



Criptografia

```
>> echo "Segurança de Computadores" |
```



Retomando a Aula Anterior: O Cenário das Ameaças Cibernéticas

- Na nossa última aula, exploramos diversos tipos de ataques cibernéticos que representam sérias ameaças à segurança de sistemas e dados.
- Discutimos como esses ataques podem comprometer a confidencialidade, integridade e disponibilidade das informações.
- Um dos ataques que ganhou destaque foi o **Ransomware**.

Ransomware: O Sequestro Digital e suas Consequências

- Ransomware: Tipo de malware que **criptografa** os arquivos da vítima, tornando-os inacessíveis. Os atacantes exigem um resgate (ex: criptomoedas) para fornecer a chave de descriptografia.
 - Geralmente se infiltra nos sistemas através de e-mails de phishing, exploração de vulnerabilidades de software ou downloads maliciosos.
- Impacto:
 - Perda de acesso a dados críticos.
 - Interrupção de operações e prejuízos financeiros significativos.
 - Danos à reputação e perda de confiança.
- Vulnerabilidade Explícita: O ransomware explora a falta de proteção adequada dos dados, tornando a **criptografia** uma arma contra a vítima.

Criptografia

- A arte e a ciência de codificar informações de forma que apenas pessoas autorizadas possam lê-las.
- Objetivo principal: garantir a **confidencialidade** dos dados.



Criptografia: um pouco de história

A história é marcada por códigos que decidiram o resultado de batalhas, provocando a morte de reis e rainhas.

Uma Jornada Através do Tempo: A História da Criptografia

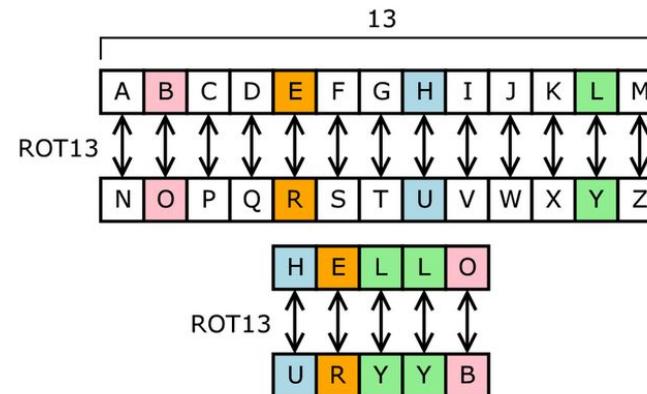
- **Antiguidade:** Cifras simples como a Cifra de César.
- **Idade Média:** Desenvolvimento de cifras mais complexas e a importância da criptografia em contextos militares e diplomáticos.
- **Renascimento:** Surgimento de técnicas mais sofisticadas e a formalização de alguns conceitos.
- **Século XX:** A revolução da criptografia com a Segunda Guerra Mundial e o desenvolvimento de máquinas como a Enigma. O nascimento da criptografia moderna com a teoria da informação e a computação.
- **Século XXI:** A criptografia como pilar da segurança na internet, comércio eletrônico, comunicação e proteção de dados em larga escala.

Uma Jornada Através do Tempo: A História da Criptografia



Cifra de César

- Método de criptografia de substituição simples
- Cada letra de um texto é substituída por outra, deslocada um número fixo de posições no alfabeto.



Ver: <https://www.101computing.net/cipher-wheel.html>

Uma Jornada Através do Tempo: A História da Criptografia



Idade Média

- Guerra dos Cem Anos (1337–1453)
 - Inglaterra vs. França: Ambos os lados usavam cifras simples para coordenar tropas.

Uma Jornada Através do Tempo: A História da Criptografia



Idade Média

- Papado e Criptografia
 - Papa Clemente VII: Usava cifras para comunicar alianças contra o Sacro Império Romano.
 - Método: Substituição com símbolos religiosos (ex.: + para A, ✠ para B).



Uma Jornada Através do Tempo: A História da Criptografia



Idade Média

- Criptoanálise Medieval
 - Quebra de Cifras: Árabes foram pioneiros em análise de frequência (século IX).
 - Al-Kindi: Descreveu como identificar letras repetidas em cifras de substituição.

Uma Jornada Através do Tempo: A História da Criptografia



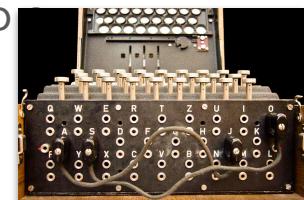
Idade Média

- Cifra de Vigenère (século XVI, mas baseada em métodos medievais)
 - Considerada inquebrável por 300 anos
- Usa uma chave alfabética para deslocar letras (polialfabética).
 - Mensagem: ATACAR
 - Chave: REI (repete-se: REIREI)
 - Texto cifrado: Cada letra de ATACAR é deslocada pelo valor da chave REIREI:
 - $A + R = 0 + 17 = 17 \rightarrow R$
 - $T + E = 19 + 4 = 23 \rightarrow X$
 - Resultado: RXRCGR

Uma Jornada Através do Tempo: A História da Criptografia

🔒 Século XX:

- Enigma: máquina de criptografia eletromecânica utilizada pela Alemanha nazista durante a Segunda Guerra Mundial para codificar e decodificar mensagens militares.
- Como funcionava:
 - Utilizava rotores que giravam ao pressionar uma tecla do teclado, alterando o código da mensagem.
 - A máquina tinha um refletor que devolvia as letras processadas pelos rotores, criando um padrão de cifragem.
 - A posição dos rotores e do refletor eram configuráveis, aumentando a complexidade do sistema de cifragem.



Tipos de Criptografia

- A criptografia pode ser amplamente classificada em duas categorias principais, baseadas no tipo de chave utilizada:
 - Criptografia Simétrica (Chave Secreta)
 - Criptografia Assimétrica (Chave Pública)

Criptografia Simétrica

- Utiliza a mesma chave secreta para criptografar e decriptografar os dados.
- A chave deve ser conhecida tanto pelo remetente quanto pelo destinatário.
- Analogia: Imagine uma caixa trancada com uma única chave. Quem tem a chave pode trancar (criptografar) e destrancar (decriptografar) a caixa.

Criptografia Simétrica



Principais Algoritmos de Criptografia Simétrica

- DES (*Data Encryption Standard*): Um dos primeiros algoritmos amplamente utilizados, considerado inseguro atualmente devido ao tamanho da chave (56 bits).
- 3DES (*Triple DES*): Uma evolução do DES que aplica o algoritmo três vezes para aumentar a segurança. Mais lento que outros algoritmos modernos.
- AES (*Advanced Encryption Standard*): O padrão atual, considerado seguro e eficiente. Utiliza tamanhos de chave de 128, 192 ou 256 bits.
- Blowfish e Twofish: Outros algoritmos simétricos robustos e amplamente utilizados.

