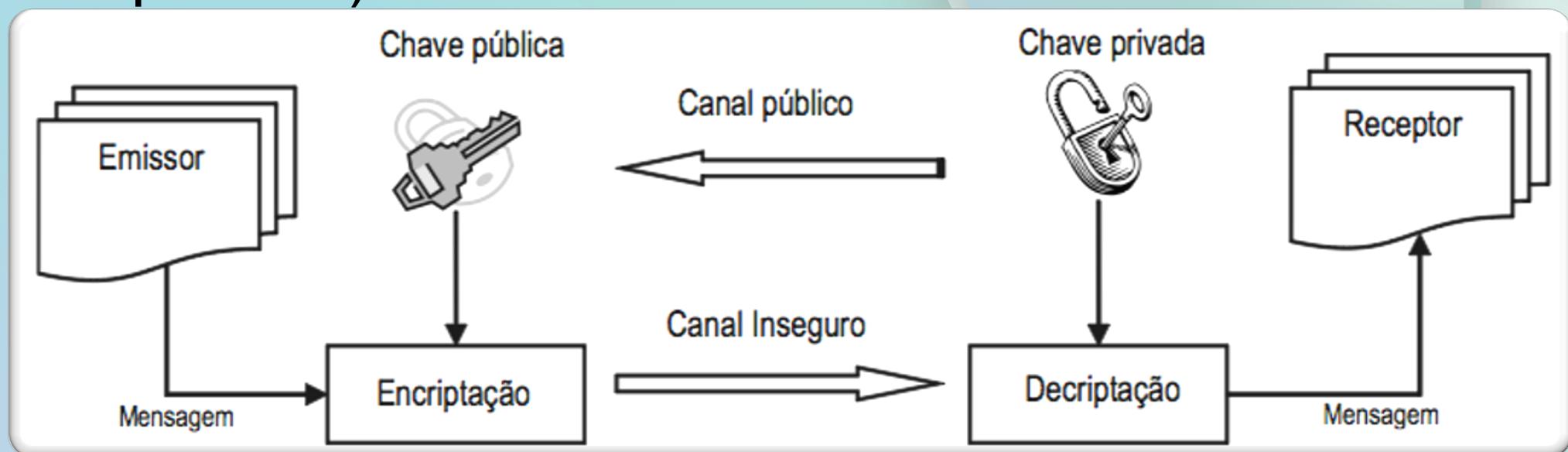
- **Chave Simétrica:**
  - Utiliza 1 única chave (encriptar / decriptar)
  - Vantagem:
    - Algoritmos mais simples, portanto mais rápido
  - Desvantagem:
    - Menos seguro, pois todos tem acesso a chave



# Chave Simétrica e Assimétrica

- **Chave Assimétrica:**

- Utiliza 2 chaves geradas juntas (matematicamente)
  - Pública: divulgada (emissor → encriptar)
  - Privada: em segredo (receptor → decriptar)
- Vantagem:
  - Qualquer um pode encriptar (chave pública)
  - Apenas quem possui pode decriptar (chave privada)

