



**LUIZ GONZAGA FONSECA MOTA**  
ESCOLA ESTADUAL DE EDUCAÇÃO PROFISSIONAL



# Infraestrutura de Redes de Computadores

## Introdução à Segurança de Redes



## Sumário

- O que é segurança de Redes?

Ameaças

Tipos de Ataques

- Princípios da Criptografia

Sistemas de Segurança


Segurança em Redes sem Fio



## O que é segurança de Redes ?

Segurança de redes é a reunião de ferramentas, protocolos, tecnologias e rotinas configuradas para frear, impedir ou barrar ameaças, vulnerabilidade dos dados e também acessos indesejados ou não permitidos.

A segurança de redes é uma das atividades mais importantes da área da tecnologia da informação por garantir a proteção de qualquer rede contra os diversos tipos de ataques cibernéticos, a instabilidade de dados e o acesso não autorizado.



# Exemplos atuais de vulnerabilidades nas redes



**CNN BRASIL** ASSISTA AGORA **AO VIVO**

## Casa Branca: Mísseis da Coreia do Norte são financiados por ataques cibernéticos

Segundo um funcionário da Casa Branca, metade do valor para bancar o programa vem de ações como roubo de criptomoedas

[INÍCIO](#) > [NOTÍCIAS](#) > [BRAZIL](#)

## Contratada pelo governo britânico, empresa é atacada e perde £20 milhões

Grupo Capita, um dos principais fornecedores das autoridades do país, sofre ataque cibernético e divulga valor do prejuízo



**DEFESA EM FOCO**

equipe forças armadas bids concurso público geopolítica meio acadêmico segurança pública

Cibersegurança

## Estudo aponta que digitalização dos negócios amplia superfícies de ataque cibernético

Por Redação Defesa em Foco - 11 de maio de 2023 07:59



**OLHAR DIGITAL** NOTÍCIAS VÍDEOS EDITORIAS SUPORTE OD SEGURANÇA OFERTAS

Olhar Digital > Segurança e Privacidade > Brasil é o principal alvo de ataques cibernéticos na América Latina

SEGURANÇA E PRIVACIDADE


## Brasil é o principal alvo de ataques cibernéticos na América Latina

Os principais setores atingidos pelos ataques cibernéticos foram as operações de telecomunicação com e sem fio

Por Vitoria Lopes Gomez, editado por Rodrigo Mozelli | © 20/04/2023 22h02, atualizada em 21/04/2023 20h54

# Exemplos atuais de vulnerabilidades nas redes

## Principais Ataques na Rede

- Personificação (masquerade)
  - DDos (Cavalo de Troia)
  - Phishing
  - Backdoor
  - Engenharia social
  - Ransomware
- 


Como resolvemos esse problema?

- Princípios de Criptografia
- Integridade das Mensagens e Assinaturas Digitais
- Autenticação