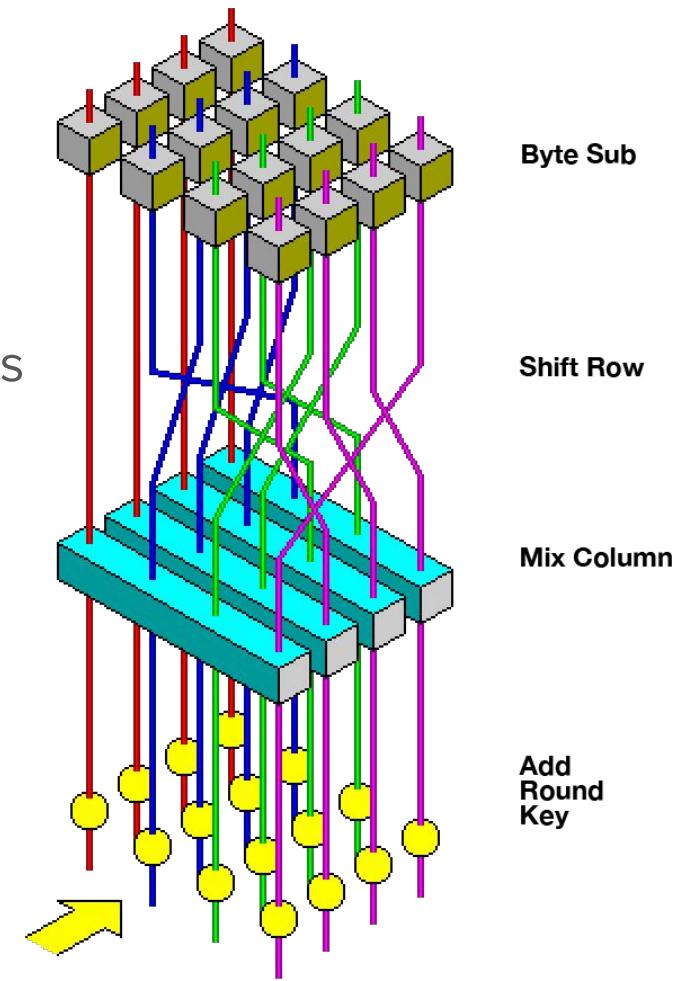
Algoritmo	Tamanho da Chave	Velocidade	Aplicações	Segurança
AES	128, 192, 256 bits	⚡ ⚡ ⚡ ⚡ ⚡	HTTPS, VPN, arquivos	★★★★★ (NIST-approved)
ChaCha20	256 bits	⚡ ⚡ ⚡ ⚡ ⚡	WhatsApp, TLS 1.3	★★★★★
3DES	168 bits	⚡ ⚡	Sistemas legados (banco)	★★ (Obsoleto)



- AES-256 é o padrão ouro (usado pelo governo dos EUA para documentos secretos).
- ChaCha20 é mais rápido em dispositivos móveis.

AES: funcionamento

- Processo (Simplificado):
 - Divisão em Blocos: Dados são divididos em blocos de 128 bits.
 - Substituição e Permutação: Usa operações matemáticas (SubBytes, ShiftRows, MixColumns).
 - Rounds: Repete o processo 10–14 vezes (dependendo do tamanho da chave).



AES

- Criptografar:

```
$ gpg --cipher-algo AES256 --symmetric filename
```

```
$ gpg --cipher-algo AES256 -c filename
```

- Pede por senha
- Gera arquivo cifrado: filename_cypher.gpg

- Descriptografar

```
$ gpg --output filename --decrypt filename_cypher.gpg
```

```
$ gpg -o filename -d filename_cypher.gpg
```

Vantagens da Criptografia Simétrica

- **Velocidade:** Geralmente mais rápida e eficiente computacionalmente do que a criptografia assimétrica.
- **Simplicidade:** O conceito e a implementação são relativamente mais simples.
- **Adequada para grandes volumes de dados:** A velocidade a torna ideal para criptografar grandes quantidades de informações.

Desvantagens da Criptografia Simétrica

- **Gerenciamento de Chaves:** O principal desafio é a distribuição segura da chave secreta entre o remetente e o destinatário antes da comunicação criptografada.
- **Escalabilidade:** Em um sistema com muitos participantes, o gerenciamento de um grande número de chaves secretas compartilhadas torna-se complexo.
- **Falta de Não Repúdio:** Não oferece uma maneira direta de provar a autoria da mensagem, pois ambos os participantes possuem a mesma chave