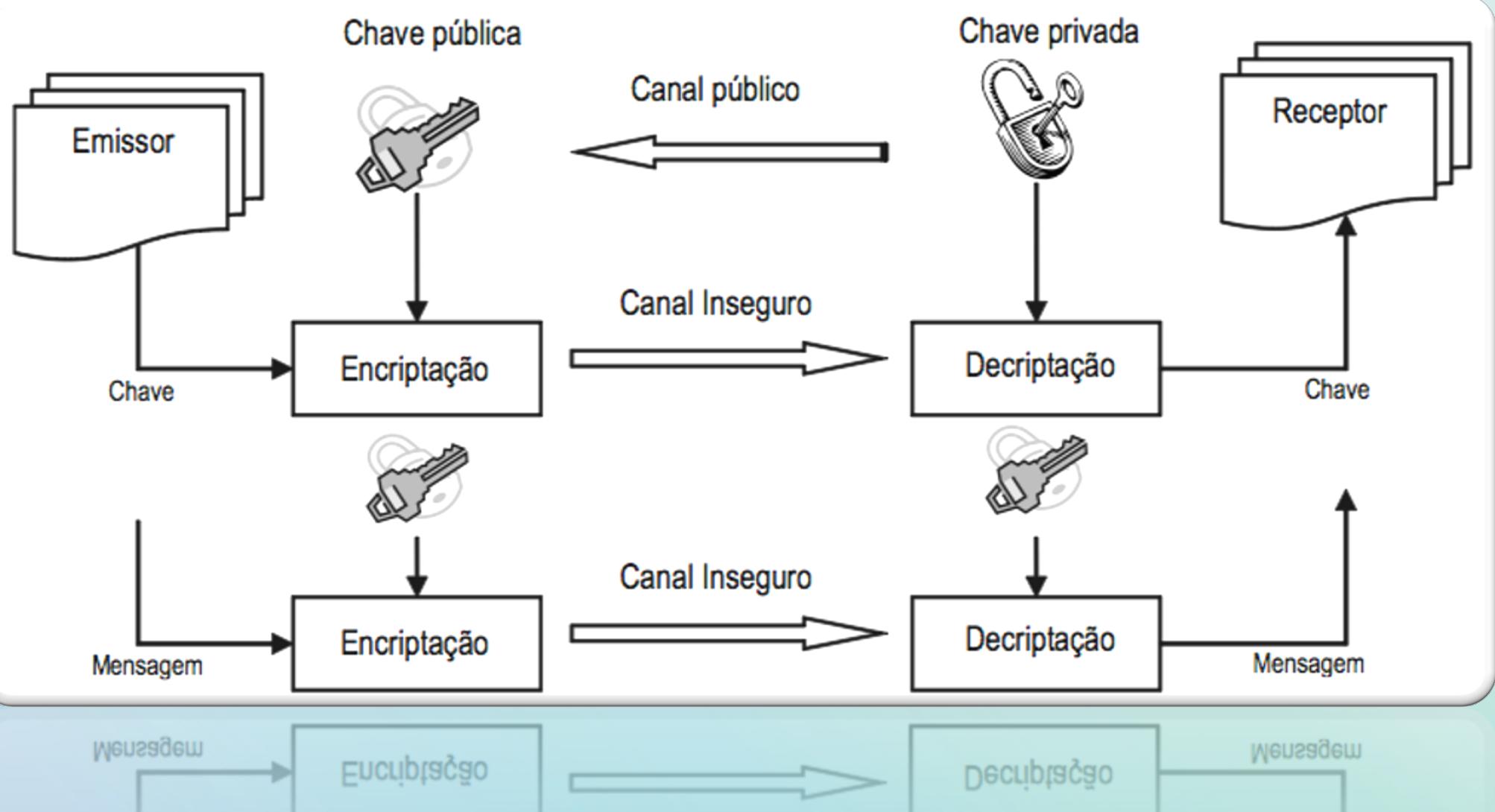


# Chave Simétrica e Assimétrica

- **Chave Híbrida:**
  - Visa alcançar as vantagens de ambas
    - **Emissor:**
    - Um **Algoritmo assimétrico** utiliza a **chave pública** para encriptar uma **chave aleatória**, que será utilizada por um **algoritmo simétrico** para encriptar a mensagem
    - **Receptor:**
    - descripta a chave com **algoritmo simétrico** e depois utiliza para decriptar a mensagem com uma **chave privada** de um **algoritmo assimétrico**

