



SEGURANÇA DE SOFTWARE

Moises Brandalise – Aula 01

Professores

MOISES BRANDALISE

Professor Convidado

Atua como Especialista em Segurança da Informação em uma instituição financeira. Na carreira, atuou no ramo da indústria por 10 anos no papel de líder técnico em infraestrutura de tecnologia e 3 anos como Analista de desenvolvimento de Sistemas em fábrica de software. Em segurança da informação, atuou na indústria da mídia por 6 anos como Analista e no segmento financeiro, por 4 anos como Especialista, além de 2 anos como Especialista em Proteção de dados pessoais, totalizando cerca de 25 anos de mercado.

AVELINO ZORZO

Professor PUCRS

Associado da Sociedade Brasileira de Computação (SBC) e da IEEE. Possui graduação em Ciência da Computação pela Universidade Federal do Rio Grande do Sul (1986-1989), mestrado em Ciência da Computação pela Universidade Federal do Rio Grande do Sul (1990-1994), doutorado em Ciência da Computação pela University of Newcastle Upon Tyne (1995-1999) e pós-doutorado na área de segurança no Cybercrime and Computer Security Centre da Newcastle University (2012-2013). Atualmente é professor titular da Escola Politécnica da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), Coordenador de Programas Profissionais da área de Computação da CAPES/MEC, avaliador de condições de ensino do Ministério da Educação, consultor ad hoc do CNPq, CAPES e da FAPERGS.

Ementa da disciplina

Estudo sobre os métodos e utilização de criptografia para transmissão e armazenamento. Estudo sobre protocolo de comunicação em navegadores (HTTPS) ou aplicativos de conversa (LibSignal). Estudo sobre segurança no desenvolvimento de software. Estudo sobre os problemas mais frequentes indicados pela OWASP. Estudo sobre métodos de autenticação e autorização.

Segurança de Software

Por Moises Brandalise

EMENTA

DA DISCIPLINA

MÉTODOS E UTILIZAÇÃO DE CRIPTOGRAFIA PARA TRANSMISSÃO E ARMAZENAMENTO.

PROTOCOLO DE COMUNICAÇÃO EM NAVEGADORES (HTTPS) OU APLICATIVOS DE CONVERSA (LIBSIGNAL).

SEGURANÇA NO DESENVOLVIMENTO DE SOFTWARE.

OS PROBLEMAS MAIS FREQUENTES INDICADOS PELA OWASP.

MÉTODOS DE AUTENTICAÇÃO E AUTORIZAÇÃO.

CONTEÚDO DAS AULAS

1. INTRODUÇÃO A SEGURANÇA DE SOFTWARE
2. MÉTODOS DE CRIPTOGRAFIA
3. PROTOCOLOS DE COMUNICAÇÃO SEGURA
4. SEGURANÇA NO DESENVOLVIMENTO DE SOFTWARE
5. PROBLEMAS COMUNS DE SEGURANÇA INDICADOS PELA OWASP
6. AUTENTICAÇÃO E AUTORIZAÇÃO

ENCONTROS DA DISCIPLINA



1ª PARTE

INTRODUÇÃO A
SEGURANÇA DE
SOFTWARE

1 HORA



2ª PARTE

MÉTODOS DE
CRIPTOGRAFIA

1 HORA



3ª PARTE

PROTOCOLOS DE
COMUNICAÇÃO
SEGURA

1 HORA

ENCONTROS DA DISCIPLINA



4º PARTE

SEGURANÇA NO
DESENVOLVIMENTO
DE SOFTWARE

1 HORA



5º PARTE

PROBLEMAS
COMUNS DE
SEGURANÇA
INDICADOS PELA
OWASP

1 HORA



6º PARTE

AUTENTICAÇÃO E
AUTORIZAÇÃO

1 HORA

PROFESSOR(A) CONVIDADO(A)

MOISES BRANDALISE

Atuação:

- Segurança da Informação no ramo financeiro (6 anos);
- Analista de Segurança (5 anos);
- Analista de Sistemas e Programador (5 anos);
- Analista de Infraestrutura (5 anos)

Formação acadêmica:

- Especialista em Gestão Estratégica de TI (Pucrs);
- Especialista em Segurança e Gestão de Redes (Ufrgs);
- Ciência da Computação (Upf);

Certificações:

- CISSP, CISM, CDPSE, ISFS.

PROFESSOR(A) PUCRS

AVELINO F. ZORZO


- Doutor em Ciência da Computação pela University of Newcastle Upon Tyne;
- Pós-doutorado na área de segurança no Cybercrime and Computer Security Centre da Newcastle University.
- Professor titular da Escola Politécnica da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS);
- Coordenador da área de Computação, Membro do CTC-ES e do Conselho Superior na CAPES/MEC.

GLOSSÁRIO

TEORIA



EXEMPLOS
PRÁTICOS

- 
1. INTRODUÇÃO A SEGURANÇA DE SOFTWARE
 2. MÉTODOS DE CRIPTOGRAFIA
 3. PROTOCOLOS DE COMUNICAÇÃO SEGURA
 4. SEGURANÇA NO DESENVOLVIMENTO DE SOFTWARE
 5. PROBLEMAS COMUNS DE SEGURANÇA INDICADOS PELA OWASP
 6. AUTENTICAÇÃO E AUTORIZAÇÃO

1. INTRODUÇÃO A SEGURANÇA DE SOFTWARE

- a. POR QUE A SEGURANÇA É IMPORTANTE...
- b. OS PRINCIPAIS RISCOS ENFRENTADOS...
- c. ORGANIZAÇÕES ENVOLVIDAS NA DEFINIÇÃO DE PADRÕES...

2. MÉTODOS DE CRIPTOGRAFIA

3. PROTOCOLOS DE COMUNICAÇÃO SEGURA

4. SEGURANÇA NO DESENVOLVIMENTO DE SOFTWARE

5. PROBLEMAS COMUNS DE SEGURANÇA INDICADOS PELA OWASP

6. AUTENTICAÇÃO E AUTORIZAÇÃO

a) POR QUE A SEGURANÇA É IMPORTANTE NO DESENVOLVIMENTO DE SOFTWARE

Com a aceleração da necessidade de Home Office e do aumento de serviços online, muito serviço foi disponibilizado rapidamente.



- Fim dos limites físicos
- Migração dos serviços em nuvem.
 - Repositórios abertos
- SQL injection diminuiu.
 - Information disclosure aumentou;
- Valor do Dado depois da LGPD;
 - Segurança by Design.
- Treinamentos
 - Poderes diferentes dentro da infra.

a) POR QUE A SEGURANÇA É IMPORTANTE NO DESENVOLVIMENTO DE SOFTWARE

OT industries targeted in 2022

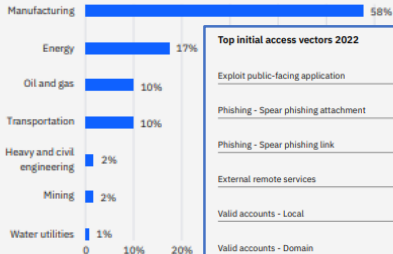


Figure 14: Proportion of IR cases by OT-related industry to which X-Force responded in 2022
Source: X-Force

Top initial access vectors 2022

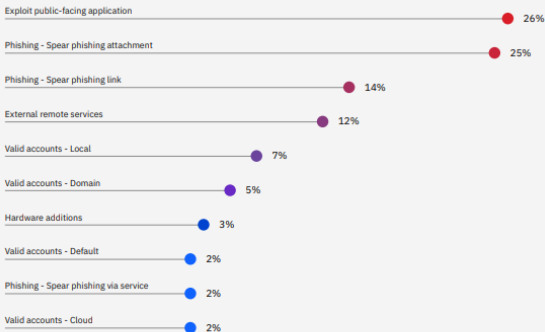



Figure 1: Top initial access vectors X-Force observed in 2022. Source: X-Force

 O surgimento dos sistemas operacionais em 1960 permitiu a criação de programas complexos.

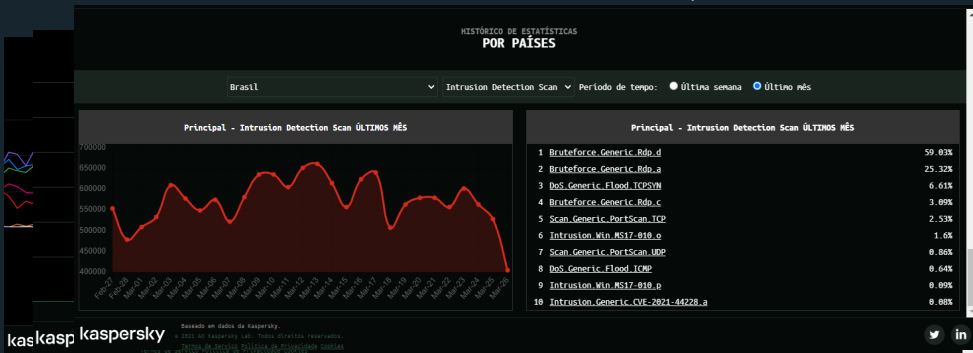
1. INTRODUÇÃO A SEGURANÇA DE SOFTWARE

a) POR QUE A SEGURANÇA É IMPORTANTE NO DESENVOLVIMENTO DE SOFTWARE



É importante que esses riscos sejam identificados e mitigados durante todo o processo de desenvolvimento de software.