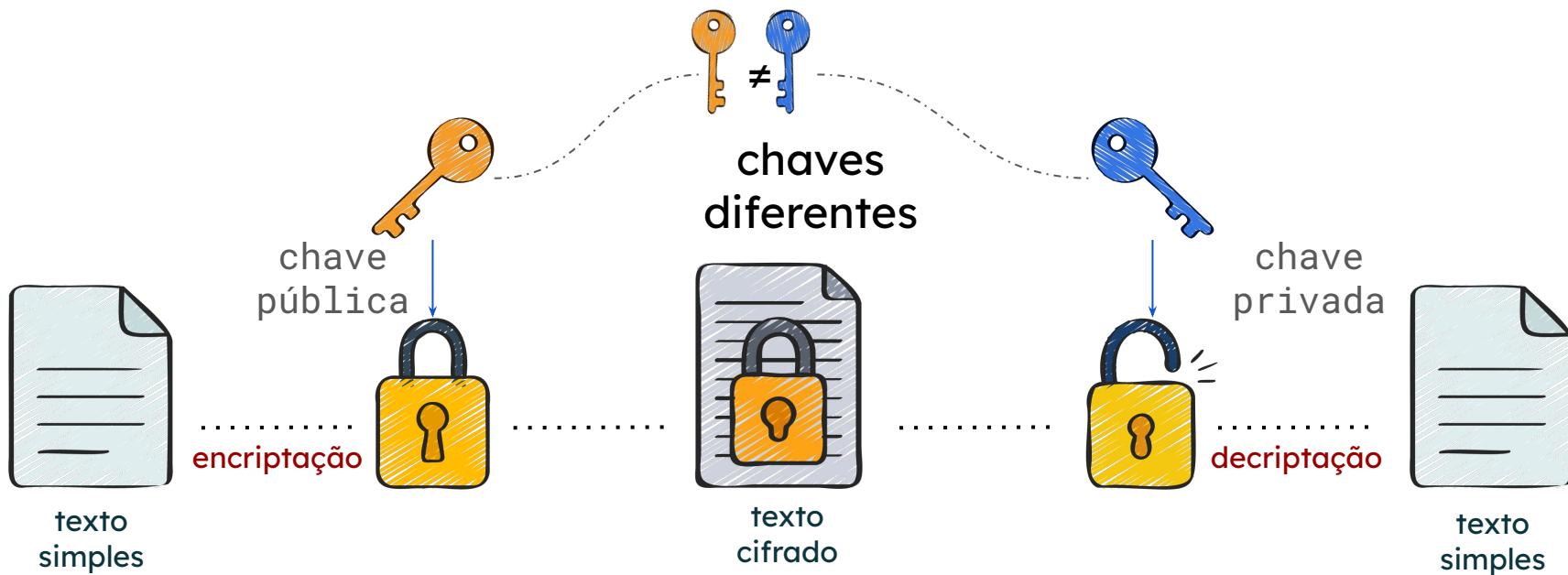
Criptografia Assimétrica

- Utiliza um **par de chaves** relacionadas: uma chave pública e uma chave privada.
- **Chave Pública:** Pode ser compartilhada livremente com qualquer pessoa.
- **Chave Privada:** Deve ser mantida em segredo pelo seu proprietário.

Criptografia Assimétrica

- Se os dados são criptografados com a **chave pública** do destinatário, somente a **chave privada** correspondente pode descriptografá-los.
- Se os dados são criptografados com a **chave privada** do remetente, a **chave pública** correspondente pode descriptografá-los (usado para assinatura digital).

Criptografia Assimétrica



Algoritmos de Criptografia Assimétrica Comuns

- RSA (Rivest–Shamir–Adleman): Um dos primeiros e mais amplamente utilizados algoritmos assimétricos. Sua segurança se baseia na dificuldade de fatorar grandes números primos.
- DSA (Digital Signature Algorithm): Usado principalmente para assinaturas digitais.
- ECDSA (Elliptic Curve Digital Signature Algorithm): Uma variante do DSA que utiliza curvas elípticas, oferecendo segurança semelhante com chaves menores.
- Diffie-Hellman: Um protocolo para troca segura de chaves simétricas sobre um canal inseguro.
- ElGamal: Outro algoritmo de chave pública usado para criptografia e assinatura digital.

Algoritmo	Base Matemática	Tamanho da Chave	Aplicações	Segurança
RSA	Fatoração de primos	2048–4096 bits	Certificados SSL, PIX	★★★★ (Vulnerável a quantum)
ECDSA	Curvas elípticas	256–521 bits	Bitcoin, assinaturas digitais	★★★★★
EdDSA	Curvas elípticas (Twisted)	256 bits	SSH, TLS 1.3	★★★★★



RSA é o mais conhecido, mas exige chaves grandes.

ECDSA é mais eficiente (ex.: chave de 256 bits ≈ segurança de RSA 3072 bits).

Vantagens da Criptografia Assimétrica

- **Gerenciamento de Chaves Simplificado:** A chave pública pode ser distribuída livremente, eliminando a necessidade de um canal seguro para troca de chaves.
- **Escalabilidade:** Facilita a comunicação segura com um grande número de participantes.
- **Suporte a Não Repúdio:** A chave privada é única para cada indivíduo, permitindo a criação de assinaturas digitais que comprovam a autoria.

Desvantagens da Criptografia Assimétrica

- **Velocidade:** Geralmente mais lenta e computacionalmente mais intensiva do que a criptografia simétrica.
- **Tamanho da Chave:** As chaves assimétricas tendem a ser maiores para oferecer o mesmo nível de segurança que chaves simétricas menores.
- **Complexidade:** Os algoritmos e a implementação são geralmente mais complexos.

Comparativo

Característica	Criptografia Simétrica 	Criptografia Assimétrica 
Chaves utilizadas	Mesma chave para criptografar e descriptografar	Um par de chaves: pública e privada
Velocidade	Mais rápida (GB/s)	Mais lenta (KB/s)
Segurança na troca de chave	Requer canal seguro para troca de chave	Chave pública pode ser compartilhada livremente
Exemplos de algoritmos	AES, DES, RC4	RSA, ECC, ElGamal
Uso típico	Criptografia de dados em massa (ex: arquivos)	Criptografia de dados em massa (ex: arquivos)

Casos de Uso

Criptografia Simétrica:

- Criptografia de grandes volumes de dados (arquivos, discos).
- Comunicações seguras dentro de um sistema fechado onde a chave pode ser gerenciada (ex: comunicação interna de um servidor).
- Protocolos como AES em conexões VPN.

Criptografia Assimétrica:

- Troca segura de chaves para comunicação simétrica (protocolo TLS/SSL).
- Assinaturas digitais para verificar autenticidade e integridade.
- Criptografia de e-mails (PGP/GnuPG).
- Acesso seguro a websites (HTTPS).

Criptografia Híbrida

- Uma abordagem comum que combina o melhor dos dois mundos.
- Utiliza a criptografia assimétrica para trocar de forma segura uma chave simétrica.
- Uma vez que a chave simétrica é compartilhada, a comunicação subsequente utiliza a criptografia simétrica para maior velocidade e eficiência na transferência de grandes volumes de dados.
- Exemplo: O protocolo TLS/SSL (usado em HTTPS) emprega essa abordagem.