# Chave Simétrica e Assimétrica

- **Chave Híbrida:**
  - Visa alcançar as vantagens de ambas



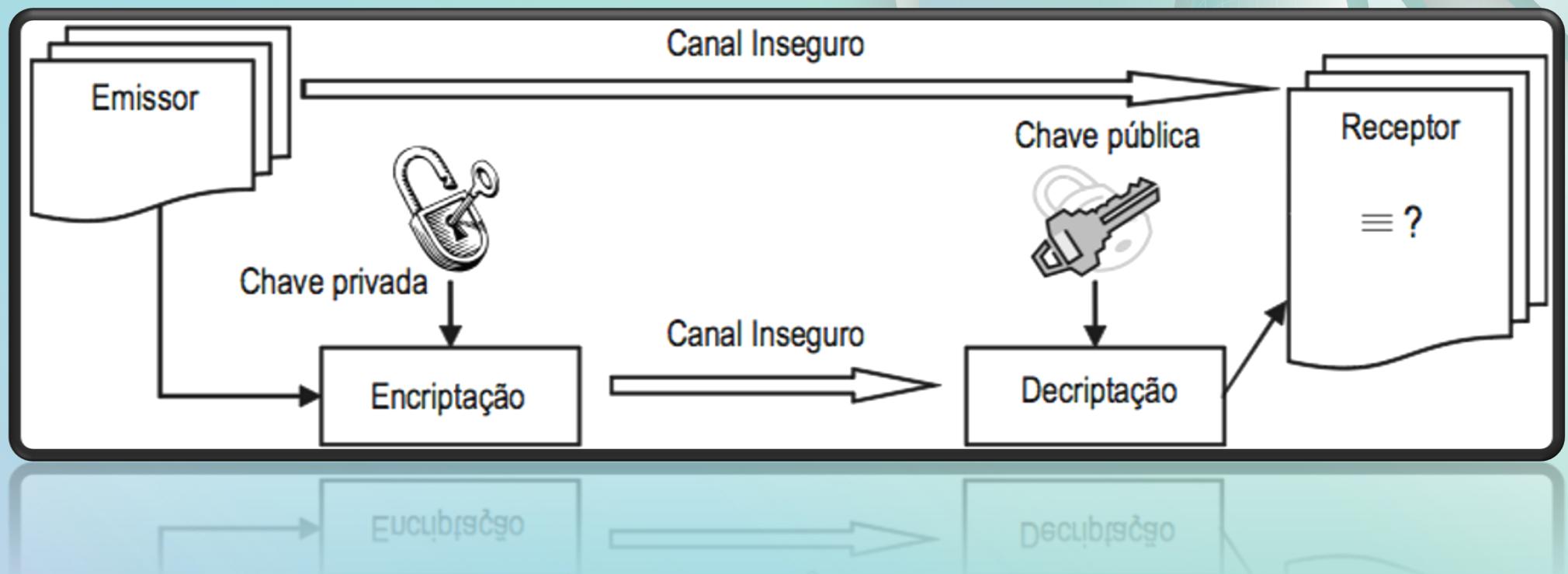
# Assinatura Digital

- **O que é assinatura digital (criptograma)?**
- Metodologia com algoritmos inversos
- Encripitar com chave privada
- Decriptitar com chave pública
  - **Desvantagem:**
  - Não garante o sigilo na mensagem, pois para decriptar usa a chave pública
- **Vantagem:**
- Garante que o emissor é autêntico pois utilizou a chave privada



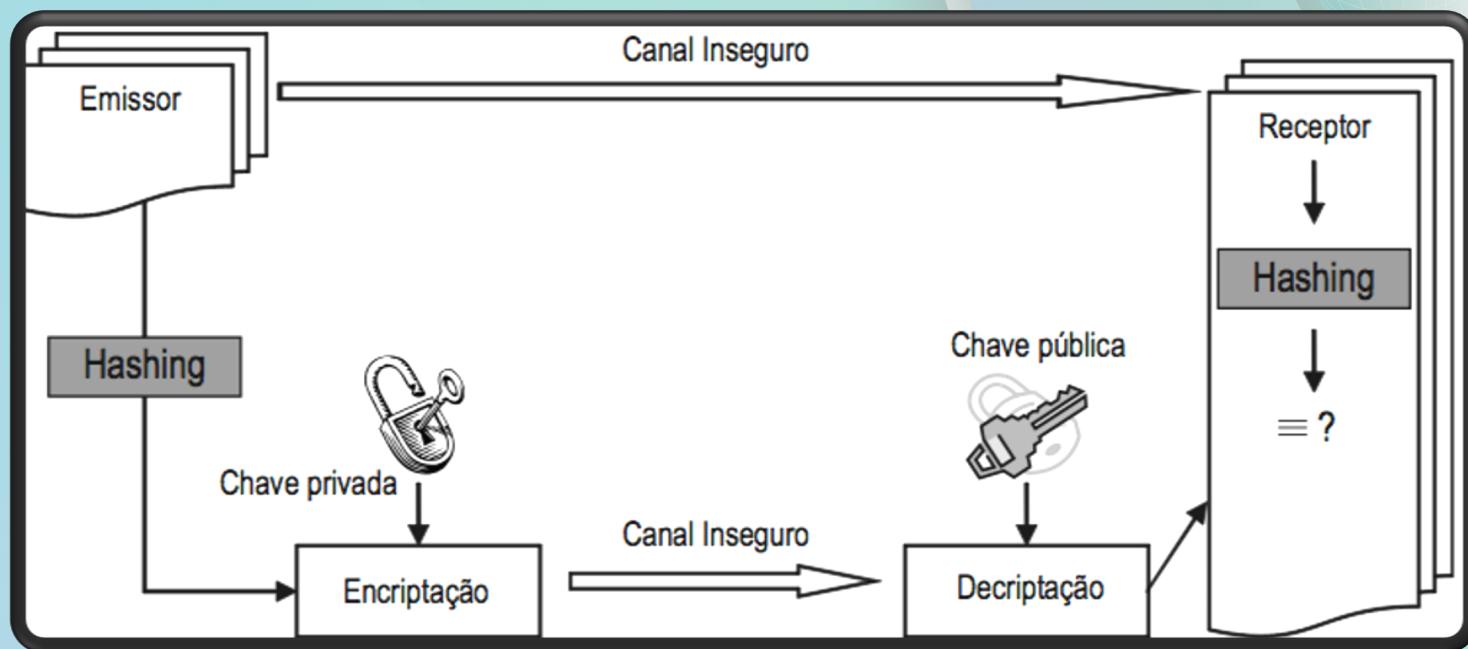
# Assinatura Digital

- Criptografia de um documento utilizando a chave privada do assinante
- Garante a identidade do emissor e que não foi alterado o documento após a assinatura