Centro de controle da Kaspersky
Detecções por Segundo



b) OS PRINCIPAIS RISCOS DE SEGURANÇA ENFRENTADOS PELOS DESENVOLVEDORES DE SOFTWARE

O software é **utilizado** em muitas áreas da **nossa** vida, incluindo **finanças**, saúde, comércio eletrônico, governança e outras.



- ATAQUES HACKERS
- VAZAMENTO DE DADOS
- ATAQUES DE PHISHING
- MALWARE



- Prevenção a fraude por roubo de identidade.
- Atrasos ou interrupções afetam a vida das pessoas.
- Preocupação, estresse, perdas financeiras....



- **Ataques Hackers**
- Vazamento de Dados
- Ataques de phishing
- Malware

b) OS PRINCIPAIS RISCOS DE SEGURANÇA ENFRENTADOS PELOS DESENVOLVEDORES DE SOFTWARE

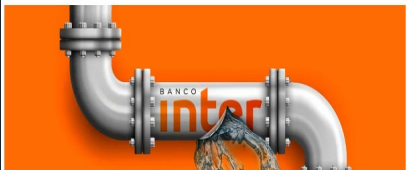


O 1º grande ataque hacker registrado foi em 1988, conhecido como o "verme de Morris"..

O banco não divulgou publicamente os detalhes.

Banco Inter é extorquido e dados de clientes são expostos; invasão é negada

04/05/2018 às 07:00 • 10 min de leitura



Um exemplo famoso de ataque de hackers foi o caso do Banco Inter em 2018. O Banco Inter é uma instituição financeira totalmente digital...

Explicação técnica: Os hackers exploraram uma vulnerabilidade de segurança do sistema do Banco Inter....



- Ataques Hackers
- **Vazamento de Dados**
- Ataques de phishing
- Malware

b) OS PRINCIPAIS RISCOS DE SEGURANÇA ENFRENTADOS PELOS DESENVOLVEDORES DE SOFTWARE



Um estudo realizado pela IBM em 2020 apontou que o custo médio de um vazamento de dados globalmente é de US\$ 3,86 milhões.

Os **vazamentos** de dados podem ser muito **prejudiciais** para os indivíduos afetados e para as **empresas** envolvidas.

DESASTRE?

TAP sofre ataque de ransomware

02/09/2022 13:26

Cibercriminosos ameaçam: "a dona do maior processo de violação de dados da história".



Em março de 2021, a companhia aérea TAP Air Portugal sofreu um vazamento de dados que afetou cerca de 10 milhões de passageiros.

Explicação técnica: O vazamento de dados pode ter ocorrido devido a uma vulnerabilidade no servidor de backup antigo que permitiu que um invasor tivesse acesso aos dados armazenados.



- Ataques Hackers
- Vazamento de Dados
- **Ataques de phishing**
- Malware

b) OS PRINCIPAIS RISCOS DE SEGURANÇA ENFRENTADOS PELOS DESENVOLVEDORES DE SOFTWARE



Alguns ataques de phishing utilizam técnicas de engenharia social para criar uma sensação de urgência ou medo nos usuários, fazendo com que eles ajam de forma impulsiva.

Utiliza de **engenharia social** para enganar as vítimas a fim de obter suas informações pessoais...



Em 2019, hackers enviaram um e-mail falso em nome da Receita Federal para enganar os contribuintes e roubar seus dados pessoais.

Explicação técnica: O e-mail continha um link para uma página falsa, muito similar ao site oficial da Receita, e pedia que o usuário informasse seus dados pessoais..



- Ataques Hackers
- Vazamento de Dados
- Ataques de phishing
- Malware

Pode causar **danos** significativos ao sistema, como a perda de dados...

b) OS PRINCIPAIS RISCOS DE SEGURANÇA ENFRENTADOS PELOS DESENVOLVEDORES DE SOFTWARE



O "Stuxnet", um dos malwares mais conhecidos da história, foi criado por governos para sabotar o programa nuclear do Irã.

Olhar Digital > Notícias > 11 apps maliciosos da Google Play assinavam serviços caros pelo usuário

NOTÍCIAS

SEGURANÇA E PRIVACIDADE

11 apps maliciosos da Google Play assinavam serviços caros pelo usuário

Aplicativos tinham um malware conhecido como 'Joker' e já foram removidos da loja do Android

Por Daniel Junqueira, editado por Flávio Pinto | 10/07/2020 20h06, atualizada em 05/04/2021 13h09

Em 2020, uma campanha de malware foi detectada no Google Play Store. O malware, conhecido como "Joker", foi encontrado em 11 aplicativos para Android....

Explicação técnica: O malware se aproveita de vulnerabilidades em aplicativos para instalar programas maliciosos no dispositivo do usuário, permitindo que os hackers roubem informações ou controlem o dispositivo.

C) AS PRINCIPAIS ORGANIZAÇÕES ENVOLVIDAS NA DEFINIÇÃO DE PADRÕES DE SEGURANÇA

Essas organizações **trabalham** em estreita colaboração com **especialistas** em segurança cibernética....



- ISO - Organização Internacional de Normalização
- W3C - Consórcio World Wide Web
- OWASP - Open Web Application Security Project
- NIST - National Institute of Standards and Technology
- IETF - Internet Engineering Task Force
- PCI SSC - Payment Card Industry Security Standards Council



- Recursos e orientações
- Maior segurança
- Conformidade regulatória:



- ISO - Organização Internacional de Normalização
- W3C - Consórcio World Wide Web
- OWASP - Open Web Application Security Project
- NIST - National Institute of Standards and Technology
- IETF - Internet Engineering Task Force
- PCI SSC - Payment Card Industry Security Standards Council

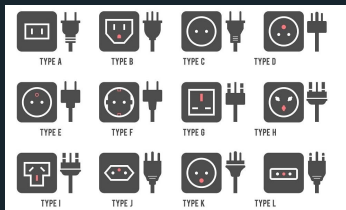
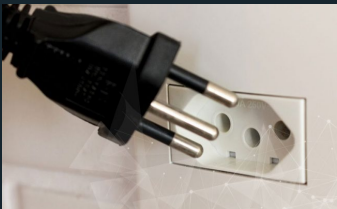
1. INTRODUÇÃO A SEGURANÇA DE SOFTWARE

c) AS PRINCIPAIS ORGANIZAÇÕES ENVOLVIDAS NA DEFINIÇÃO DE PADRÕES DE SEGURANÇA.



As coisas padronizadas tendem a ser mais interoperáveis, o que significa que diferentes sistemas podem trabalhar juntos.

A padronização possibilita a interoperabilidade





- **ISO - Organização Internacional de Normalização**
- W3C - Consórcio World Wide Web
- OWASP - Open Web Application Security Project
- NIST - National Institute of Standards and Technology
- IETF - Internet Engineering Task Force
- PCI SSC - Payment Card Industry Security Standards Council

International Organization for Standardization

c) AS PRINCIPAIS ORGANIZAÇÕES ENVOLVIDAS NA DEFINIÇÃO DE PADRÕES DE SEGURANÇA.



Fundada em 1947 após a Segunda Guerra Mundial, com o objetivo de promover a cooperação internacional e facilitar o comércio internacional.

ISO/IEC 27001:

é uma norma de segurança da informação que estabelece requisitos para um sistema de gestão de segurança da informação (SGSI).

ISO/IEC 27002:

é um código de práticas para a segurança da informação, que fornece diretrizes e controles de segurança que podem ser implementados pelo SGSI.

ISO/IEC 27034:

Fornecer orientações para o **ciclo** de vida completo do desenvolvimento de **software** e a seleção e implementação de medidas de segurança apropriadas.

Gestão de Ativos
Política de Segurança da Informação
Gestão de Acessos

...

Controle de acesso
Gerenciamento de vulnerabilidades
Gerenciamento de mudanças

...



- ISO - Organização Internacional de Normalização
- **W3C - Consórcio World Wide Web**
- OWASP - Open Web Application Security Project
- NIST - National Institute of Standards and Technology
- IETF - Internet Engineering Task Force
- PCI SSC - Payment Card Industry Security Standards Council

O World Wide Web Consortium...