Criptografia Híbrida: encriptação



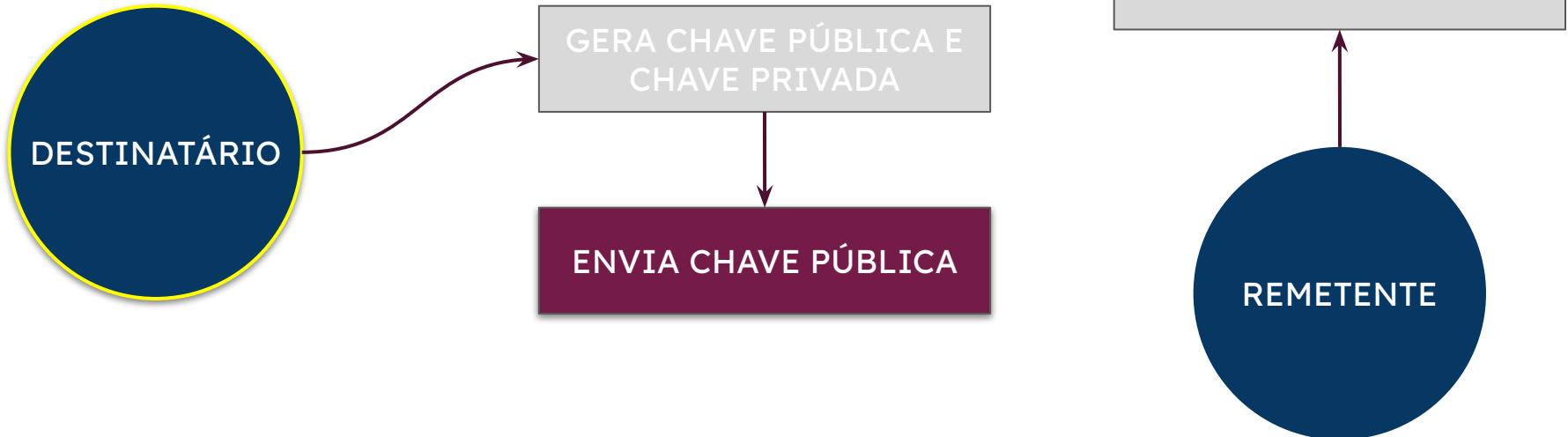
Criptografia Híbrida: encriptação



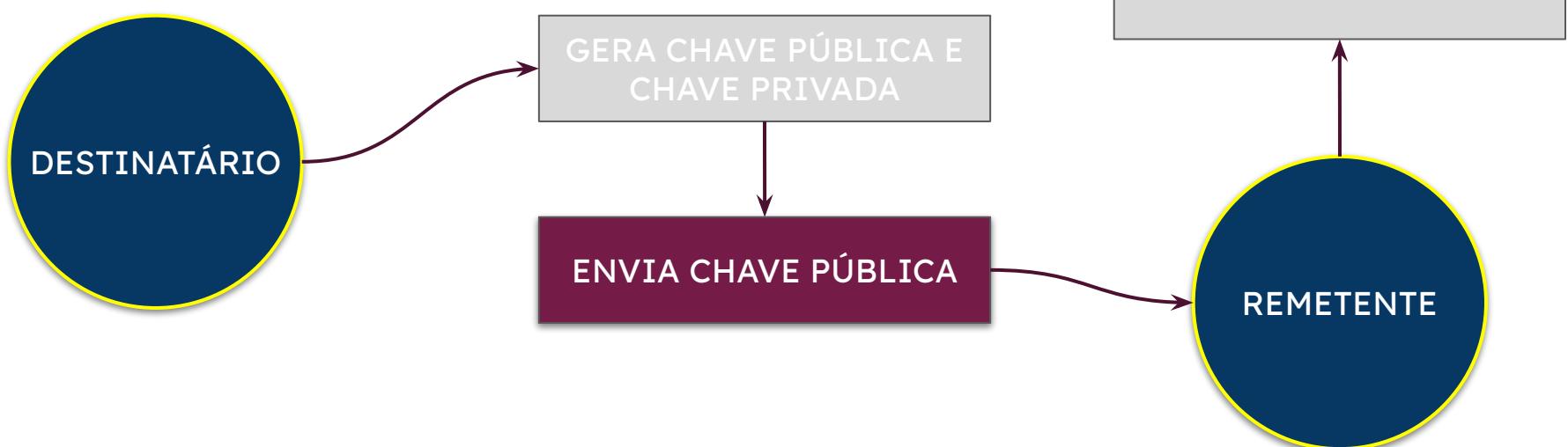
Criptografia Híbrida: encriptação



Criptografia Híbrida: encriptação



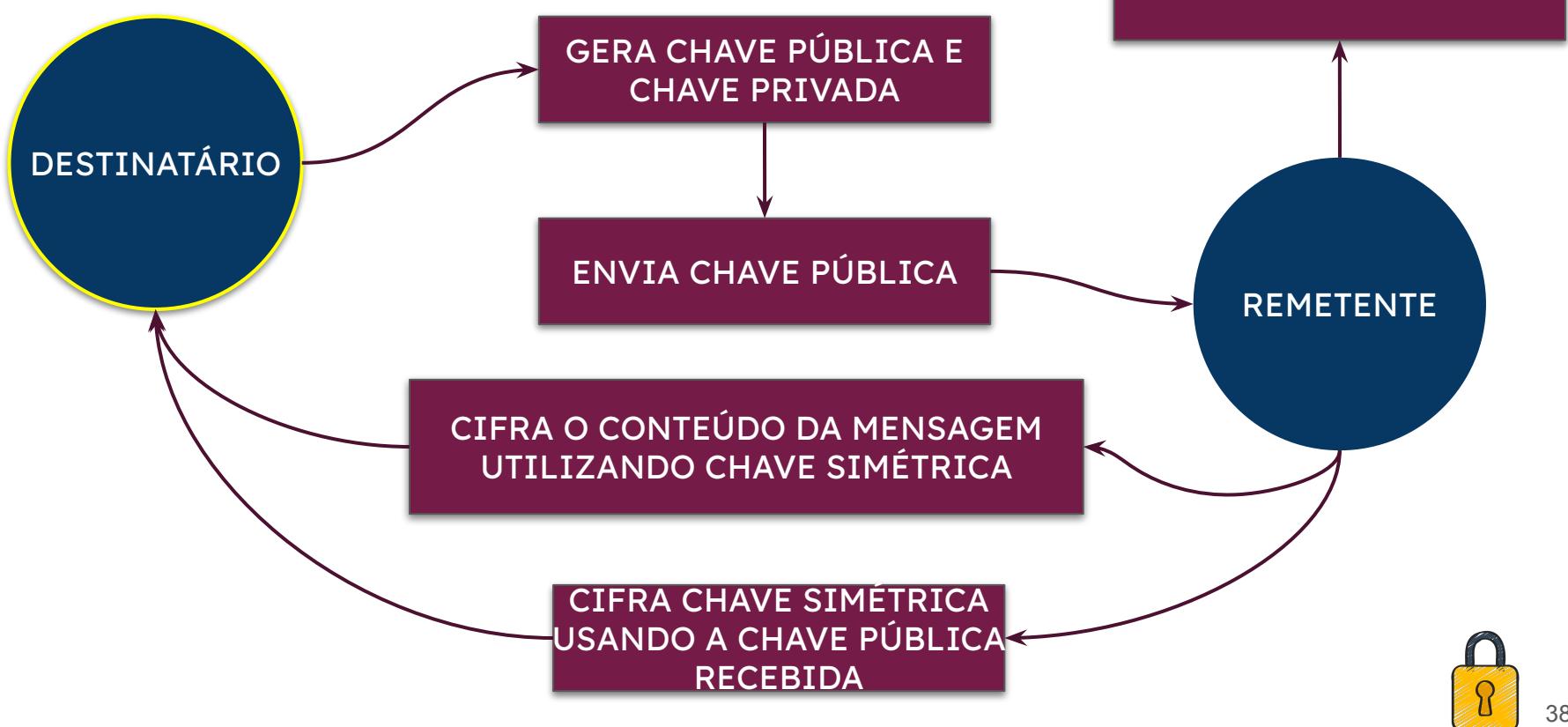
Criptografia Híbrida: encriptação



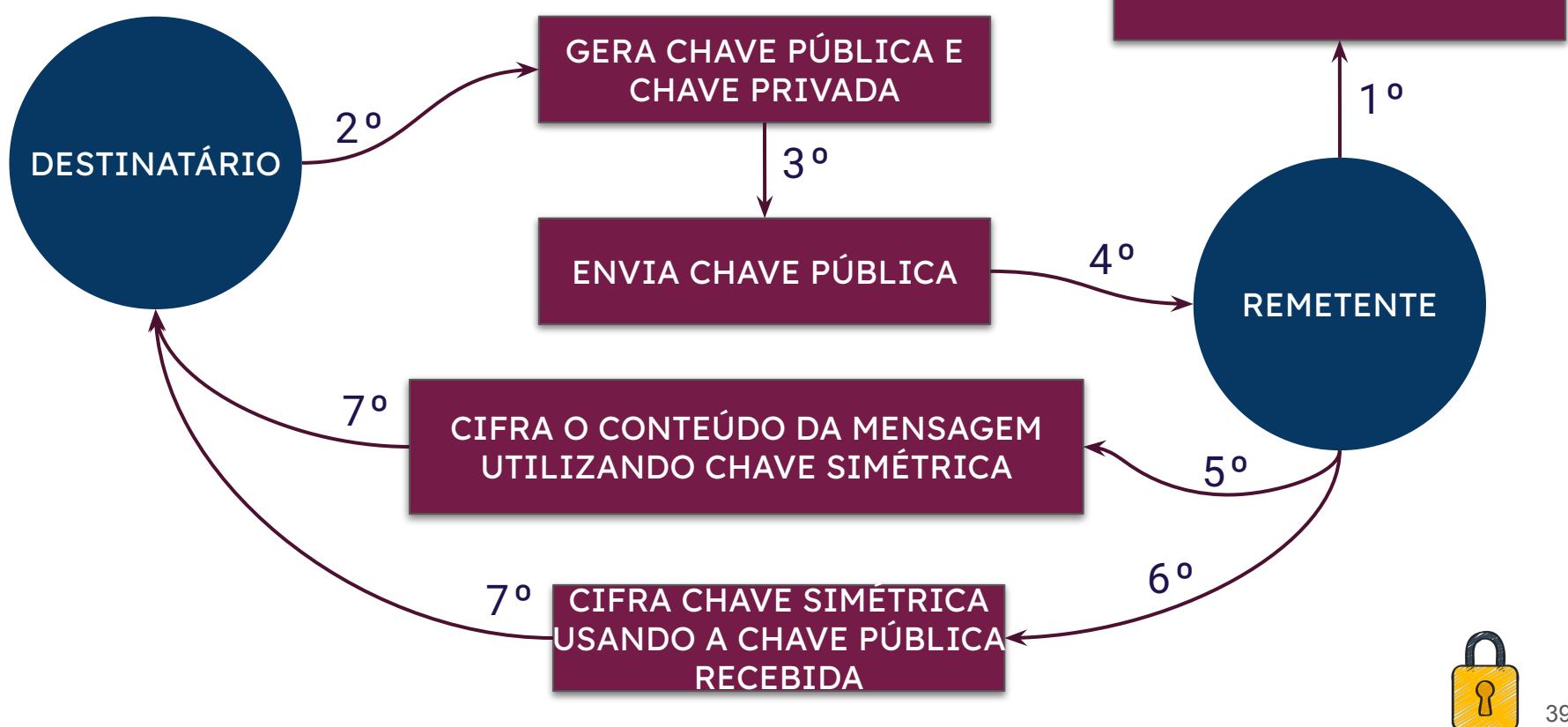
Criptografia Híbrida: encriptação



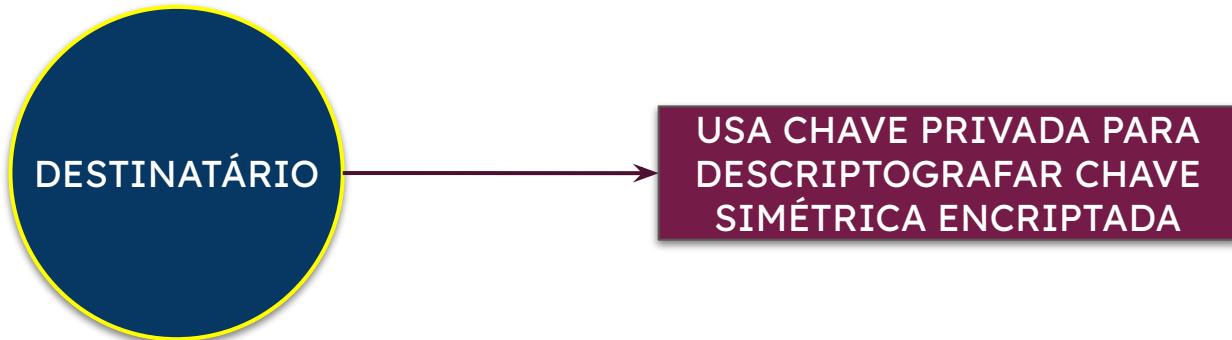
Criptografia Híbrida: encriptação



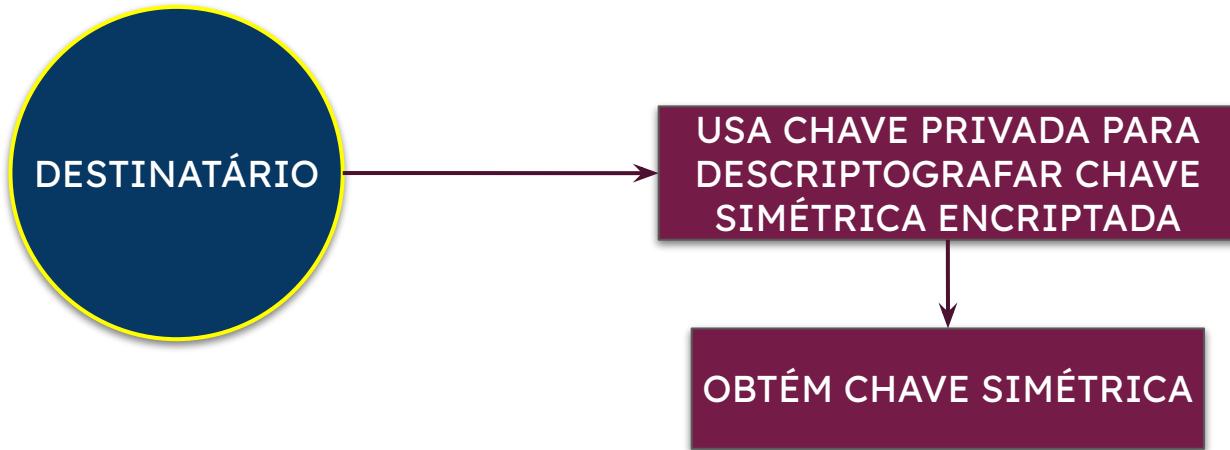
Criptografia Híbrida: encriptação



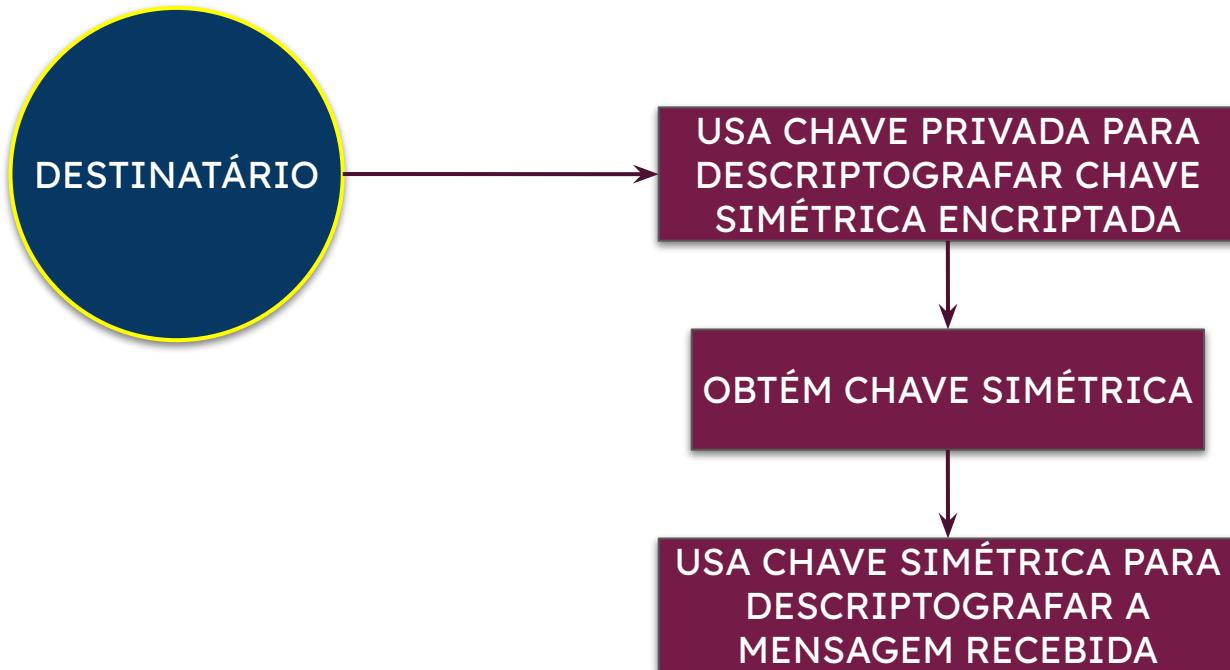
Criptografia Híbrida: decriptação



Criptografia Híbrida: decriptação



Criptografia Híbrida: decriptação



Exemplos

- **TLS/SSL (HTTPS)**
 - Quando acessamos um site seguro (HTTPS), o navegador e o servidor web usam a criptografia híbrida para estabelecer uma conexão segura.
 - Eles usam algoritmos assimétricos (como RSA ou ECDSA) para trocar e autenticar chaves de sessão simétricas (como AES).