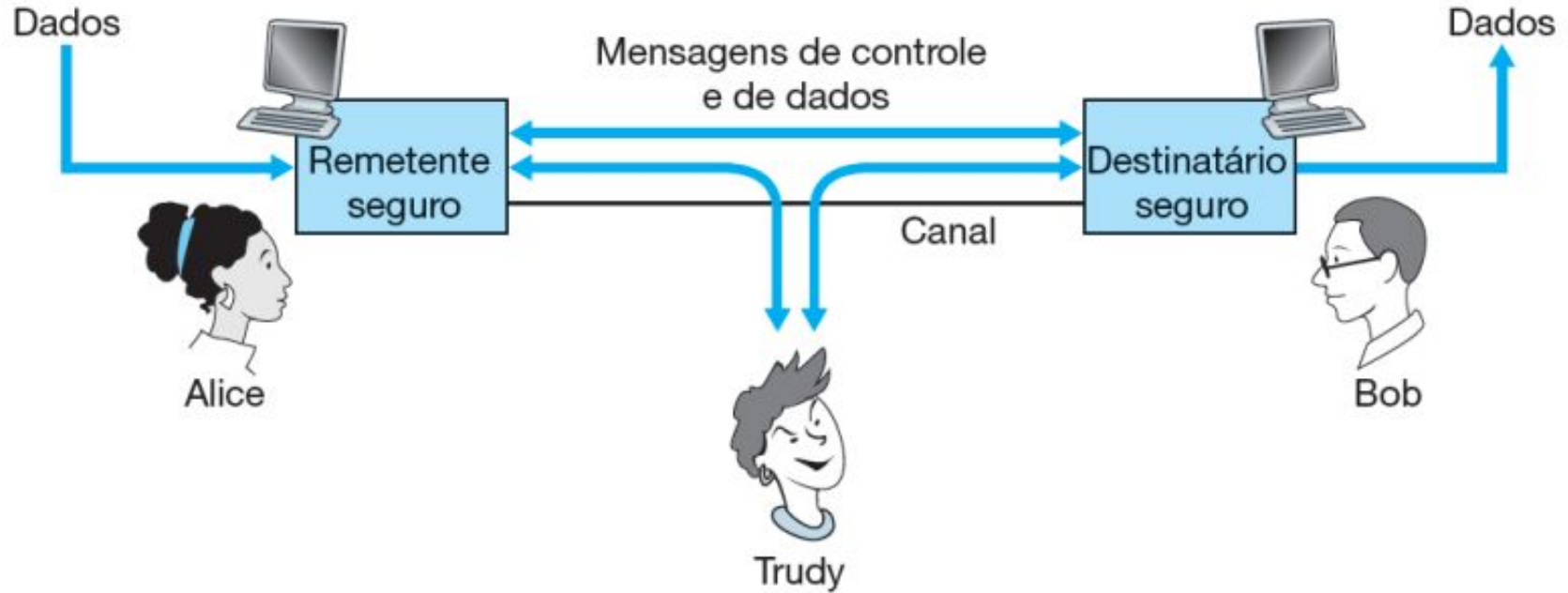


## Como resolvemos esse problema?

Criptografia é a prática de proteger informações por meio do uso de algoritmos codificados, hashes e assinaturas. As informações podem estar em repouso (como um arquivo em um disco rígido), em trânsito (como comunicação eletrônica trocada entre duas ou mais partes) ou em uso (durante a computação de dados).



# Exemplos de Criptografia





# Princípios da criptografia

Podemos identificar as seguintes propriedades desejáveis da comunicação segura:

- Confidencialidade
- Integridade de mensagem
- Autenticação do ponto final
- Segurança operacional



# Exemplos de Criptografia

**Confidencialidade:** apenas o transmissor e o receptor desejado devem “entender” o conteúdo da mensagem

transmissor codifica msg

receptor decodifica msg

**Integridade de mensagem:** transmissor e receptor querem garantir que a mensagem não seja alterada (em trânsito ou após) sem que isto seja detectado.

**Autenticação do ponto final:** transmissor e receptor querem confirmar a identidade um do outro.

**Segurança operacional:** os serviços devem estar acessíveis e disponíveis para os usuários (detecção de invasão, worms, firewalls, Internet pública...).



# Exemplos de Criptografia

**Confidencialidade:** apenas o transmissor e o receptor desejado devem “entender” o conteúdo da mensagem

transmissor codifica msg

receptor decodifica msg

**Integridade de mensagem:** transmissor e receptor querem garantir que a mensagem não seja alterada (em trânsito ou após) sem que isto seja detectado.

**Autenticação do ponto final:** transmissor e receptor querem confirmar a identidade um do outro.

**Segurança operacional:** os serviços devem estar acessíveis e disponíveis para os usuários (detecção de invasão, worms, firewalls, Internet pública...).