HTML (Hypertext Markup Language):

Linguagem de marcação usada para criar páginas web.

CSS (Cascading Style Sheets):

Linguagem usada para estilizar o conteúdo HTML, como cores, fontes e layout.

Protocolo HTTPS e padrões de uso da criptografia TLS:

Definição de padrões de criptografia, como o TLS, para garantir que as informações confidenciais sejam armazenadas e transmitidas de forma segura.

1. INTRODUÇÃO A SEGURANÇA DE SOFTWARE

c) AS PRINCIPAIS ORGANIZAÇÕES ENVOLVIDAS NA DEFINIÇÃO DE PADRÕES DE SEGURANÇA.



O WorldWideWeb foi projetado para ser uma forma de compartilhar informações entre pesquisadores do CERN e de outras instituições acadêmicas.

//seletor de classe (class selector)

```
.destaque {  
    color: red;  
    font-weight: bold;  
}
```



- ISO - Organização Internacional de Normalização
- W3C - Consórcio World Wide Web
- **OWASP - Open Web Application Security Project**
- NIST - National Institute of Standards and Technology
- IETF - Internet Engineering Task Force
- PCI SSC - Payment Card Industry Security Standards Council

Open Worldwide Application Security Project

OWASP Top 10:

Lista das **10 principais vulnerabilidades** de segurança em aplicativos da web para ajudar os desenvolvedores a identificar e mitigar riscos de segurança em seus projetos.

Colaboração:

Fornecendo informações e recursos gratuitos para desenvolvedores e profissionais de segurança cibernética sobre as **melhores práticas** para proteger aplicativos da web.

Pesquisas:

Realizando pesquisas e desenvolvendo ferramentas de segurança para ajudar os desenvolvedores a criar aplicativos da web mais seguros.

c) AS PRINCIPAIS ORGANIZAÇÕES ENVOLVIDAS NA DEFINIÇÃO DE PADRÕES DE SEGURANÇA.



Listas são visualmente atraentes, pois permitem "escanear" o conteúdo rapidamente e identificar as informações mais importantes.



- ISO - Organização Internacional de Normalização
- W3C - Consórcio World Wide Web
- OWASP - Open Web Application Security Project
- **NIST - National Institute of Standards and Technology**
- IETF - Internet Engineering Task Force
- PCI SSC - Payment Card Industry Security Standards Council

National Institute of Standards and Technology

1. INTRODUÇÃO A SEGURANÇA DE SOFTWARE

c) AS PRINCIPAIS ORGANIZAÇÕES ENVOLVIDAS NA DEFINIÇÃO DE PADRÕES DE SEGURANÇA.



Empresas que trabalham com o governo dos Estados Unidos são obrigadas a cumprir os rigorosos padrões de segurança da informação estabelecidos pelo governo.

Governo EUA:

Agência governamental dos Estados Unidos que desenvolve e promove **padrões de segurança cibernética**.

Cyber Ameaças:

Fornecer orientações e recursos para ajudar as organizações a proteger seus sistemas e dados contra ameaças cibernéticas

NIST Cybersecurity Framework:

Ajuda as organizações a gerenciar e reduzir o risco de segurança cibernética. O framework é composto por uma série de práticas, orientações e normas.



- ISO - Organização Internacional de Normalização
- W3C - Consórcio World Wide Web
- OWASP - Open Web Application Security Project
- NIST - National Institute of Standards and Technology
- **IETF - Internet Engineering Task Force**
- PCI SSC - Payment Card Industry Security Standards Council

Internet Engineering Task Force

c) AS PRINCIPAIS ORGANIZAÇÕES ENVOLVIDAS NA DEFINIÇÃO DE PADRÕES DE SEGURANÇA.



Suas reuniões são realizadas três vezes por ano, em diferentes locais ao redor do mundo, e qualquer pessoa pode participar.

SSL, TLS e Ipsec:

Responsável pelo desenvolvimento de muitos padrões de criptografia utilizados em aplicativos de software.

TCP/IP:

Desenvolveu muitos padrões de protocolo de rede, como TCP/IP, que são essenciais para a comunicação segura e confiável entre sistemas e aplicativos de software.

Kerberos:

Desenvolveu vários padrões de autenticação que ajuda a garantir que apenas usuários autorizados tenham acesso a sistemas e aplicativos



- ISO - Organização Internacional de Normalização
- W3C - Consórcio World Wide Web
- OWASP - Open Web Application Security Project
- NIST - National Institute of Standards and Technology
- IETF - Internet Engineering Task Force
- **PCI SSC - Payment Card Industry Security Standards Council**

Desde 2006.

Visa, MasterCard e American Express:

Criada pelas principais empresas de cartões de crédito para estabelecer padrões de segurança para a indústria de cartões de pagamento.

PA-DSS:

Desenvolvimento de **diretrizes** para a segurança de aplicativos de **software** de pagamento.

PCI DSS:

Certifica empresas ajudando a garantir que estejam em conformidade com os padrões de segurança de cartões de pagamento e protejam as informações de seus clientes.

1. INTRODUÇÃO A SEGURANÇA DE SOFTWARE

c) AS PRINCIPAIS ORGANIZAÇÕES ENVOLVIDAS NA DEFINIÇÃO DE PADRÕES DE SEGURANÇA.



O primeiro cartão de crédito moderno foi lançado em 1950 pela Diners Club.

1. INTRODUÇÃO A SEGURANÇA DE SOFTWARE

2. MÉTODOS DE CRIPTOGRAFIA

a) O QUE É CRIPTOGRAFIA E COMO ELA FUNCIONA.

b) TIPOS DE CRIPTOGRAFIA: SIMÉTRICA, ASSIMÉTRICA E HASH.

c) COMO UTILIZAR CRIPTOGRAFIA PARA ARMAZENAMENTO E TRANSMISSÃO DE DADOS.

d) PADRÕES DE CRIPTOGRAFIA RECOMENDADOS PARA DIFERENTES TIPOS DE DADOS.

3. PROTOCOLOS DE COMUNICAÇÃO SEGURA

4. SEGURANÇA NO DESENVOLVIMENTO DE SOFTWARE

5. PROBLEMAS COMUNS DE SEGURANÇA INDICADOS PELA OWASP

6. AUTENTICAÇÃO E AUTORIZAÇÃO

a) O QUE É CRIPTOGRAFIA E COMO ELA FUNCIONA.

A criptografia é **importante** para garantir a **privacidade** e a integridade de informações pessoais e sensíveis...



- **O QUE É**
- COMO FUNCIONA
- ONDE É USADO



- Dignidade, danos financeiros, impeça exercício dos direitos.
- Intimidade e a vida privada.
- Uso de documentos e dados para fraudes.
- Soberania da nação.



- **O que é**
- Como funciona
- Onde é usado

Muito importante principalmente pelas questões de Confidencialidade.

Transformação:

Informações **legíveis** em um formato **ininteligível** para protegê-las contra acesso não autorizado.

Matemática:

Algoritmos matemáticos complexos que transformam o texto original em um formato criptografado.

Exemplo: Quando você cria uma senha, ela é criptografada e armazenada em um banco de dados. Quando você faz login, o que acontece?

a) O QUE É CRIPTOGRAFIA E COMO ELA FUNCIONA.



O serviço postal da Inglaterra foi criado em 1635, antes disso, as cartas eram entregues por mensageiros sem garantia de que não eram lidas.





- O que é
- **Como funciona**
- Onde é usado

Um dado legível transformado em dado codificado.

a) O QUE É CRIPTOGRAFIA E COMO ELA FUNCIONA.



Um dos filmes mais conhecidos sobre criptografia é "O Jogo da Imitação".

Chaves criptográficas:

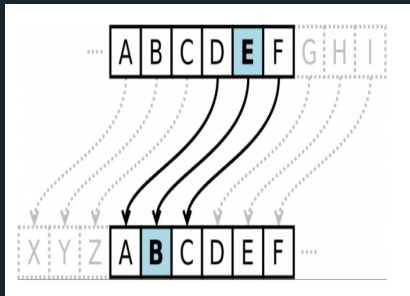
A criptografia usa chaves para codificar e decodificar informações. Uma **chave** é um **valor secreto** que é usado para transformar a informação.

Cifras Simétricas e assimétricas:

As chaves **simétricas** usam a **mesma** chave para criptografar e descriptografar dados, enquanto as **assimétricas** usam um **par** de chaves diferentes: uma pública e outra privada.

Reversão:

O princípio é a dificuldade ou impossibilidade de reversão de um dado que foi criptografado.





- O que é
- Como funciona
- Onde é usado

Para armazenar ou transferir dados em sigilo.

Proteção


... muitas áreas, incluindo **comunicações seguras**, transações **financeiras**, proteção de dados pessoais e segurança cibernética.