 - Toda a comunicação subsequente é criptografada usando essa chave simétrica para velocidade e eficiência.

Exemplos

- **Conexões VPN**
 - Algumas VPNs utilizam a criptografia híbrida durante a fase de handshake para estabelecer um canal seguro, trocando chaves simétricas que serão usadas para criptografar todo o tráfego de dados.

Cenário Híbrido geral

1. RSA criptografa uma chave AES
2. AES criptografa os dados reais
 - Usado em HTTPS, PIX, etc.

Criptografia como Contramedida: Transformando a Vulnerabilidade em Defesa

- Diante de ameaças como o ransomware, a criptografia emerge também como uma ferramenta de defesa fundamental.
- Se os seus dados já estiverem criptografados de forma robusta antes de um ataque de ransomware, os invasores encontrarão arquivos ilegíveis, mesmo que consigam acessá-los.

Criptografia como Contramedida: Transformando a Vulnerabilidade em Defesa

- **Dados Não Criptografados:** Vulneráveis ao sequestro e à extorsão.
- **Dados Fortemente Criptografados:** Inúteis para os atacantes sem a chave correta, tornando o ataque de ransomware ineficaz em relação à confidencialidade dos dados.
- Além do Ransomware: A criptografia também protege contra outras ameaças, garantindo a confidencialidade e integridade dos dados em diversas situações.

Futuro da Criptografia

- Criptografia Pós-Quântica:
 - Algoritmos resistentes a quânticos (ex.: *Lattice-based cryptography*).
- Privacy-Enhancing Tech:
 - ZKP (*Zero-Knowledge Proofs*): Provar conhecimento sem revelar dados
- Regulamentação:
 - Leis como EU Digital Markets Act exigem E2EE para mensagens.

Criptografia Pós-Quântica

- A criptografia pós-quântica é um novo tipo de criptografia projetada para resistir a computadores quânticos, máquinas superpoderosas que podem quebrar os sistemas de segurança atuais.
- Analogia:
 - Pense na criptografia atual como um **cadeado comum**, e nos computadores quânticos como um **super abridor de cadeados**.
 - A criptografia pós-quântica seria um **cadeado à prova desse super abridor**.