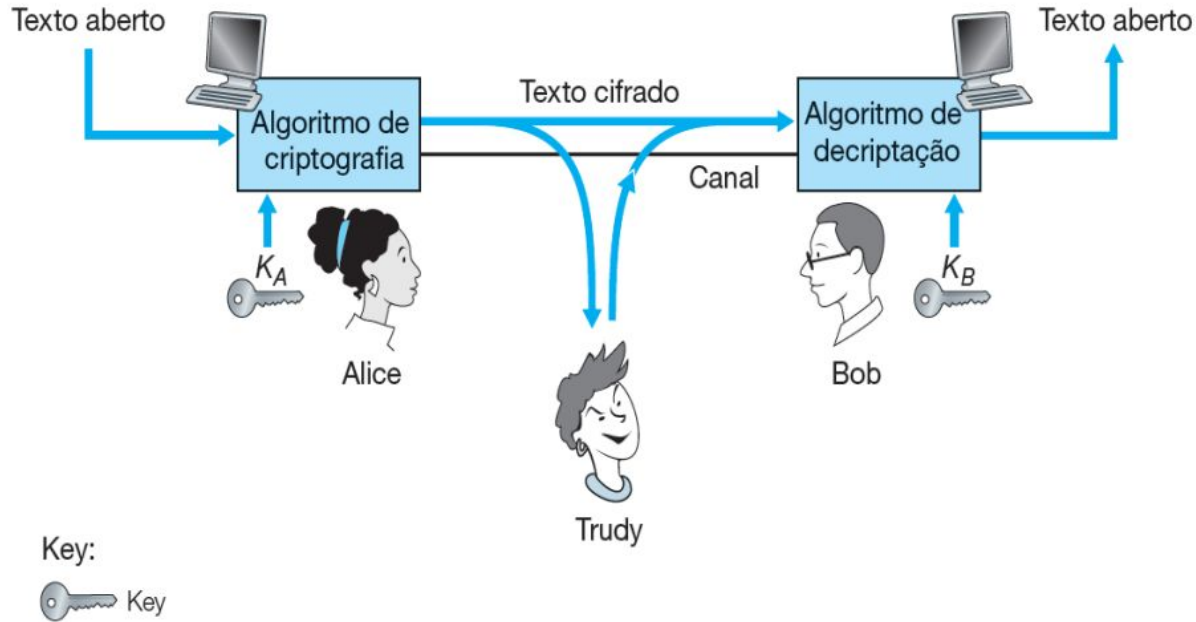
## Exemplos de Criptografia

**Criptografia de chave simétrica:** as chaves do transmissor e do receptor são idênticas

**Criptografia de chave pública:** cifra com chave pública, decifra com chave secreta (privada)



# Componentes da Criptografia

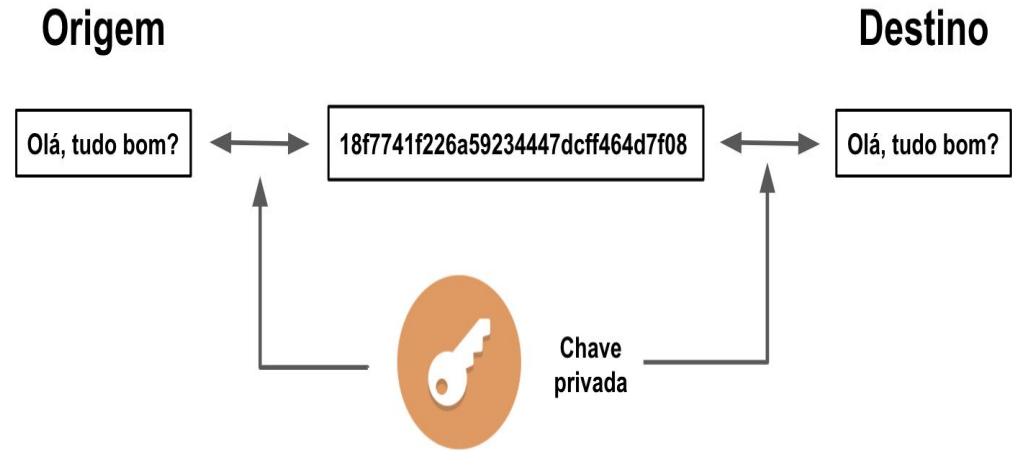


# Criptografia Simétrica

Essa é a criptografia mais básica que existe hoje.

Basicamente a chave usada na criptografia é a mesma usada na descryptografia.

O principal problema é que se o invasor descobrir a chave ele irá facilmente descobrir a informação contida na mensagem.