# Hash

- **Assinatura digital:**
  - Na prática é diferente pois:
  - Não aplica no documento todo
  - Mas sim numa parte dele (resumo)
  - Obtido pela função *hashing*, com a saída de tamanho fixo independente do tamanho da mensagem.



# Aplicações

- **Assinatura digital:** Existem várias aplicações
  - Assinatura de documento
    - Garante que um documento eletrônico foi emitido por um órgão ou empresa, comprovando sua autenticidade
  - Autenticidade de páginas na internet
    - Garante que uma página seja quem ela diz ser
    - Lojas virtuais, bancos e órgãos governamentais

# Certificados Digitais

- **Assinatura digital:**
  - É uma assinatura digital válida que possa ser comprovada por uma Autoridade Certificadora
  - ICP-Brasil (Infraestrutura de Chaves Públicas Brasileiras)
    - Homologa as entidades emissoras de assinaturas digitais
    - Criada 1 vez para cada pessoa/empresa
    - A1: validade de 1 ano e armazena no computador
    - A3: validade de 3 anos e armazena cartão/ token

# Firewalls

## O que é firewall?

- É um roteador interligando duas redes
- Filtra o que pode ou não passar entre elas
- Ideia original: Isolar a rede interna da internet
  - Analisa os cabeçalhos dos pacotes IP
  - Descobre os protocolos e portas
  - Compara com as regras
  - Permitido
  - Recusa (deny) ou Descarta (drop)



# Firewalls

## O que é firewall DMZ (Rede Desmilitarizada)?

- Implementa-se 2 firewalls:
  - Externo
  - Interno
- Externo (mais comum):
  - Isolar a rede interna da internet
- Interno:
  - Isolar os servidores da rede interna
  - Para evitar ataques internos



# Firewalls

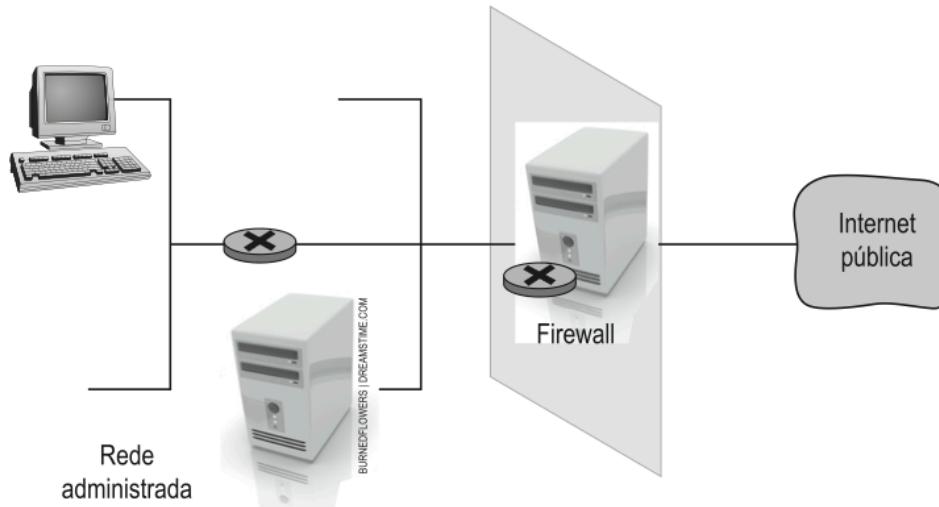


Figura 34 – Firewall.