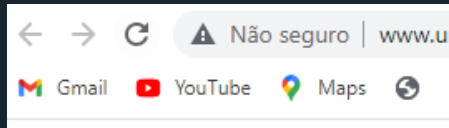
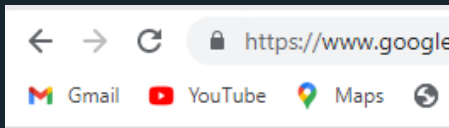
Integridade dos Dados

... garantir a integridade dos dados, **validar** se as informações não foram **modificadas** ou adulteradas durante a transmissão.

Exemplo: Ao acessar um site, sobre o HTTP é incluída uma camada de criptografia TLS (HTTPS), que pode na maioria das vezes utiliza algoritmos AES.

a) O QUE É CRIPTOGRAFIA E COMO ELA FUNCIONA.

 *Algoritmos de criptografia mal implementados ou mal usados podem ser quebrados por pessoas mal intencionadas com recursos suficientes e tempo necessário*



b) TIPOS DE CRIPTOGRAFIA: SIMÉTRICA, ASSIMÉTRICA E HASH.

A criptografia **ajuda** as pessoas a manterem suas informações **privadas** e seguras, o que é **essencial** no mundo digital em que vivemos atualmente.



- CRIPTOGRAFIA SIMÉTRICA
- CRIPTOGRAFIA ASSIMÉTRICA
- FUNÇÕES HASH



- Roubo de identidade
- Fraude financeira
- Vazamento de informações confidenciais
- Espionagem industrial e governamental



- **Criptografia Simétrica**
- Criptografia Assimétrica
- Funções Hash

A **mesma chave** é usada para criptografar e descriptografar os dados.

Velocidade:

Geralmente mais rápida do que a criptografia assimétrica, pois não utiliza operações matemáticas com alto custo computacional.

Segurança:

Depende da proteção adequada da chave secreta compartilhada. Se a chave secreta for comprometida, a segurança pode ser comprometida.

Uso:

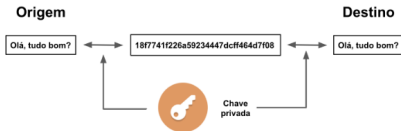
Cenários em que a **confidencialidade** é o principal **objetivo**, como transações financeiras, comunicações militares e segurança de rede.

b) TIPOS DE CRIPTOGRAFIA: SIMÉTRICA, ASSIMÉTRICA E HASH.



A criptografia simétrica foi usada pelos alemães na Segunda Guerra Mundial, até ser quebrada pelos aliados.

Criptografia de chave privada - simétrica

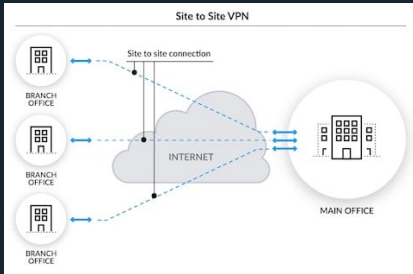




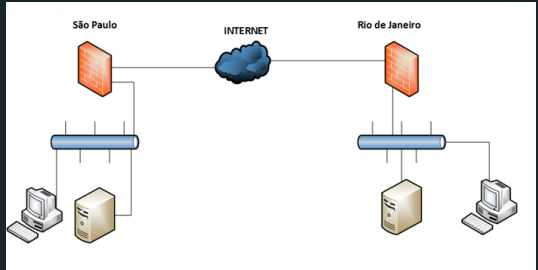
- **Criptografia Simétrica**
- Criptografia Assimétrica
- Funções Hash

b) TIPOS DE CRIPTOGRAFIA: SIMÉTRICA, ASSIMÉTRICA E HASH.

Exemplo 1



Exemplo 2





- Criptografia Simétrica
- **Criptografia Assimétrica**
- Funções Hash

Conhecida como criptografia de chave pública, é um método em que **duas chaves** diferentes são usadas para criptografar e descriptografar os dados.

Duas chaves:

Utiliza um **par** de chaves: uma **pública** e uma **privada**.

Chave pública:

A chave pública é **distribuída livremente** e amplamente conhecida. Usada para **criptografar** os dados enviados.

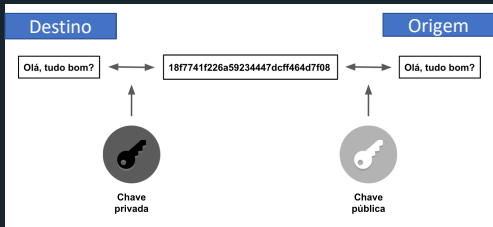
Chave privada:

A chave privada é **mantida em segredo** pelo proprietário da chave e é usada para **descriptografar** os dados recebidos.

b) TIPOS DE CRIPTOGRAFIA: SIMÉTRICA, ASSIMÉTRICA E HASH.



Os antigos egípcios usavam hieróglifos para ocultar informações importantes em seus monumentos e papiros.

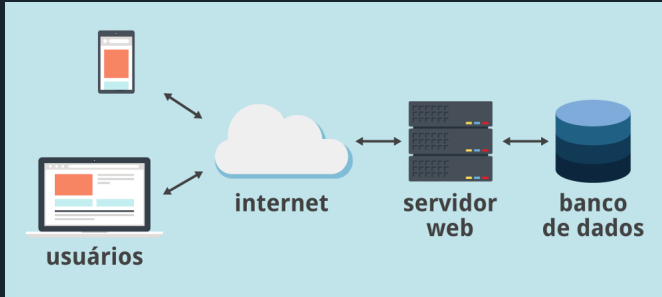




- Criptografia Simétrica
- **Criptografia Assimétrica**
- Funções Hash

b) TIPOS DE CRIPTOGRAFIA: SIMÉTRICA, ASSIMÉTRICA E HASH.

Front + Back = Onde está a criptografia dos dados em trânsito?





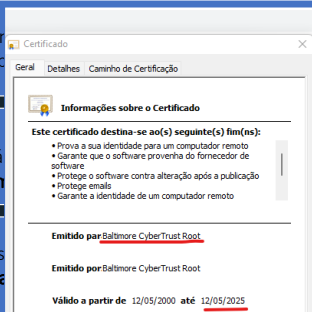
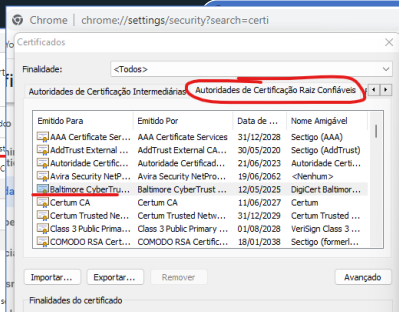
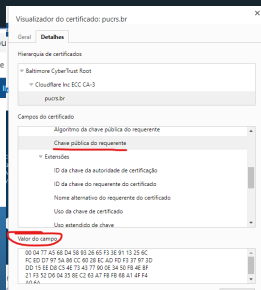
- Criptografia Simétrica
- **Criptografia Assimétrica**
- Funções Hash

b) TIPOS DE CRIPTOGRAFIA: SIMÉTRICA, ASSIMÉTRICA E HASH.

Certificados Digitais são **usados** para autenticar e **proteger** as **comunicações** eletrônicas....



Na Babilônia havia um sistema de impressão de selos em argila para autenticar transações comerciais e documentos oficiais.





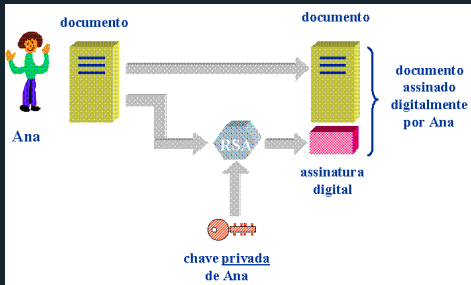
- Criptografia Simétrica
- **Criptografia Assimétrica**
 - **Assinatura Digital**
- Funções Hash

Trata-se de uma forma de verificar a autenticidade e integridade de um documento ou mensagem.

b) TIPOS DE CRIPTOGRAFIA: SIMÉTRICA, ASSIMÉTRICA E HASH.



A primeira patente de uma assinatura digital foi registrada em 1983 por David Chaum, um criptógrafo americano.



Assinatura Digital:

Esquema matemático para verificar a autenticidade de mensagens ou documentos digitais.

Assinatura Eletrônica:

Qualquer mecanismo eletrônico, não necessariamente criptográfico, para identificar alguém.

Exemplos:

Ass. Digital: e-CPF, Portal gov.br...

Ass. Eletrônica: DocuSign, ClickSign...