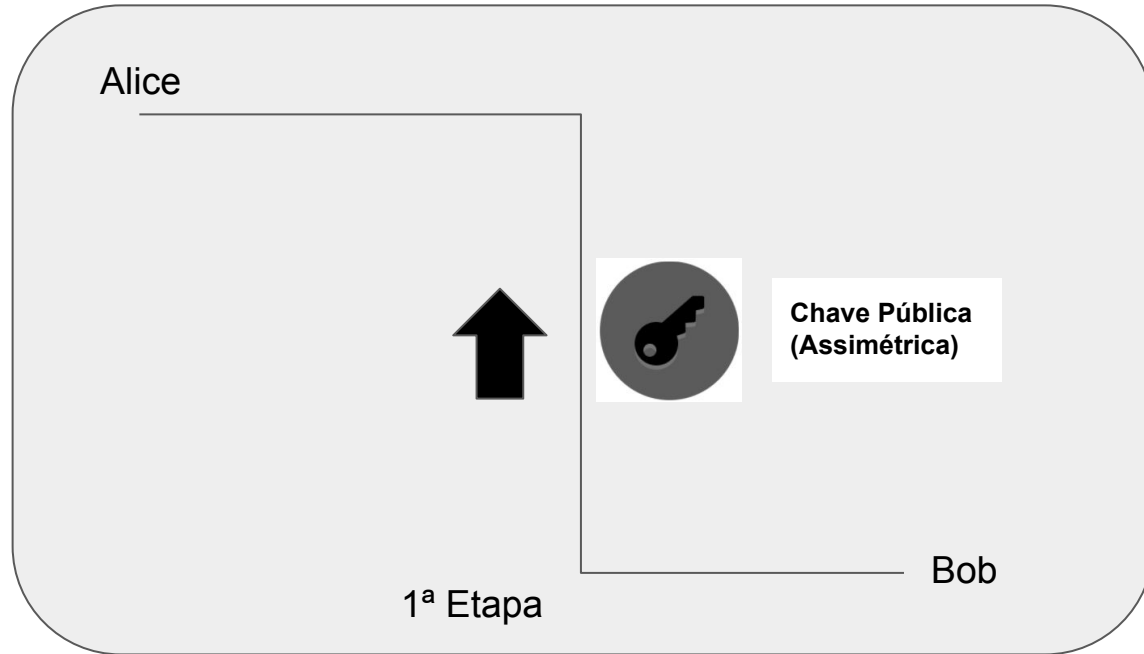


# Criptografia Assimétrica

São usadas duas chaves para fazer a comunicação, chave Pública e a Chave Privada.

## 1ª Etapa

Alice irá solicitar a chave pública para enviar uma mensagem a bob.