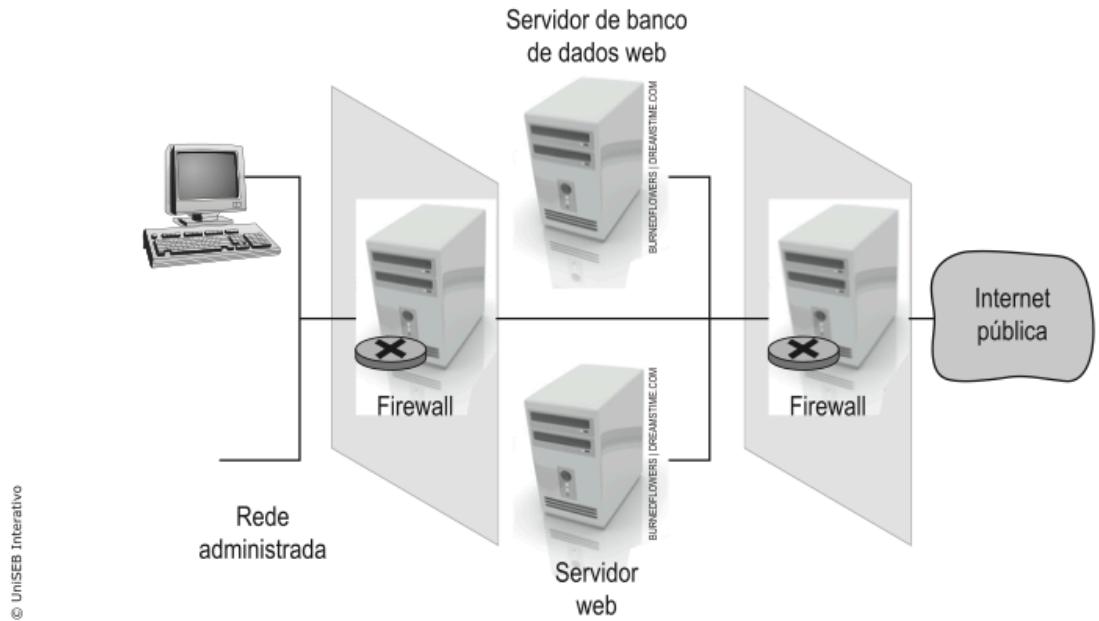


Figura 35 – Firewalls com DMZ.

Fonte: adaptado de Kurose (2003).

# Filtragem de conteúdo

- Firewalls não analisam os conteúdos (dados)
- Interessante maior controle sobre conteúdo
  - Bloquear: sexo, pedofilia, downloads etc
  - Vírus através de e-mails
- Maioria das ameaças chegam por eles
- Filtrar por:
  - Assuntos, palavras-chaves e conteúdos
  - Anexos, executáveis, scripts etc

# Ciência da Computação

## Redes de Computadores

### Aula 7

Prof. Dr. Diego R. Moraes  
[diego.moraes@docente.unip.br](mailto:diego.moraes@docente.unip.br)



# Exercício 1/3

Responda SIM ou NÃO

- 1) O documento assinado eletronicamente é reconhecido da mesma forma que um documento assinado de forma manuscrita?



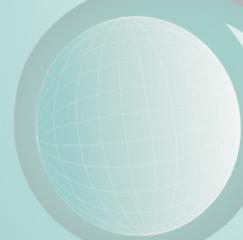
# Resposta 1/3

- 1) O documento assinado eletronicamente é reconhecido da mesma forma que um documento assinado de forma manuscrita?
- RESPOSTA: **SIM**
- (art. 10, da MP n° 2.200)
- Documentos eletrônicos assinados digitalmente por meio de certificados emitidos fora do âmbito da ICP-Brasil também têm validade jurídica, mas esta dependerá da aceitação de ambas as partes, emitente e destinatário, conforme determina a redação do § 2º do art. 10 da MP n° 2.200-2.

# Exercício 2/3

Responda SIM ou NÃO

- 2) A assinatura digital confere sigilo ao documento eletrônico?



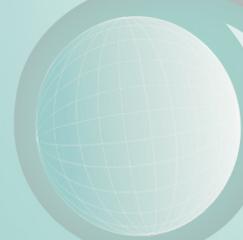
## Resposta 2/3

- 2) A assinatura digital confere sigilo ao documento eletrônico?
- RESPOSTA: NÃO
- A assinatura digital NÃO torna o documento eletrônico sigiloso, pois ele em si não é criptografado.
- O sigilo do documento eletrônico poderá ser resguardado mediante a cifragem da mensagem com a chave pública do destinatário, pois somente com o emprego de sua chave privada o documento poderá ser decifrado.
- Já a integridade e a comprovação da autoria são características primeiras do uso da certificação digital para assinar.

# Exercício 3/3

Responda SIM ou NÃO

- 3) Assinatura digital é o mesmo que assinatura digitalizada?



## Resposta 3/3

- 3) Assinatura digital é o mesmo que assinatura digitalizada?
- RESPOSTA: NÃO
- A assinatura digitalizada é a reprodução da assinatura de próprio punho como imagem por um equipamento tipo scanner.
- Ela não garante a autoria e integridade do documento eletrônico, portanto não existe uma associação inequívoca entre o assinante e o texto digitalizado, uma vez que ela pode ser facilmente copiada e inserida em outro documento.