- Criptografia Simétrica
- **Criptografia Assimétrica**
 - Assinatura Digital
- Funções Hash

b) TIPOS DE CRIPTOGRAFIA: SIMÉTRICA, ASSIMÉTRICA E HASH.

e-CPF	A1	1 ano	Instalado no computador
	A3	1 ano 2 anos 3 anos	Token ou <i>smart card</i>
e-CNPJ	A1	1 ano	Instalado no computador
	A3	1 ano 2 anos 3 anos	Token ou <i>smart card</i>

Autoridade Certificadora

É quem assina digitalmente o certificado.

Autoridade Emissora

Maioria das vezes é quem faz contato com o cliente. Precisa estar ligada a uma AC.



- Criptografia Simétrica
- Criptografia Assimétrica
- **Funções Hash**

b) TIPOS DE CRIPTOGRAFIA: SIMÉTRICA, ASSIMÉTRICA E HASH.

Uma forma de criptografia que usa um algoritmo matemático para transformar um



Em jogos de vídeo game, as funções hash são usadas para gerar números aleatórios para imagens, objetos e eventos.

Este é um teste para a aula de segurança de software.

6B663008AE3B0ED303B98156DA375C788D43CE70C9F7ABA4AAA6F179E25BE278

Diferença:

Ao contrário de uma chave necessária.

Este é um teste para a aula de segurança de software

77F140B717D844EBCB8FEAC5EB4841680D7B13A9B0A5B194E3ED74EEBB3591C2

Objetivo:

Usadas principalmente para verificar a integridade dos dados.

Este é um teste para a aula de segurança de software.

6B663008AE3B0ED303B98156DA375C788D43CE70C9F7ABA4AAA6F179E25BE278

Exemplo:

- Arquivos baixados da internet;
- Tecnologias de blockchain;

Hash aqui:

ware.

Gerar SHA256 Hash!

io? Por quê? ⓘ

a partir daqui.

6B663008AE3B0ED303B98156DA375C788D43CE70C9F7ABA4AAA6F179E25BE278

c) COMO UTILIZAR CRIPTOGRAFIA PARA ARMAZENAMENTO E TRANSMISSÃO DE DADOS.

A criptografia pode ser usada para proteger dados em repouso (**armazenamento**) e em movimento (**transmissão**).



- IMPLEMENTAÇÃO CORRETA
- GERENCIAMENTO SEGURO DE CHAVES
- PREVENÇÃO DE ATAQUES
- TESTE E AUDITORIA



- Privacidade
- Garantia da integridade dos dados
- Proteção contra roubo de identidade
- Confidencialidade



*Em 2016, cientistas de dados da Universidade de Southampton, no Reino Unido, armazenaram um arquivo de 360 **terabytes** em um único disco de quartzo de tamanho de um selo postal.*



- **Implementação correta**
- Gerenciamento seguro de chaves
- Prevenção de ataques
- Teste e auditoria

Escolher algoritmos criptográficos robustos e usar técnicas de implementação seguras para proteger os dados.

Em repouso

Para proteger dados em repouso, é possível usar criptografia de disco rígido ou criptografia de banco de dados.

Em movimento

Para proteger dados em movimento, é possível usar protocolos de segurança como HTTPS, SSL/TLS e VPNs.

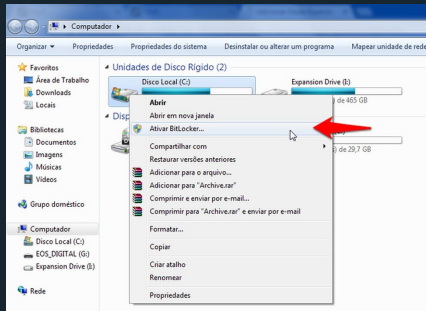
Exemplos.

- Bitlocker: recurso de criptografia de volume da MS.
- VPN: Estabelece canal seguro de comunicação.

c) COMO UTILIZAR CRIPTOGRAFIA PARA ARMAZENAMENTO E TRANSMISSÃO DE DADOS.



A transmissão quântica de dados é baseada em partículas subatômicas chamadas qubits, que podem ser usadas para transmitir dados.





- Implementação correta
- **Gerenciamento seguro de chaves**
- Prevenção de ataques
- Teste e auditoria

A criptografia é tão forte quanto suas chaves.

Gerenciar as chaves

Garantir a segurança de dados em ambientes digitais.

Geração e Distribuição

Gestão do ciclo de vida das chaves.

Exemplo

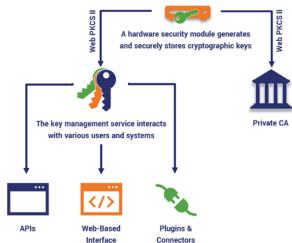
Vault (vários), Azure, AWS, etc....

c) COMO UTILIZAR CRIPTOGRAFIA PARA ARMAZENAMENTO E TRANSMISSÃO DE DADOS.



Em menos de duas horas, em 2011, um pesquisador usou uma EC2 da Amazon (gratuita) para quebrar uma chave de 512 bits, considerada segura na época.

The Relationship Between a KMS and HSM





- Implementação correta
- Gerenciamento seguro de chaves
- **Prevenção de ataques**
- Teste e auditoria

c) COMO UTILIZAR CRIPTOGRAFIA PARA ARMAZENAMENTO E TRANSMISSÃO DE DADOS.

Desenvolvedores podem ajudar....

```
std::string generateSalt(int length) {
    std::string salt;
    salt.resize(length);

    RAND_bytes((unsigned char*)&salt[0], length);
```

```
int main() {
    std::string password = "mypassword";
    std::string salt = generateSalt(16);
    std::string hashedPassword = generateHash(password, salt);

    std::cout << "Salt: " << salt << std::endl;
    std::cout << "Hashed password: " << hashedPassword << std::endl;

    return 0;
}
```

```
std::string password, std::string salt) {
    word = salt + password;
    256_DIGEST_LENGTH];
    )&saltedPassword[0], saltedPassword.length(), hash);

    GEST_LENGTH * 2 + 1];
    A256_DIGEST_LENGTH; i++) {
        * 2], "%02x", hash[i]);
    }
}
```

```
return std::string(hexHash);
}
```

Exemplo

A aplicação prática mais comum do salting é na criptografia de senhas armazenadas em bancos de dados de logins.



- Implementação correta
- Gerenciamento seguro de chaves
- Prevenção de ataques
- **Teste e auditoria**

É importante testar e auditar regularmente as implementações criptográficas para garantir que elas continuem a ser seguras.

Como:

Isso envolve testes de penetração, revisão de código e auditoria de terceiros.

Conflitos:

Em uma empresa pequena ou média, muitas vezes o papel do nível 2 e 3 é realizado pela mesma equipe.

Exemplo:

Ao escrever código (1ª linha) pode-se ter o papel de uma empresa (2ª linha auxiliando) e uma auditoria (3ª linha testando).

c) COMO UTILIZAR CRIPTOGRAFIA PARA ARMAZENAMENTO E TRANSMISSÃO DE DADOS.

⚠ Os faraós utilizavam inspetores para garantir a qualidade e a integridade de seus suprimentos de alimentos e materiais de construção.

O Modelo das Três Linhas do The IIA



d) PADRÕES DE CRIPTOGRAFIA RECOMENDADOS PARA DIFERENTES TIPOS DE DADOS.

Os padrões de criptografia recomendados podem **variar** dependendo do **tipo** de dados que está sendo **protegido**.



- AES (Advanced Encryption Standard)
- RSA (Rivest-Shamir-Adleman)
- SHA (Secure Hash Algorithm)



- Proteger os dados em repouso
- Proteger dados em movimento.
- Garantir autenticidade



- **AES (Advanced Encryption Standard)**
- RSA (Rivest-Shamir-Adleman)
- SHA (Secure Hash Algorithm)

Usado para criptografar dados em repouso e em movimento.

Velocidade

Rápido e eficiente em termos de processamento de dados, o que o torna adequado para **aplicações** que exigem alto desempenho.

Ampla utilização

Adotado por **organizações** governamentais e empresas em todo o mundo, tornando-se uma das **escolhas** mais **populares**.

Exemplo 1

Ao fazer **upload** de um arquivo no **Dropbox**, o serviço usa o AES para **criptografar** o arquivo usando uma **chave** de criptografia.

Exemplo 2

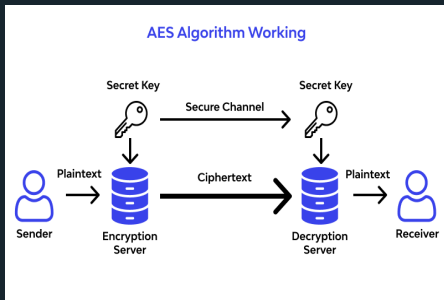
Criptografar **informações** confidenciais, como números de **cartão** de **crédito** ou **senhas**, durante transações financeiras online.

2. MÉTODOS DE CRIPTOGRAFIA

d) PADRÕES DE CRIPTOGRAFIA RECOMENDADOS PARA DIFERENTES TIPOS DE DADOS.