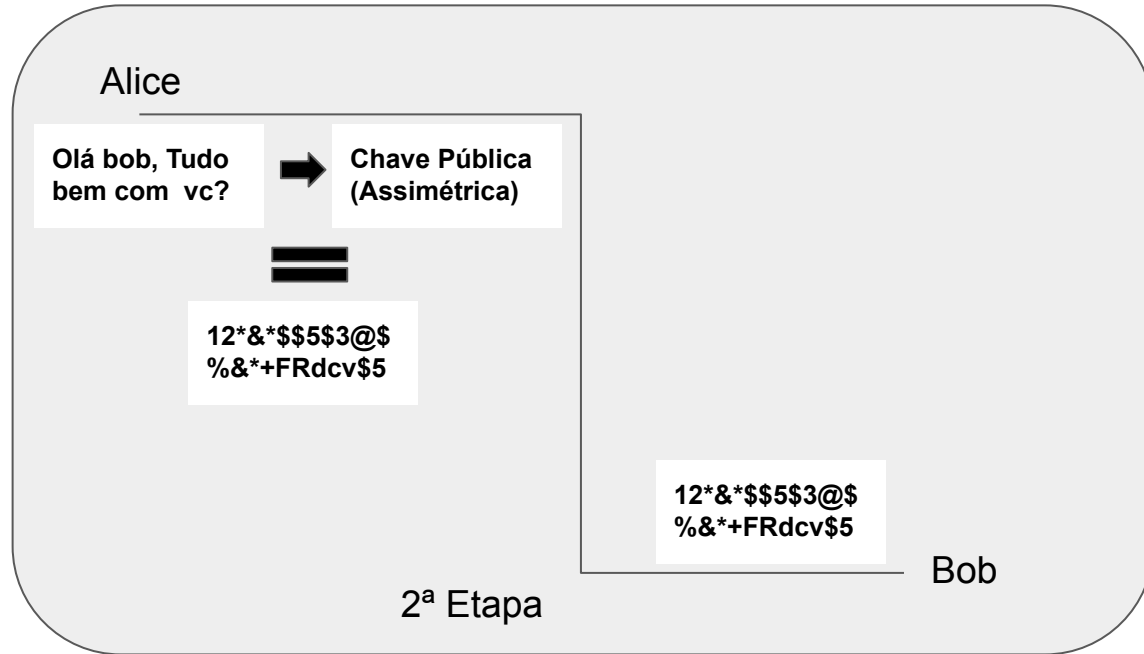


# Criptografia Assimétrica

## 2ª Etapa

Tendo posse da chave Pública, alice irá usar essa chave para criptografar sua mensagem.

Bob irá receber a mensagem criptografada pela alice usando sua chave pública.