Criptografia Pós-Quântica

- Computadores quânticos podem quebrar algoritmos atuais (como RSA e ECC) em segundos, usando o algoritmo de Shor
 - Algoritmo de Shor: algoritmo quântico que permite a fatoração de grandes números inteiros em números primos.
- Isso colocaria em risco:
 - Bancos (transações, PIX).
 - Governos (segredos militares).
 - Blockchain (Bitcoin, contratos inteligentes).
- Exemplo Prático:
 - Se um computador quântico ficar pronto em 2030, todas as senhas e transações criptografadas com RSA poderiam ser decifradas retroativamente.

Considerações

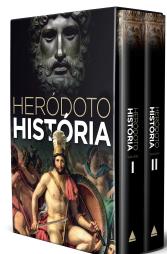
- A criptografia simétrica e assimétrica são ferramentas fundamentais para garantir a segurança e a privacidade das informações no mundo digital.
- Cada tipo possui suas próprias vantagens e desvantagens, tornando-os adequados para diferentes cenários.
- A criptografia híbrida combina os benefícios de ambas as abordagens para oferecer segurança e eficiência.

Criptografia no cenário atual

- Internet Global: 5.3 bilhões de usuários online (2024).
- Ameaças: Ransomware, vazamentos de dados, e espionagem estatal.
- Regulamentações: LGPD, GDPR e outras exigem proteção de dados.
- Dados Chave:
 - 95% do tráfego web é criptografado (HTTPS) — Let's Encrypt, 2024.
 - Mercado de criptografia vale US\$ 50 bilhões (Grand View Research, 2024).

A evolução da escrita secreta

- Alguns dos primeiros relatos sobre escritas secretas datam de Heródoto (484-425 a.C.),
- Heródoto, que escreveu "História", narrou os conflitos entre a Grécia e a Pérsia, ocorridos no quinto século antes de Cristo.
- De acordo com Heródoto, foi a arte da escrita secreta que salvou a Grécia de ser conquistada por Xerxes, Rei dos Reis, o déspota líder dos persas.



Um pouco de história

- A antiga inimizade entre a Grécia e a Pérsia evoluiu para uma crise logo depois que Xerxes começou a construir a cidade de Persépolis, a nova capital de seu reino.
- Presentes e tributos chegaram de todas as regiões do império e dos estados vizinhos, com a notável exceção de Atenas e Esparta.
- Determinado a vingar esta insolência, Xerxes começou a mobilizar um exército e declarou: “Nós devemos estender o império da Pérsia de modo que suas fronteiras sejam o próprio céu de Deus, que o sol não se posicione sobre nenhuma terra além das fronteiras do que é nosso.”
 - Ele passou os cinco anos seguintes montando secretamente a maior força de combate da história

Um pouco de história

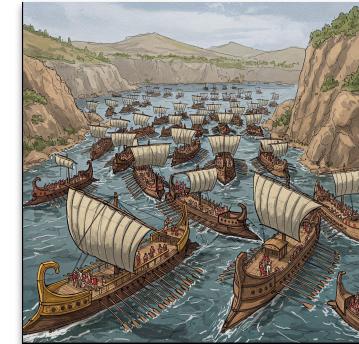
- Então, no ano 480 a.C., ele estava pronto para lançar um ataque-surpresa.
 - Demarato, um grego que fora expulso de sua terra natal e vivia na cidade persa de Susa.
- Apesar de ser um exilado, ele ainda sentia alguma lealdade para com a Grécia e decidiu enviar uma mensagem para advertir os espartanos dos planos de invasão de Xerxes.
 - O desafio era como enviar a mensagem sem que ela fosse interceptada pelas guardas

Um pouco de história

" perigo de ser descoberto era grande; havia apenas um modo pelo qual a mensagem poderia passar: isso foi feito **raspando a cera de um par de tabuletas de madeira, e escrevendo embaixo o que Xerxes pretendia fazer, depois a mensagem foi coberta novamente com cera.** Deste modo, as tabuletas pareceriam estar em branco e não causariam problemas com os guardas ao longo da estrada. Quando a mensagem chegou ao seu destino, ninguém foi capaz de perceber o segredo, até que, pelo que entendi, a filha de Cleômenes, Gorgo, que era casada com Leônidas, adivinhou e contou aos outros que se eles rasgassem a cera encontrariam alguma coisa escrita na madeira. isto foi feito, revelando a mensagem, então transmitida para os outros gregos."

Um pouco de história

- Xerxes perdera o elemento vital da surpresa
- Os persas acreditavam ter encorralado a marinha grega, mas os gregos estavam deliberadamente atraindo seus navios para dentro da baía.
 - dentro do espaço restrito da baía, poderiam manobrar melhor.
- O pânico se instalou, mais navios persas colidiram e os gregos lançaram um ataque total. Em um dia as forças formidáveis da Pérsia tinham sido humilhadas.





Esteganografia

- A esteganografia é a arte e a ciência de ocultar informações dentro de outras informações de forma que a presença da mensagem escondida não seja aparente.
- Grego
 - "*steganos*" → "coberto" ou "oculto"
 - "*graphein*" → "escrita"

Esteganografia: como funciona

- A esteganografia pode ser aplicada a diversos tipos de mídia digital, incluindo:
 - Imagens: A técnica mais comum envolve alterar os bits menos significativos dos pixels de uma imagem. Essas alterações são geralmente imperceptíveis ao olho humano, mas podem ser usadas para codificar dados.
 - Áudio: Mensagens podem ser escondidas em arquivos de áudio através de pequenas alterações no volume, fase ou frequência do som.
 - Vídeo: Similar ao áudio e imagens, o vídeo oferece muitas oportunidades para ocultar dados devido ao grande volume de informações que ele contém.

Esteganografia: como funciona

- A esteganografia pode ser aplicada a diversos tipos de mídia digital, incluindo:
 - Texto: A esteganografia em texto pode envolver alterar a formatação do texto, usar espaços extras, mudar a capitalização de letras de maneiras sutis ou até mesmo usar certas palavras em sequências específicas para codificar uma mensagem.
 - Rede: Informações podem ser ocultadas em protocolos de rede, como nos cabeçalhos de pacotes TCP/IP.

Esteganografia: Exemplos Históricos

- A esteganografia não é uma técnica nova. Historicamente, existem diversos exemplos de seu uso:
 - Grécia Antiga: Mensagens eram escritas em tábuas de madeira e cobertas com cera.
 - Heródoto: Relata que Histiaeus raspou a cabeça de um escravo, tatuou uma mensagem em seu couro cabeludo e esperou que o cabelo crescesse para enviá-lo.
 - Tinta Invisível: Usada para escrever mensagens secretas entre linhas de texto aparentemente inocente.
 - Micropontos: Pequeníssimas fotografias usadas para esconder grandes quantidades de informação.