O projeto Aurora, supostamente desenvolvido pela Agência Central de Inteligência dos Estados Unidos (CIA), é um programa que pode hackear sistemas de controle industrial.





- AES (Advanced Encryption Standard)
- **RSA (Rivest-Shamir-Adleman)**
- SHA (Secure Hash Algorithm)

Considerado um dos algoritmos de criptografia mais seguros disponíveis atualmente.

Utilização de chaves públicas e privadas:

A chave pública é compartilhada com outras pessoas para que possam criptografar as mensagens.

Versátil

Pode ser utilizado para criptografar uma variedade de dados, como mensagens de texto, arquivos, imagens, vídeos

Navegação web (httpS)

Seu navegador usa o algoritmo RSA para trocar chaves com o servidor e estabelecer uma conexão segura.

2. MÉTODOS DE CRIPTOGRAFIA

d) PADRÕES DE CRIPTOGRAFIA RECOMENDADOS PARA DIFERENTES TIPOS DE DADOS.



O primeiro navegador foi criado em 1990 por Tim Berners-Lee, um cientista da computação britânico.

Campos do certificado

*.google.com

▼ Certificado

Versão

Número de série

Algoritmo de assinatura do certificado

Emissor

▼ Validade

Valor do campo

PKCS #1 SHA-256 com criptografia RSA



- AES (Advanced Encryption Standard)
- RSA (Rivest-Shamir-Adleman)
- **SHA (Secure Hash Algorithm)**

Garantia de autenticidade.... Importantíssimo.

Resistência a colisões:

Extremamente improvável que duas mensagens diferentes gerem a mesma impressão digital.

Não reversibilidade

Praticamente impossível reverter o processo e recuperar a mensagem original.

Navegação web (httpS)

Usado para calcular uma "impressão digital" do certificado digital, garantindo que o certificado não tenha sido adulterado.

Download de Arquivo.

Nos downloads de arquivos, o site oferece um código hash para validação.

2. MÉTODOS DE CRIPTOGRAFIA

d) PADRÕES DE CRIPTOGRAFIA RECOMENDADOS PARA DIFERENTES TIPOS DE DADOS.



O Projeto Manhattan foi um programa ultrassecreto do governo dos EUA durante a Segunda Guerra Mundial para desenvolver a primeira bomba atômica.

Campos do certificado

*.google.com

osdn.net/projects/hash-linux/downloads/75117/Hash-I-AWESOME-2021.05.13-x86_64.iso/

Gmail YouTube Maps

Download Magazine Develop

OSDN > Find Software > Hash Linux > Download File List > Download

Hash Linux

Description Downloads


Download of AWESOME HASH-AWESOME-I-20210513-213234 (Hash-I-AWESOME-2021.05.13-x86_64.iso: 2,039,164,928 bytes) will be signed with AWESOME-2021.05.13-x86_64.iso.

Valor

File Information

File Size	2,039,164,928 bytes
MD5	51b9f9e989c63cde7111c5c9fb3c6f
SHA1	74539d536e2046c768748673e7c88246a33d967
SHA256	cd42207d446cd21ab6305206a9ca21ed2ae1a960215d97d3bbe3fbed997125db

Where do you want to go next?

- 
1. INTRODUÇÃO A SEGURANÇA DE SOFTWARE
 2. MÉTODOS DE CRIPTOGRAFIA
 3. **PROTOCOLOS DE COMUNICAÇÃO SEGURA**
 - a) MODELO REFERENCIAL OSI
 - b) PRINCIPAIS PROTOCOLOS
 4. SEGURANÇA NO DESENVOLVIMENTO DE SOFTWARE
 5. PROBLEMAS COMUNS DE SEGURANÇA INDICADOS PELA OWASP
 6. AUTENTICAÇÃO E AUTORIZAÇÃO

a) MODELO REFERENCIAL OSI

Protocolos são **conjuntos** de **regras** e procedimentos que permitem a **troca** de informações entre sistemas computacionais, **dispositivos** eletrônicos de uma rede de computadores.



- VISÃO GERAL DO MODELO OSI
- AS 7 CAMADAS DO MODELO OSI



- Interconexão de sistemas
- Facilita solução dos problemas por facilitar a identificação



- **Visão Geral do modelo OSI**
- As 7 camadas do modelo OSI

a) MODELO REFERENCIAL OSI

É um modelo teórico de rede que **define** sete **camadas** diferentes que descrevem **como** os **dispositivos** de rede devem se **comunicar** entre si.

Surgimento

O modelo OSI (Open Systems Interconnection) foi desenvolvido pela ISO (*International Organization for Standardization*) no final da década de 1970 e início da década de 1980.

Objetivo

Interoperabilidade entre dispositivos e serviços de rede de diferentes fabricantes.

Exemplo

Um computador que se **conecta** a uma rede Ethernet utiliza as **camadas física** e de **enlace** do modelo OSI para enviar e receber dados.





- Visão Geral do modelo OSI
- As 7 camadas do modelo OSI

Cada **camada** tem uma função específica na **comunicação** entre dispositivos de rede e é responsável por se comunicar com a sua **camada** mais **próxima**.

As camadas:

Cada camada é **independente** das outras camadas, mas **trabalha** em **conjunto** para permitir a comunicação entre dispositivos de rede.

Organização

As camadas oferecem uma estrutura organizada para entender como os dispositivos de rede se comunicam.

Exemplo

Usado como uma ferramenta de ensino para compreender os conceitos básicos de redes de computadores e protocolos de comunicação.

a) MODELO REFERENCIAL OSI



O Tor é um navegador que fornece navegação anônima e segura na internet. Seu símbolo é uma cebola como alusão as camadas de criptografia.





- Visão Geral do modelo OSI
- As 7 camadas do modelo OSI

a) MODELO REFERENCIAL OSI





- Visão Geral do modelo OSI
- **As 7 camadas do modelo OSI**

a) MODELO REFERENCIAL OSI



HTTP, SMTP, FTP.

SSL/TLS

NetBIOS, NFS ,RPC

TCP, UDP

IP, ICMP

ARP, PPP, MAC.

Ethernet, Wi-Fi, Fibre Channel....



b) PRINCIPAIS PROTOCOLOS

Protocolos permitem que os **dispositivos** de rede troquem **informações** e dados de maneira **estruturada** e organizada, independentemente de sua origem ou destino.



- TCP/IP (Transmission Control Protocol/Internet Protocol)
- HTTP/HTTPS (Hypertext Transfer Protocol/HTTP Secure)
- FTP/FTPS (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- DNS (Domain Name System)
- LIBSIGNAL (criptografia de ponta a ponta)



- Segurança e garantia de entrega
- Flexibilidade de uso para os desenvolvedores



- **TCP/IP (Transmission Control Protocol/Internet Protocol)**
- HTTP/HTTPS (Hypertext Transfer Protocol/HTTP Secure)
- FTP/FTPS (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- DNS (Domain Name System)
- LIBSIGNAL (criptografia de ponta a ponta)

3. PROTOCOLOS DE COMUNICAÇÃO SEGURA

b) PRINCIPAIS PROTOCOLOS



....

O TCP (Transmission Control Protocol) permite a comunicação entre dispositivos em uma rede IP de computadores.

Confiabilidade:

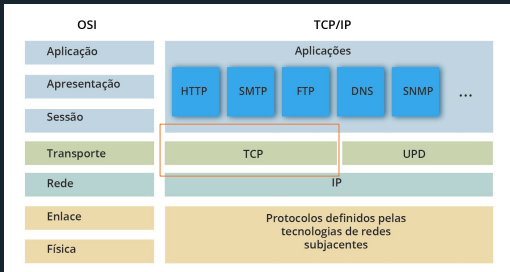
Comunicação entre dispositivos em uma rede IP. Usa o TCP para **estabelecer** e **manter** conexões de rede confiáveis.

Interoperabilidade:

Utilizado em **redes** baseadas em protocolo **IP**, incluindo a **Internet** e muitas redes corporativas.

Flexibilidade:

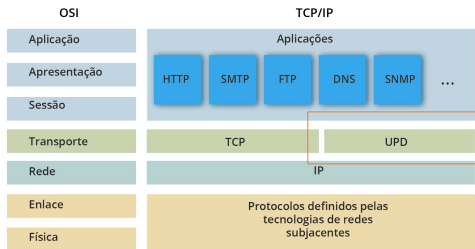
Permite que o **desenvolvedor escolha** os protocolos de transporte e aplicação que melhor atendam às **necessidades da aplicação**.





- **TCP/IP (Transmission Control Protocol/Internet Protocol)**
- HTTP/HTTPS (Hypertext Transfer Protocol/HTTP Secure)
- FTP/FTPS (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- DNS (Domain Name System)
- LIBSIGNAL (criptografia de ponta a ponta)

Os protocolos TCP e UDP oferecem diferentes níveis de confiabilidade e controle de fluxo de dados.