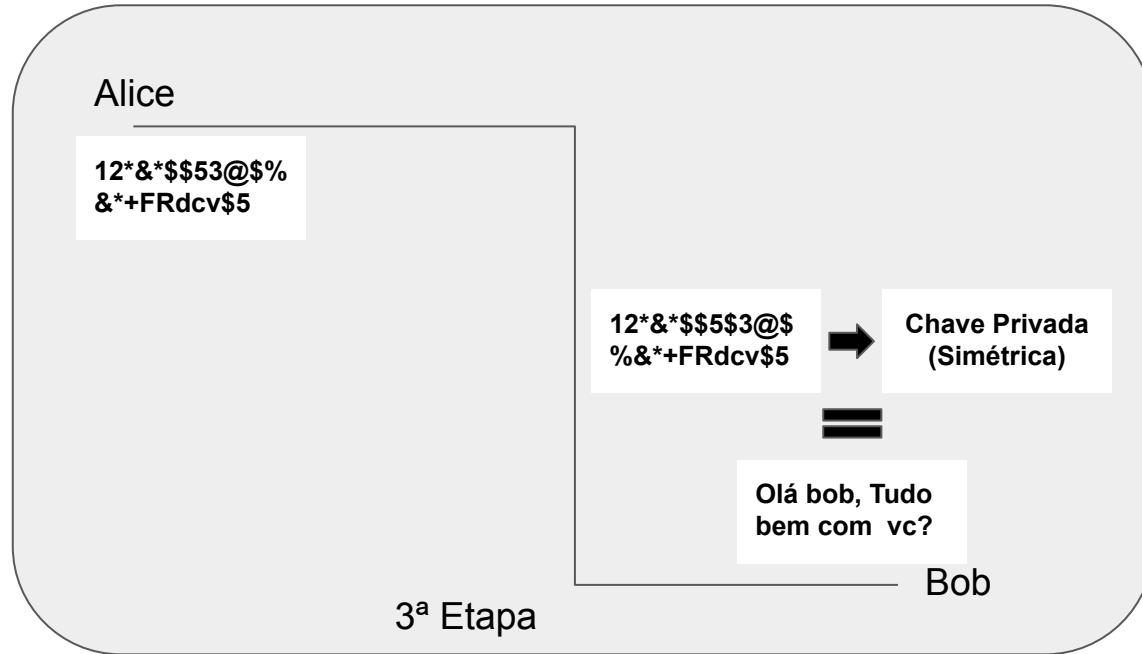


# Criptografia Assimétrica

## 3ª Etapa

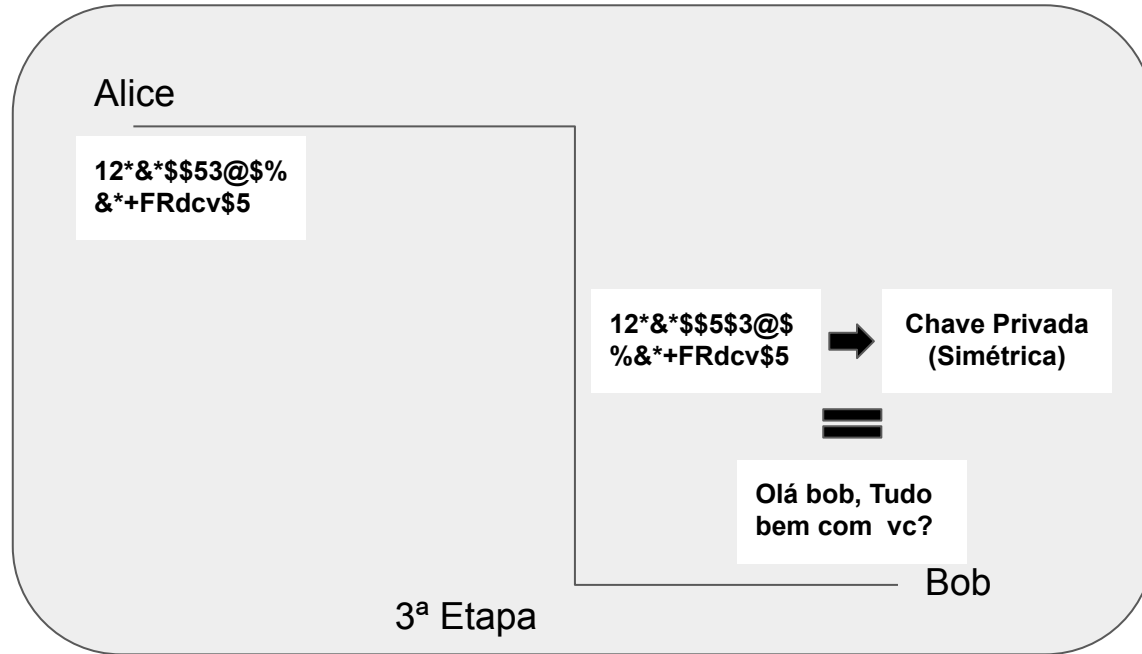
Ao receber a mensagem Bob irá usar sua Chave Privada para Descriptografar a mensagem enviada por Alice.

Perceba, em momento algum Bob entregou a sua chave privada para Alice, entregando apenas a chave Pública.



# Criptografia Assimétrica


Dessa maneira a Chave Pública tem função apenas de Criptografia, mesmo que o invasor consiga o acesso a chave pública ele não consegue descriptografar a mensagem pois não tem a chave privada que tem essa função.



## Sistemas de Segurança

Uma assinatura digital é um esquema matemático para verificar a autenticidade de mensagens ou documentos digitais. Uma assinatura digital válida, ou seja, aquela em que os pré-requisitos são atendidos, dá ao destinatário uma confiança muito alta de que a mensagem foi criada por um remetente conhecido (autenticidade) e que a mensagem não foi alterada em trânsito (integridade).

As assinaturas digitais são um elemento padrão da maioria dos conjuntos de protocolos criptográficos e são comumente usadas para distribuição de software, transações financeiras, software de gerenciamento de contratos e em outros casos em que é importante detectar falsificação ou adulteração.



## Atividade

1. Qual o conceito de ameaça para você? E de onde elas podem vir?
  2. Qual a função da segurança de Redes?
  3. Quais os tipos de ataque você acredita que a escola está mais vulnerável e porque? A resposta mais criativa ganha 1 ponto na prova.
  4. O que é Criptografia?
  5. Quais os principais princípios da criptografia e diga com suas palavras a o conceito de cada um deles.
  6. Qual o tipo de chave usada na criptografia simétrica?
  7. Qual o tipo de chave usada na criptografia assimétrica?
  8. Explique brevemente como ocorre o processo de comunicação usando a criptografia assimétrica.
- 