Esteganografia: Aplicações Modernas

- No mundo digital, a esteganografia tem diversas aplicações, tanto **legítimas** quanto maliciosas:
 - **Marcas d'água digitais:** Usadas para proteger direitos autorais, incorporando informações sobre o proprietário em arquivos de mídia.
 - **Comunicação secreta:** Embora controversa, pode ser usada para comunicação privada onde a existência da mensagem precisa ser oculta.
 - **Segurança de dados:** Pode ser usada como uma camada adicional de segurança, escondendo dados confidenciais dentro de arquivos aparentemente inócuos.

Esteganografia: Aplicações Modernas

- No mundo digital, a esteganografia tem diversas aplicações, tanto legítimas quanto **maliciosas**:
 - **Malware:** A esteganografia pode ser usada para esconder código malicioso dentro de arquivos de imagem ou outros tipos de mídia para evitar detecção por softwares antivírus.
 - **Exfiltração de dados:** Atacantes podem usar esteganografia para esconder dados roubados dentro de tráfego de rede normal ou arquivos de mídia para evitar a detecção durante a saída da informação.

Detecção (Estegoanálise)

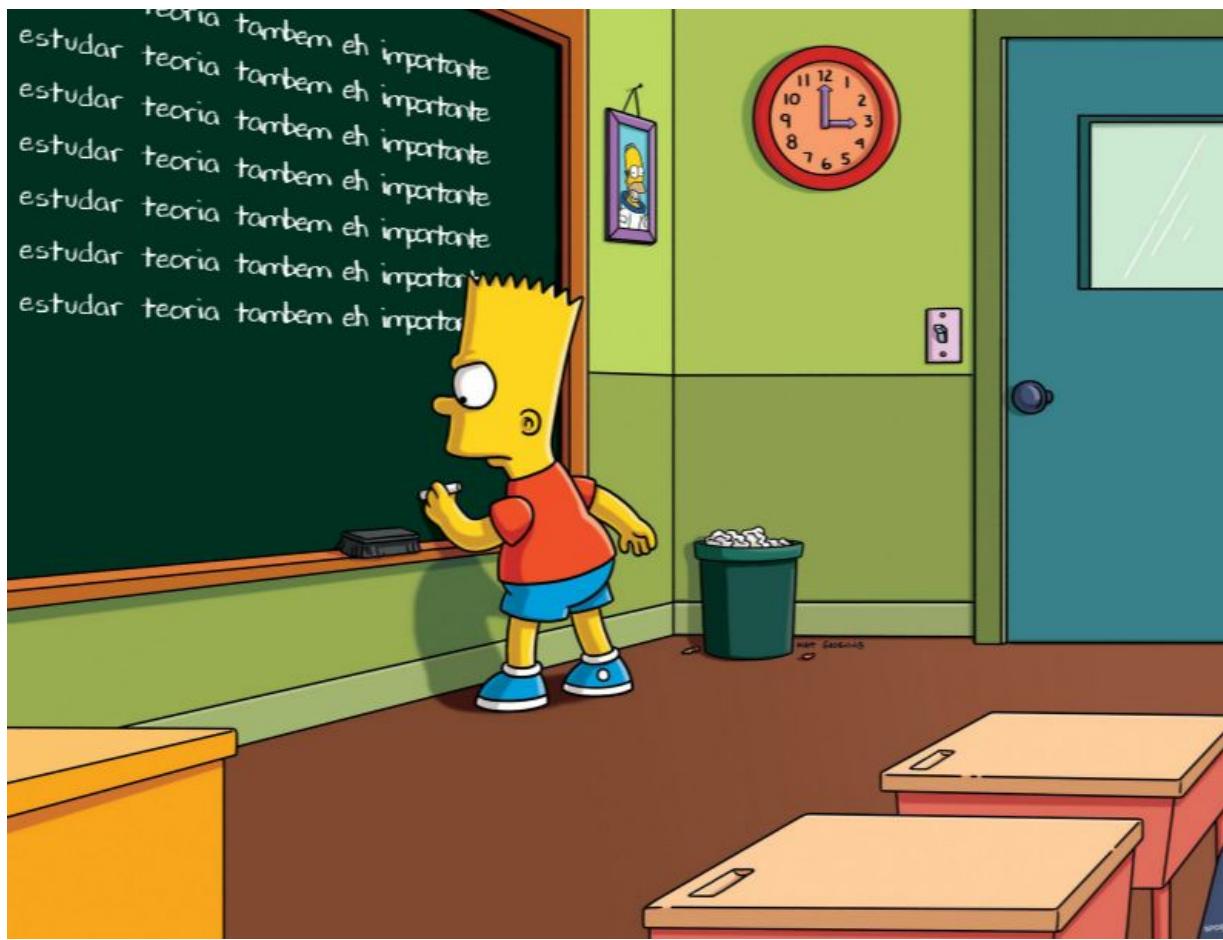
- A detecção de mensagens escondidas usando esteganografia é chamada de estegoanálise.
- É um campo complexo que envolve a análise de arquivos em busca de padrões incomuns ou anomalias estatísticas que possam indicar a presença de dados ocultos.

Esteganografia

- Esteganografia é usada por criminosos (ex.: malware escondido em imagens).
- Sempre verifique arquivos suspeitos com ferramentas como [binwalk](#).

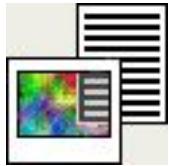
Esteganografia x Criptografia

- Enquanto a criptografia embaralha uma mensagem para torná-la ilegível sem a chave correta, a esteganografia busca esconder a própria existência da mensagem.
- Com a criptografia, você sabe que há uma mensagem secreta (embora não consiga lê-la), enquanto com a esteganografia, o objetivo é que ninguém suspeite que haja alguma informação oculta.



Exemplo: <https://github.com/ciberseguranca-pucpr/esteganografia>

StegHide



<https://www.kali.org/tools/steghide/>

<https://www.hackingarticles.in/comprehensive-guide-to-steghide-tool/>

Atividade

- Extrair dados esteganografados de imagens nos slides usando steghide
- Descriptografar a mensagem obtida
- Concluir a atividade proposta

? Qual a senha mais popular e fácil do mundo?

- 8 caracteres
- escrito em letras minúsculas