3. PROTOCOLOS DE COMUNICAÇÃO SEGURA

b) PRINCIPAIS PROTOCOLOS



Sem garantia

É um protocolo **sem conexão** que não oferece garantias de entrega ou controle de fluxo.

Rápido

Ideal para aplicações que não exigem uma entrega confiável de dados e podem tolerar perda ou duplicação de pacotes.

Exemplo:

Aplicações que **não requerem** uma entrega confiável, como jogos online, serviços de streaming de áudio e vídeo.



- TCP/IP (Transmission Control Protocol/Internet Protocol)
- **HTTP/HTTPS (Hypertext Transfer Protocol/HTTP Secure)**
- FTP/FTPS (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- DNS (Domain Name System)
- LIBSIGNAL (criptografia de ponta a ponta)

3. PROTOCOLOS DE COMUNICAÇÃO SEGURA

b) PRINCIPAIS PROTOCOLOS

Utilizado para a comunicação entre um **navegador web** e um **servidor web**.

Servidor Web

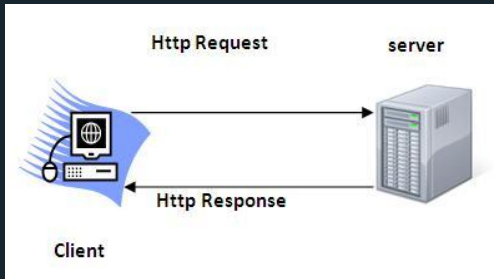
Protocolo **define** como as solicitações de páginas web são feitas pelo navegador e como as respostas são enviadas pelo servidor.

Segurança

O HTTPS é uma extensão do HTTP que utiliza protocolo TLS para garantir a segurança na transmissão de dados.

Exemplo:

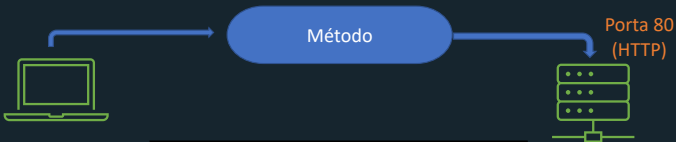
Protege informações confidenciais, como **senhas** e informações de pagamento, **durante a transmissão** pela internet.





- TCP/IP (Transmission Control Protocol/Internet Protocol)
- **HTTP/HTTPS (Hypertext Transfer Protocol/HTTP Secure)**
- FTP/FTPS (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- DNS (Domain Name System)
- LIBSIGNAL (criptografia de ponta a ponta)

Quando o **servidor** web **recebe** a solicitação, ele analisa a URL para determinar qual recurso está sendo solicitado.



```
PUT /exemplo.php?id=10 HTTP/1.1
Host: www.exemplo.com
Content-Type: application/json

{"nome":"Joao","idade":25}
```

3. PROTOCOLOS DE COMUNICAÇÃO SEGURA

b) PRINCIPAIS PROTOCOLOS

GET

Usado para solicitar um recurso específico do servidor.

POST

Usado para enviar dados ao servidor.

PUT

Usado para atualizar um recurso específico no servidor.

DELETE

Usado para excluir um recurso específico do servidor.

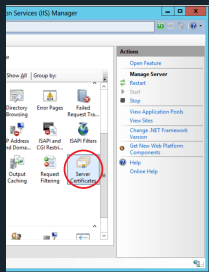
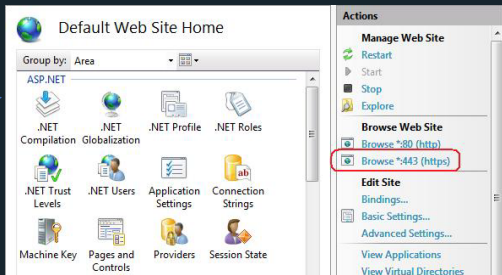


- TCP/IP (Transmission Control Protocol/Internet Protocol)
- **HTTP/HTTPS (Hypertext Transfer Protocol/HTTP Secure)**
- FTP/FTPS (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- DNS (Domain Name System)
- LIBSIGNAL (criptografia de ponta a ponta)

3. PROTOCOLOS DE COMUNICAÇÃO SEGURA

b) PRINCIPAIS PROTOCOLOS

O certificado digital deve gerado por uma Autoridade Certificadora. Uma opção **gratuita** é o Let's Encrypt, que também é uma CA.



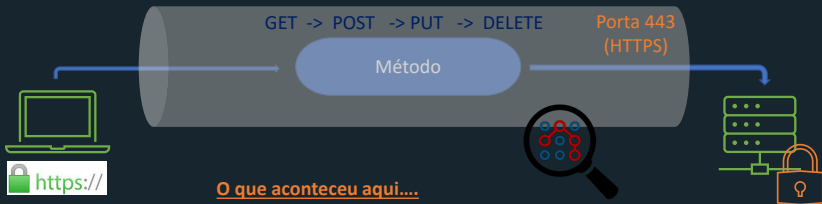


- TCP/IP (Transmission Control Protocol/Internet Protocol)
- **HTTP/HTTPS (Hypertext Transfer Protocol/HTTP Secure)**
- FTP/FTPS (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- DNS (Domain Name System)
- LIBSIGNAL (criptografia de ponta a ponta)

3. PROTOCOLOS DE COMUNICAÇÃO SEGURA

b) PRINCIPAIS PROTOCOLOS

Uma solicitação contém várias informações importantes.



O que aconteceu aqui....

- Troca de chaves RSA (assimétrico)
- Certificado Digital Assinado com SHA (hash)
- Criptografia AES 256 (Simétrica)



- TCP/IP (Transmission Control Protocol/Internet Protocol)
- HTTP/HTTPS (Hypertext Transfer Protocol/HTTP Secure)
- **FTP/FTPS (File Transfer Protocol)**
- SMTP (Simple Mail Transfer Protocol)
- DNS (Domain Name System)
- LIBSIGNAL (criptografia de ponta a ponta)

3. PROTOCOLOS DE COMUNICAÇÃO SEGURA

b) PRINCIPAIS PROTOCOLOS

Utilizado para a transferência de arquivos entre sistemas em uma rede.

Protocolo:

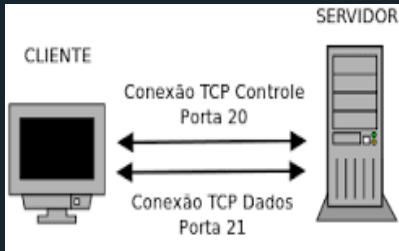
O FTP é um protocolo **não seguro**, o que significa que os dados são transmitidos em **texto simples**.

Autenticação:

Usa autenticação **de usuário e senha** para acessar o servidor. O cliente fornece suas credenciais de login e o servidor verifica se elas são válidas

Exemplo:

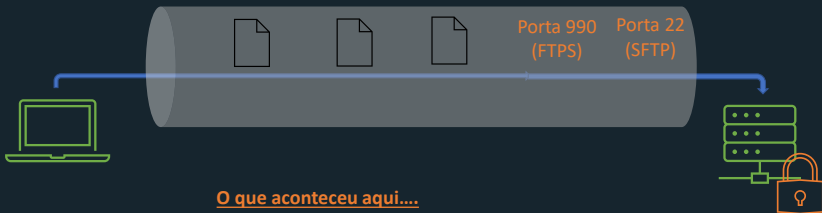
Um site que precisa ser atualizado regularmente com novas imagens, arquivos de áudio, etc.



b) PRINCIPAIS PROTOCOLOS



- TCP/IP (Transmission Control Protocol/Internet Protocol)
- HTTP/HTTPS (Hypertext Transfer Protocol/HTTP Secure)
- **FTP/FTPS (File Transfer Protocol)**
- SMTP (Simple Mail Transfer Protocol)
- DNS (Domain Name System)
- LIBSIGNAL (criptografia de ponta a ponta)



O que aconteceu aqui....

- Troca de chaves RSA (assimétrico)
- Certificado Digital Assinado com SHA (hash)
- Criptografia AES 256 (Simétrica)



- TCP/IP (Transmission Control Protocol/Internet Protocol)
- HTTP/HTTPS (Hypertext Transfer Protocol/HTTP Secure)
- FTP/FTPS (File Transfer Protocol)
- **SMTP (Simple Mail Transfer Protocol)**
- DNS (Domain Name System)
- LIBSIGNAL (criptografia de ponta a ponta)

3. PROTOCOLOS DE COMUNICAÇÃO SEGURA

b) PRINCIPAIS PROTOCOLOS

Utilizado para enviar e receber e-mails na internet.

Protocolo:

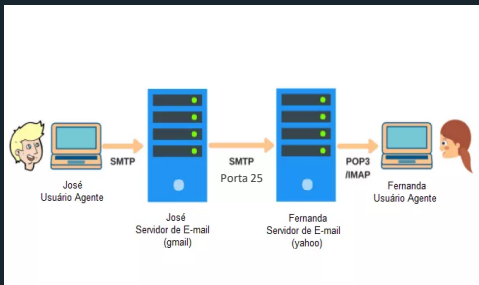
Define como os **servidores** de e-mail trocam mensagens entre si e como as mensagens são **entregues**.

Autenticação:

Garantir que os servidor de origem tem **autenticidade** para enviar e-mail **em nome** de um determinado **domínio**.

Envio de email:

Ao enviar um e-mail para um amigo, o servidor utiliza o SMTP para enviar a mensagem ao servidor de destino do e-mail. Este utiliza SMTP para entregar para o destinatário.



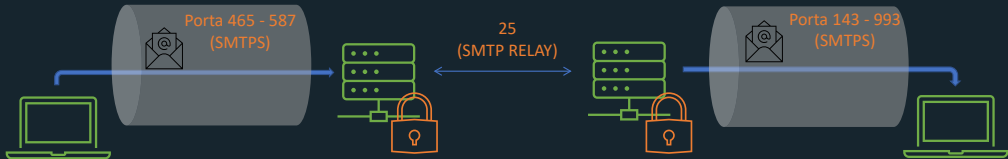


- TCP/IP (Transmission Control Protocol/Internet Protocol)
- HTTP/HTTPS (Hypertext Transfer Protocol/HTTP Secure)
- FTP/FTPS (File Transfer Protocol)
- **SMTP (Simple Mail Transfer Protocol)**
- DNS (Domain Name System)
- LIBSIGNAL (criptografia de ponta a ponta)

3. PROTOCOLOS DE COMUNICAÇÃO SEGURA

b) PRINCIPAIS PROTOCOLOS

O SMTP define uma série de comandos e respostas para a transmissão de mensagens de e-mail.



O que aconteceu aqui....

- Troca de chaves RSA (assimétrico)
- Certificado Digital Assinado com SHA (hash)
- Criptografia AES 256 (Simétrica)



- TCP/IP (Transmission Control Protocol/Internet Protocol)
- HTTP/HTTPS (Hypertext Transfer Protocol/HTTP Secure)
- FTP/FTPS (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- **DNS (Domain Name System)**
- LIBSIGNAL (criptografia de ponta a ponta)

Utilizado para traduzir nomes de domínio em endereços IP na internet.

Tradução:

Ele permite que os usuários acessem sites e serviços na internet por meio de nomes de domínio, em vez de endereços IP.

Hierarquia

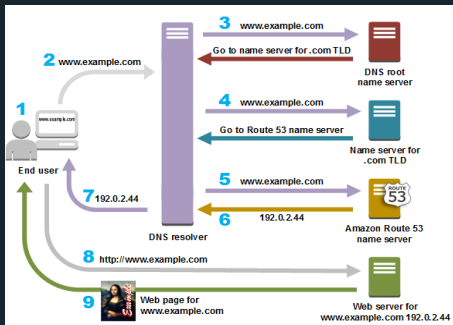
O DNS utiliza uma hierarquia de servidores para armazenar e distribuir informações sobre nomes de domínio e seus correspondentes endereços IP.

Exemplo:

Ao digitar o endereço de um site na barra de endereço do seu navegador, o navegador envia uma solicitação DNS para o servidor DNS do seu provedor de internet.

3. PROTOCOLOS DE COMUNICAÇÃO SEGURA

b) PRINCIPAIS PROTOCOLOS





- TCP/IP (Transmission Control Protocol/Internet Protocol)
- HTTP/HTTPS (Hypertext Transfer Protocol/HTTP Secure)
- FTP/FTPS (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- **DNS (Domain Name System)**
- LIBSIGNAL (criptografia de ponta a ponta)

3. PROTOCOLOS DE COMUNICAÇÃO SEGURA

b) PRINCIPAIS PROTOCOLOS

Como é feito o registro do nome

Registro.br:

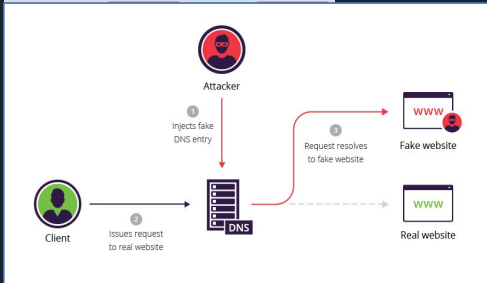
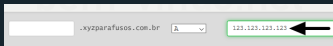
Responsável pela tradução de nomes do .BR. O serviço é mantido pela FAPESP.

Hierarquia

O registro.br tem autorização e está configurado do TLD para responder pelo subdomínios de .BR.

Exemplo:

Ao procurar pelo endereço **xyzparafusos.com.br**, o registro.BR informa qual o IP do servidor web da xyzparafusos.com.br.





- TCP/IP (Transmission Control Protocol/Internet Protocol)
- HTTP/HTTPS (Hypertext Transfer Protocol/HTTP Secure)
- FTP/FTPS (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- DNS (Domain Name System)
- **LIBSIGNAL (criptografia de ponta a ponta)**

A segurança das comunicações dos usuários é uma responsabilidade importante

Porque é importante:

Cada vez mais os usuários buscam privacidade e segurança em suas trocas de mensagens.

Segurança

Protocolo de criptografia de ponta a ponta.

Exemplo

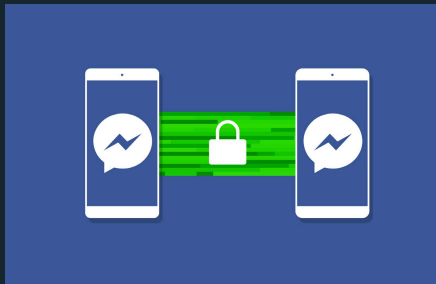
Usado em aplicativos de mensagens criptografadas, como Signal, WhatsApp e Facebook Messenger.

3. PROTOCOLOS DE COMUNICAÇÃO SEGURA

b) PRINCIPAIS PROTOCOLOS



Libsignal foi desenvolvida originalmente por Moxie Marlinspike e Trevor Perrin em 2013 para uso no aplicativo de mensagens Signal.





- TCP/IP (Transmission Control Protocol/Internet Protocol)
- HTTP/HTTPS (Hypertext Transfer Protocol/HTTP Secure)
- FTP/FTPS (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- DNS (Domain Name System)
- **LIBSIGNAL (criptografia de ponta a ponta)**

3. PROTOCOLOS DE COMUNICAÇÃO SEGURA

b) PRINCIPAIS PROTOCOLOS

Implementar o protocolo libsignal em seu próprio projeto.

Código-fonte

Pode ser baixado e incorporado ao seu projeto
<https://signal.org/docs/>

Funcionalidades

Oferece várias funcionalidades, como a **geração de chaves criptográficas....**

Documentação

É extensa e **detalhada**. Leia a documentação para entender como o **protocolo funciona**.

Configurar chaves

Você precisará **configurar** as **chaves** criptográficas dos **usuários** para que eles possam trocar mensagens.

Criptografia de chave pública

Cada **usuário** tem um par de chaves, uma **pública** e outra **privada**.

API local ou da Signal

Pode-se usar um **servidor de API** de terceiros para enviar e receber mensagens criptografadas.



- TCP/IP (Transmission Control Protocol/Internet Protocol)
- HTTP/HTTPS (Hypertext Transfer Protocol/HTTP Secure)
- FTP/FTPS (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- DNS (Domain Name System)
- **LIBSIGNAL (criptografia de ponta a ponta)**

Passo a Passo

1 – Servidor

git clone <https://github.com/signalapp/libsignal-protocol-javascript.git>

2 - Dependências:

npm install

3 – Importar modulo libsignal

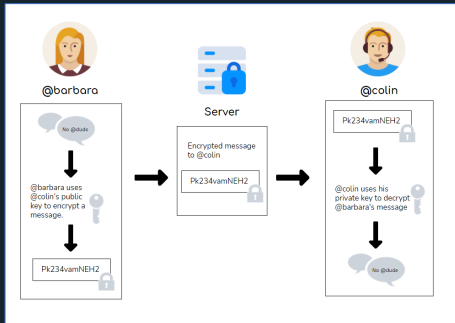
```
const libsignal = require('libsignal');
```

4 – Código

```
const message = 'Olá, como vai?';  
const recipientId = 'usuário-destino';  
.....
```

3. PROTOCOLOS DE COMUNICAÇÃO SEGURA

b) PRINCIPAIS PROTOCOLOS



PUCRS online  **uol** edtech.